Network Security & Firewall Implementation

MOD002685

By 1068664

Contents

Table of Figures

Background

The Directorate of Diplomatic Offices has recently decided that they would like a new network implemented.

This network requires interconnectivity of the offices based in Cambridge, Chicago and Rome. It also requires that a resilient T1 mesh network be implemented.

The anticipation of the number of potential hosts in each office is as follows:

- Cambridge 1,093
- Chicago 1,093
- Rome 2,300

They would also like to add a reservation of addresses for 12 further offices with a minimum of 550 hosts in each of these offices.

The organisation has not previously been connected to the internet, therefore they have not been allocated any blocks of addresses other than the dedicated internet link from Cambridge.

Requirements

- The organisation has the following requirements:
- Only users from Cambridge, Chicago & Rome can access the corporate data centre
- Only users on the Chicago administration VLAN can access the finance server
- Only users from Cambridge and Rome can access the research database using FTP, HTTP & HTTPS
- All users to be able to access an email server using POP, IMAP & SMTP
- Block access to IRC file sharing on various networks as will be provided
- Only allow connections to the internet that are internally initiated
- Log all security violation is a Syslog server

This report aims to implement all the requirements that are needed by the organisation.

Addressing

The major network address that will be utilised across all offices will be that of 10.0.0.0/8. Utilising this address will allow the organisation to issue address to all required hosts.

The number of address available in this major network is 16,777,214. The number of addresses needed by the organisation is 10, 492. The number of addresses available by subnetting is 14,312.

A little over 0% of the major network address space is used and 73% of subnetted address space is used. This will still allow for more hosts to be added should the need arise.

The public IP address block will need to be negotiated with the ISP, but it would be wise to try and obtain a block that is on the 209.123.234.0 network.

By utilising the 10.0.0.0/8 major network, this will allow the scalability of addressing that the organisation requires. The organisation is able to add more hosts to the current offices in Cambridge, Chicago and Rome. The potential is there to scale as much as is required by the organisation.

It is suggested that the organisation implement a hierarchical topology. This will be invaluable to the organisation when it needs to scale up or scale down as required. This topology allows for a set number of clients per switch, and a set number of access switches per distribution switch and so forth until the core layer switches.

This will allow the organisation to see where clients and switches need to be added and this can be done with ease based on this kind of topology.

Access Control

The access to the data centre, finance server, research database, mail server and ISP will be implemented through access control lists (ACL).

It is proposed that the following lists be created:

- Cambridge-In
- Cambridge-Out
- Chicago-Main-In
- Chicago-Main-Out
- Chicago-Admin-In
- Chicago-Admin-Out

- Rome-In
- Rome-Out

These lists will ensure that the necessary controls will be in place to implement the requirements as previously mentioned by the organisation.

The lists will be placed on the Ethernet subinterfaces of the routers at each of the offices. It was proposed to implement these on the Serial links between the routers, but this only served to prevent OSPF from properly propagating routes to neighbours.

These lists will be implemented on each of the sub interfaces as is necessary. The content of each list can be found in Appendix 1, along with flowcharts to show the logical flow.

Security

The routers and switches will be enabled with console (CON) and virtual teletype (VTY) access security. This will ensure that only those authorised to remotely access the routers and switches can. It will help prevent any unauthorised access to the devices.

The CON and VTY lines will be enabled with a timeout function, set to 5 minutes. They will also have a function that limits incorrect login attempts – this will be limited to 2 login attempts within 2 minutes. If this occurs, the remote user will be informed that connections are not allowed.

PPP CHAP authentication will be enabled on the SE ports on the routers to enable the receiving router to verify the identity of the sending router, thus allowing communication to take place.

The standard VLAN of 1 will be shut down and not utilised in any way on the networks as this poses a major security issue within the network.

A syslog server will be set up in the Cambridge office to handle all security violation logging. This will include login attempts to the routers and switches. It will also include ACL logging. Since ACL logging is CPU intensive, a balance will need to be struck. This balance will be achievable by limiting the type of violations logged, the interval between logs and the number of items logged.

The Network

The network will be set up as shown in the following few paragraphs. The design and setup will be represented in Packet Tracer to allow the organisation to virtually see how the network will be set up. As this is done virtually, some of the set up in real world will be different as Packet Tracer does not allow all commands and configurations to be utilised. Where this is the case, it will be noted in Appendix 3.

Each office is talked about along with the equipment and addressing utilised there. Topologies of each office network are also shown.

Cambridge

The Cambridge office is hosted on network 10.0.16.0.

The office at Cambridge will host the DHCP server and the Syslog server. The reason that they are both hosted at Cambridge is due to the organisation not stipulating that they are to be hosted on an address out with their network.

The DHCP server at Cambridge is to be considered as the main DHCP server. Backups of the DHCP server will be provided at both the Chicago and Rome offices. This offers a level of redundancy and also serves to offer continuity should any disaster arise at any of the offices.

The DHCP server also acts as the DNS server. Please see Appendix 2 for the DNS entries.

There are 4 PCs in Cambridge and these represent the required 1,093 hosts requested by the organisation.

These are all accessible across the entire network.

The router at Cambridge provides the clock speed to both Chicago and Rome.

The layout of Cambridge can be seen in figure 1.

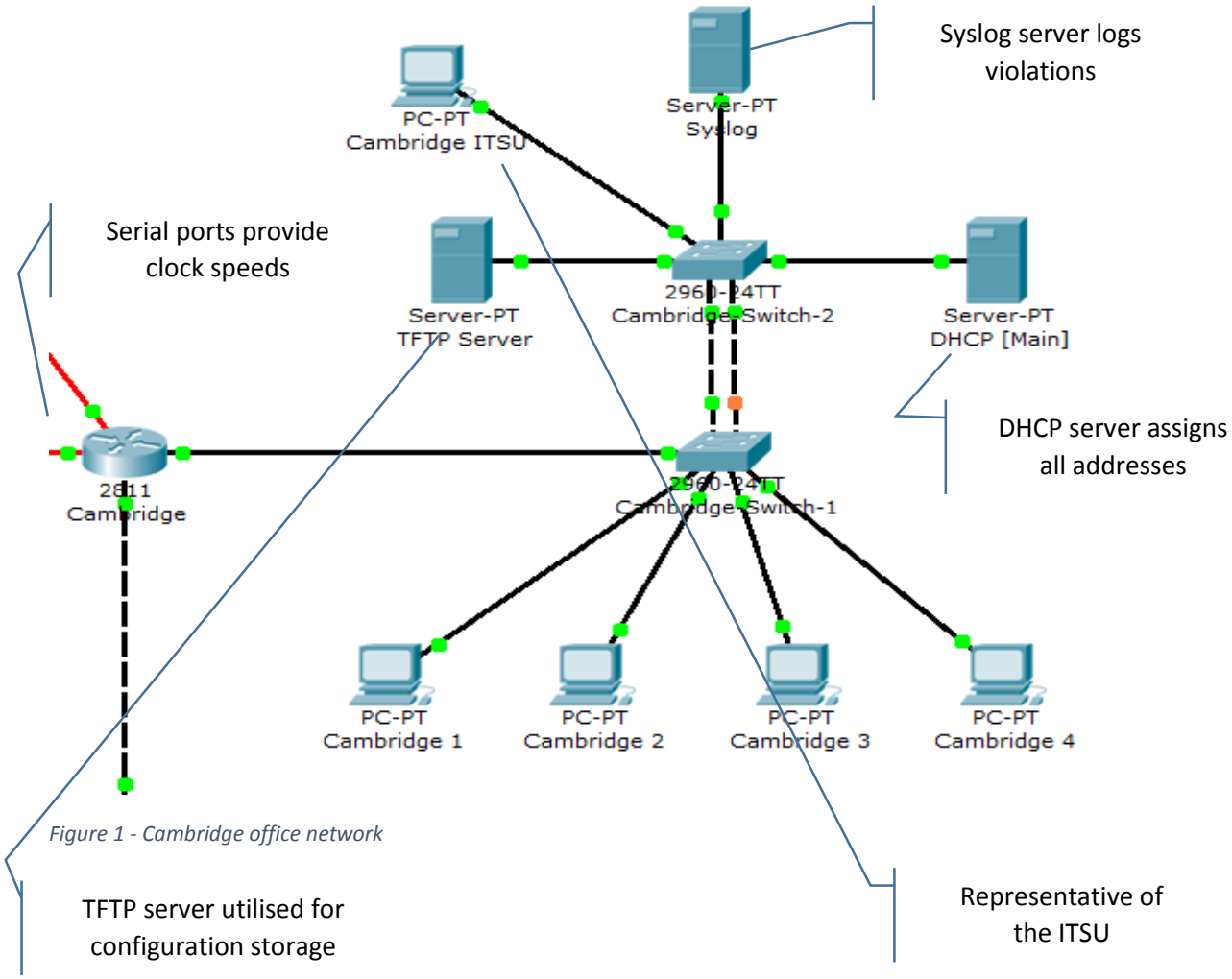

Figure 1 - Cambridge office network

Chicago

The Chicago office is hosted on networks 10.0.0.0 for regular host access and 10.0.15.0 for administration host access

The office at Chicago will host a backup DHCP server for purposes of continuity and disaster recovery.

There are 4 PCs in Chicago and these represent the required 2,300 hosts requested by the company. 1 of the PCs will be used to represent the administration VLAN to enable and show the implementation of the ACL as requested by the organisation.

These are all accessible across the entire network.

The router at Chicago provides no clock speeds, instead working at the speeds set by both Cambridge and Rome.

The layout of Chicago can be seen in figure 2.

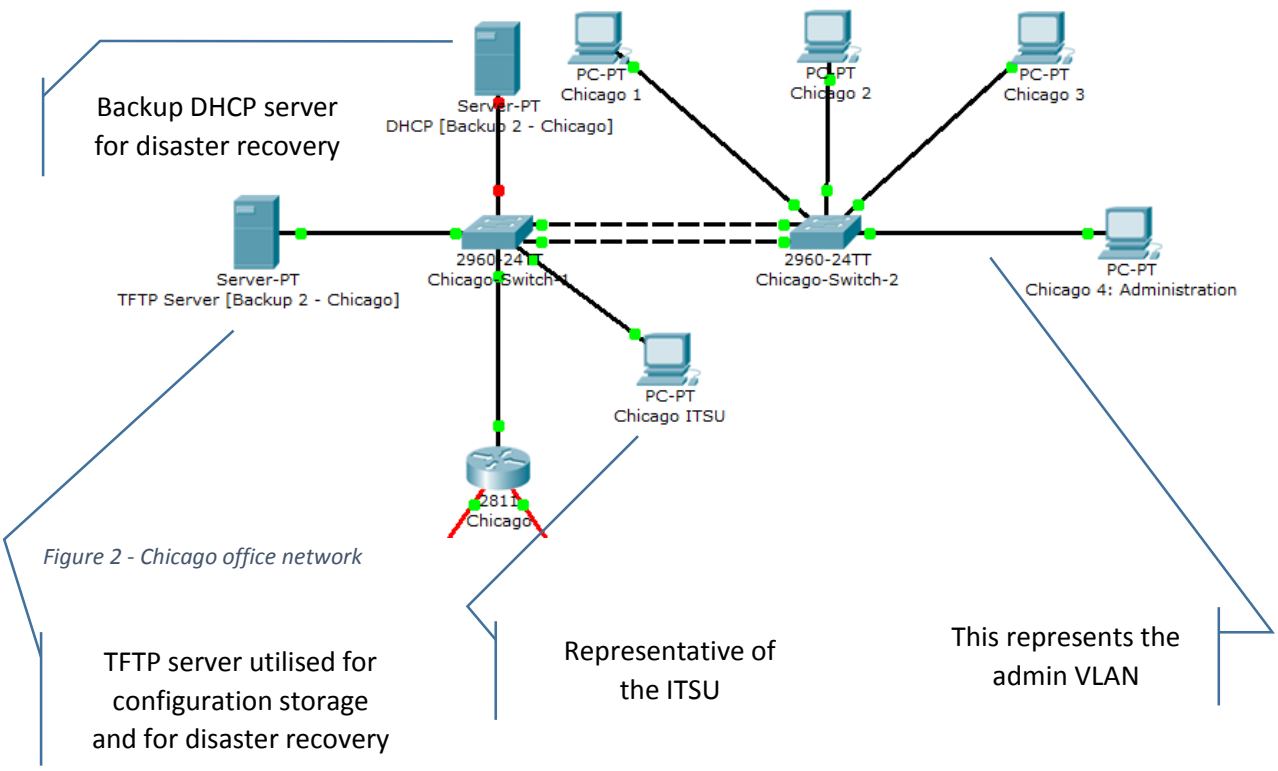

Figure 2 - Chicago office network

Rome

The Rome office is hosted on network 10.0.24.0

The office in Rome will also host a backup DHCP server for disaster recovery and continuity purposes. The office also has 4 PCs that represent the required 1,093 hosts as requested by the organisation.

These are all accessible across the entire network.

The Rome router provides the clock speed to Chicago.

The layout of Rome can be seen in figure 3.

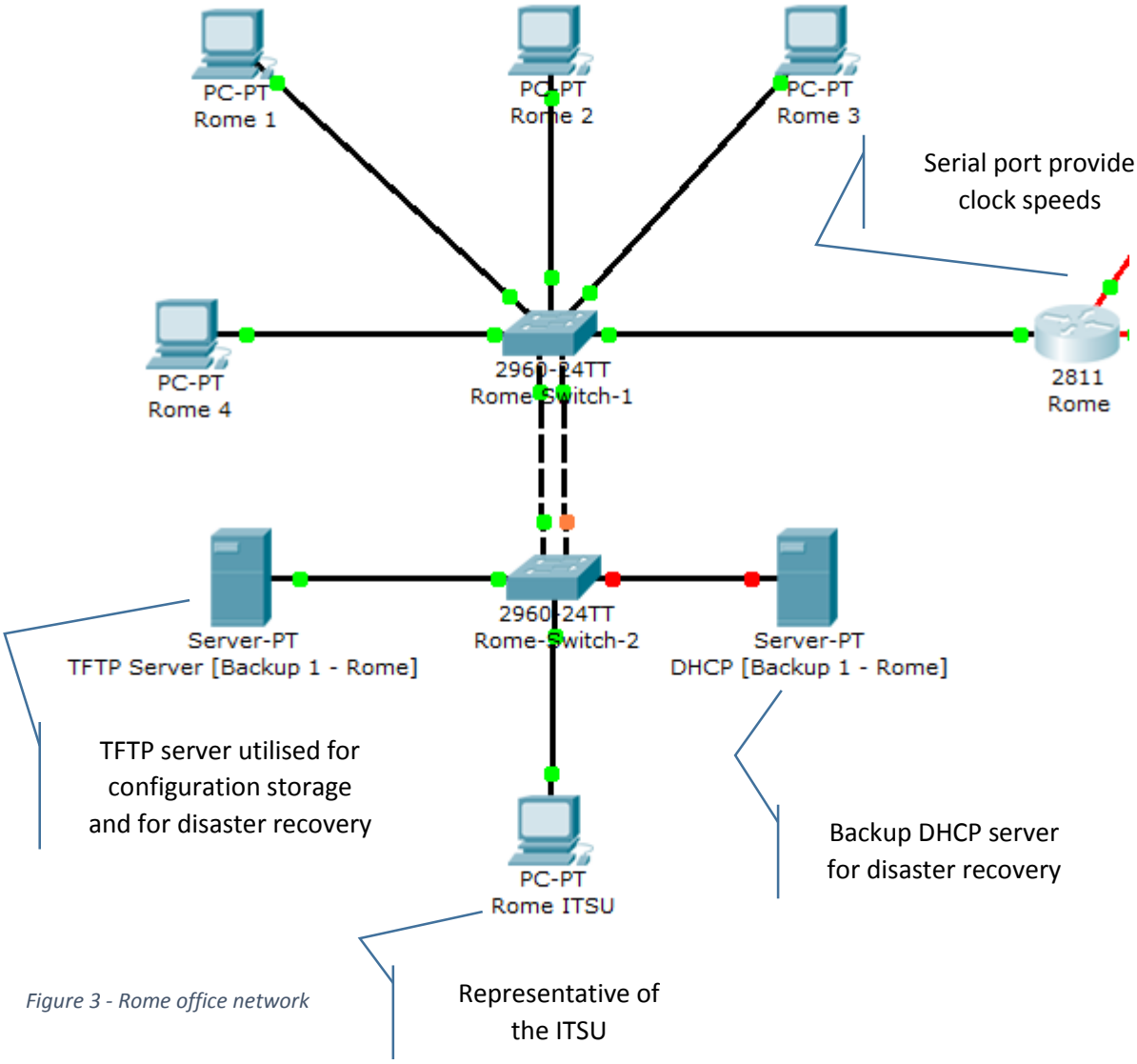

Figure 3 - Rome office network

ISP

As previously mentioned, the ISP represented by a router so that the network can be simulated to the organisation and to help ensure all requirements are met.

The ISP will host access to the finance server, mail server, research database and data centre.

In a real world networked environment, some of these services may be provided via Infrastructure as a Service (IaaS) or Software as a Service (SaaS) in the cloud.

This will be mentioned, where appropriate, when writing about the servers themselves.

The ISP router and switch have very basic configurations as they are only in place to simulate the ISP. Any configurations would be performed out with the network and the network team of the organisation.

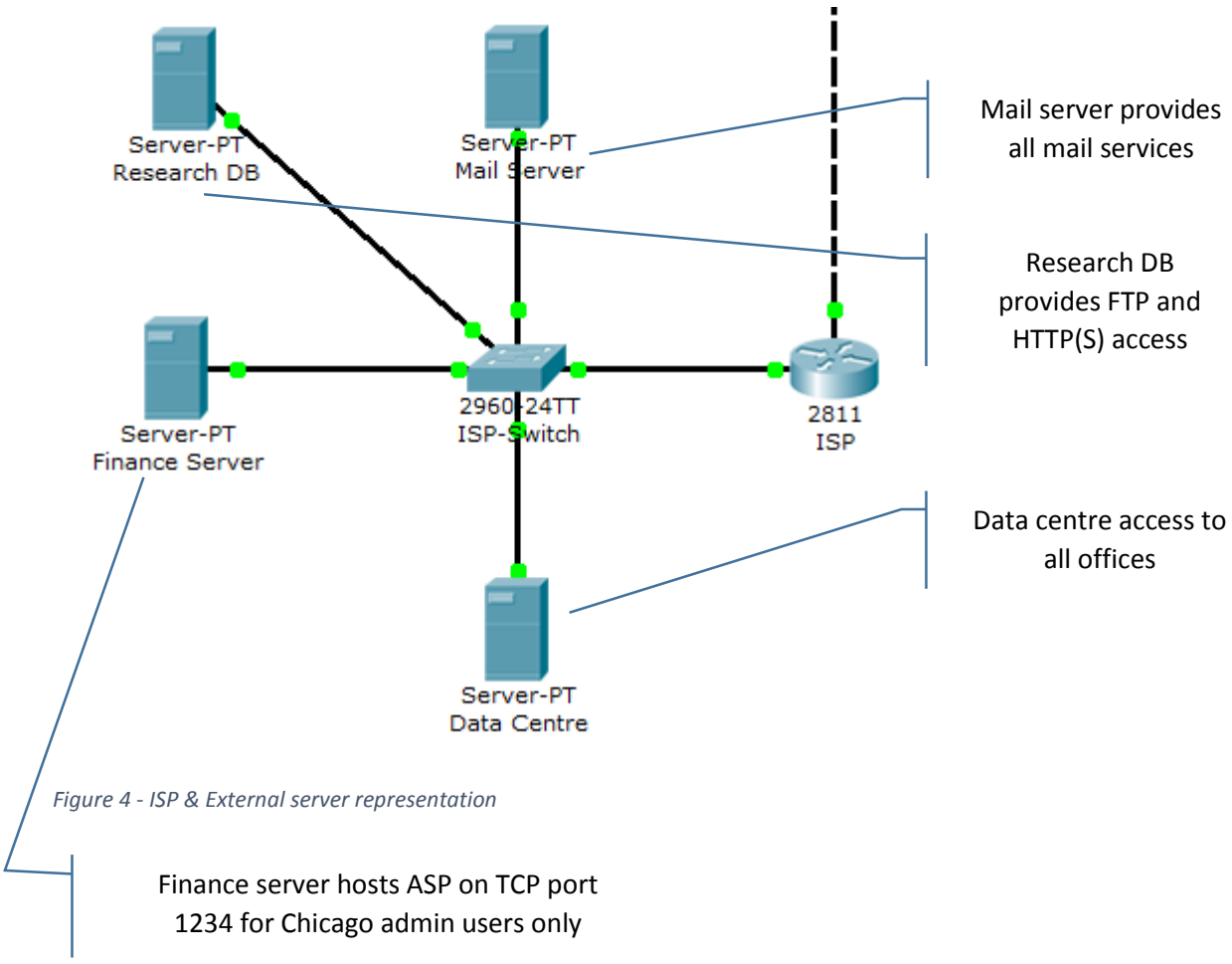

Figure 4 - ISP & External server representation

Clock Speeds

In a real world networked environment, the clock speed to Cambridge would be provided via the ISP utilising frame relay techniques.

Cambridge would then provide this speed to Rome. Rome, in turn, would provide this to Chicago.

Frame Relay

Frame relay works by utilising Virtual Private Circuits or VPCs. This enables the network to have a dedicated connection to other hosts and servers associated with the organisation. This will also ensure that no other network utilises the circuit for the length of the transfer helping to ensure data is not lost, corrupted and eavesdropped upon.

Mail Server

The mail server is to be accessed by all hosts on the network. The address that is to be used is 180.145.22.33. It is only to be accessed using POP, IMAP and SMTP.

All company users will be set up with a mail box and the email address will be username@mail.dipoff.com

Data Centre

The data centre is to be accessed at an address of 199.199.199.199. As no requirements were made other than all offices be allowed access, access types will not be limited.

In a real world networked environment, the data centre can be either a physical data centre with racks rented by the organisation, or it can be provided to them via IaaS or SaaS. In the technological era the organisation is now in, it will be most likely that the data centre will be utilised from the cloud allowing the data centre to be virtualised.

Finance Server

As previously mentioned, the finance server will only be accessible to the Chicago administration VLAN utilising a form of SaaS on TCP port 1234. Due to Packet Tracer limitations, the ACL required for this can only be demonstrated using a complex packet.

Research Database

The research database is only to be accessed by users in Cambridge and Rome. The database will be hosted at 194.123.88.99.

The access to the server has been defined by the organisation as FTP, HTTP and HTTPS. The ACL has been written to reflect this and can be demonstrated fairly easily in Packet Tracer.

File Sharing

File sharing has been identified utilising IRC on the following networks:

- 206.206.83.0
- 206.207.82.0
- 206.207.83.0
- 206.207.84.0
- 206.207.85.0

An ACL has been implemented to block these networks from being accessed using IRC. This block applies network wide.

SNMP

SNMP will be utilised network wide. This will enable the network to be monitored and managed to help ensure the smooth running of the network and to help fix any problems as soon as they arise.

All routers will be configured to allow SNMP to be implemented and an MIB will be set up to allow this monitoring to take place. The monitoring is utilised through IP addresses and communities.

This monitoring will be performed on the serial interfaces of the routers. Read Only communities will be implemented for the monitoring. The monitoring will gather some basic information that includes the basic location of each router and contact details for each network.

Packet Tracer PCs allow a very basic form of SNMP using the inbuilt MIB browser. The process will be able to be simulated utilising this browser on any of the office PCs.

TFTP

TFTP servers will be utilised at all sites. The servers will enable the configurations of the switches and routers to be backed up. This will enable the configurations to be recovered in the event of a disaster, power failure or faulty equipment that needs to be replaced. They are utilised across all sites to aid in disaster recovery and business continuity.

Recommendations

For the organisation, it is recommended that backup servers be utilised. It is also recommended to utilise cloud services where possible to help reduce the cost and strain on the network. These cloud services should include the data centre at the very least. Further options can be explored as and when it is deemed necessary for the organisation. At this stage, it is important that the organisation know these options are there.

It is also recommended that Frame Relay be implemented, with provision for this from the service provider. It is also recommended to implement VPN's to allow remote working for employees, helping to save costs for the organisation.

Conclusion

Utilising Packet Tracer has enabled the network to be simulated to the requirements of the organisation.

There have been some minor issues doing it this way and these have also been documented.

The original requirements of the organisations addressing and host requirement have been able to be met utilising an address of 10.0.0.0/8. This has also enabled hosts to be reserved for future use.

Appendix 1 - ACL

Cambridge In

remark ACL for inbound Access VLAN
permit udp any any eq bootps
permit udp any any eq domain
permit tcp any any eq domain
permit udp any any eq snmp
permit ip 10.0.16.0 0.0.7.255 199.199.199.0 0.0.0.255
permit tcp 10.0.16.0 0.0.7.255 194.123.88.0 0.0.0.255 eq 20
permit udp 10.0.16.0 0.0.7.255 194.123.88.0 0.0.0.255 eq 20
permit tcp 10.0.16.0 0.0.7.255 194.123.88.0 0.0.0.255 eq ftp
permit tcp 10.0.16.0 0.0.7.255 194.123.88.0 0.0.0.255 eq www
permit tcp 10.0.16.0 0.0.7.255 194.123.88.0 0.0.0.255 eq 443
permit tcp 10.0.16.0 0.0.7.255 180.145.22.0 0.0.0.255 eq 143
permit tcp 10.0.16.0 0.0.7.255 180.145.22.0 0.0.0.255 eq pop3
permit tcp 10.0.16.0 0.0.7.255 180.145.22.0 0.0.0.255 eq smtp
permit ip 10.0.16.0 0.0.7.255 209.123.234.4 0.0.0.3
permit ip 10.0.16.0 0.0.7.255 10.0.0.0 0.0.15.255
permit ip 10.0.16.0 0.0.7.255 10.0.16.0 0.0.7.255
permit udp 10.0.16.0 0.0.7.255 10.0.16.0 0.0.7.255 eq 514
permit ip 10.0.16.0 0.0.7.255 10.0.24.0 0.0.7.255
permit ip 10.0.16.0 0.0.7.255 10.0.32.0 0.0.0.127
permit ip 10.0.16.0 0.0.7.255 10.0.32.128 0.0.0.15
permit ip 10.0.16.0 0.0.7.255 10.0.32.144 0.0.0.15
permit ip 10.0.16.0 0.0.7.255 10.0.32.160 0.0.0.15
deny udp 10.0.16.0 0.0.7.255 206.206.83.0 0.0.0.255 eq 194
deny tcp 10.0.16.0 0.0.7.255 206.206.83.0 0.0.0.255 eq 194
deny udp 10.0.16.0 0.0.7.255 206.207.82.0 0.0.0.255 eq 194
deny tcp 10.0.16.0 0.0.7.255 206.207.82.0 0.0.0.255 eq 194
deny udp 10.0.16.0 0.0.7.255 206.207.83.0 0.0.0.255 eq 194
deny tcp 10.0.16.0 0.0.7.255 206.207.83.0 0.0.0.255 eq 194
deny udp 10.0.16.0 0.0.7.255 206.207.84.0 0.0.0.255 eq 194
deny tcp 10.0.16.0 0.0.7.255 206.207.84.0 0.0.0.255 eq 194
deny udp 10.0.16.0 0.0.7.255 206.207.85.0 0.0.0.255 eq 194
deny tcp 10.0.16.0 0.0.7.255 206.207.85.0 0.0.0.255 eq 194
deny ip 10.0.16.0 0.0.7.255 200.200.200.0 0.0.0.255
deny ip any any

Cambridge Out

remark ACL for outbound Access VLAN
permit ospf any any
permit icmp any any ttl-exceeded
permit ip 199.199.199.0 0.0.0.255 10.0.16.0 0.0.7.255
permit tcp 194.123.88.0 0.0.0.255 10.0.16.0 0.0.7.255 eq 20
permit udp 194.123.88.0 0.0.0.255 10.0.16.0 0.0.7.255 eq 20
permit tcp 194.123.88.0 0.0.0.255 10.0.16.0 0.0.7.255 eq ftp
permit tcp 194.123.88.0 0.0.0.255 10.0.16.0 0.0.7.255 eq www
permit tcp 194.123.88.0 0.0.0.255 10.0.16.0 0.0.7.255 eq 443
permit tcp 180.145.22.0 0.0.0.255 10.0.16.0 0.0.7.255 eq smtp established
permit tcp 180.145.22.0 0.0.0.255 10.0.16.0 0.0.7.255 eq 143 established
permit tcp 180.145.22.0 0.0.0.255 10.0.16.0 0.0.7.255 eq pop3 established
permit tcp 209.123.234.4 0.0.0.3 10.0.16.0 0.0.7.255 established
permit ip 10.0.0.0 0.0.15.255 10.0.16.0 0.0.7.255
permit ip 10.0.16.0 0.0.7.255 10.0.16.0 0.0.7.255
permit ip 10.0.24.0 0.0.7.255 10.0.16.0 0.0.7.255
permit ip 10.0.32.0 0.0.0.127 10.0.16.0 0.0.7.255
permit ip 10.0.32.128 0.0.0.15 10.0.16.0 0.0.7.255
permit ip 10.0.32.144 0.0.0.15 10.0.16.0 0.0.7.255
permit ip 10.0.32.160 0.0.0.15 10.0.16.0 0.0.7.255
permit udp 10.0.32.176 0.0.0.3 host 10.0.16.253 eq 514
permit udp 10.0.32.180 0.0.0.3 host 10.0.16.253 eq 514
permit udp 10.0.32.128 0.0.0.3 host 10.0.16.253 eq 514
permit udp 10.0.32.144 0.0.0.15 host 10.0.16.253 eq 514
permit udp 10.0.32.160 0.0.0.15 host 10.0.16.253 eq 514
deny ip any any

Chicago Main In

remark ACL for inbound Access VLAN
permit udp any any eq bootps
permit udp any any eq domain
permit tcp any any eq domain
permit udp any any eq snmp
permit ip 10.0.0.0 0.0.15.255 199.199.199.0 0.0.0.255
permit ip 10.0.0.0 0.0.15.255 209.123.234.4 0.0.0.3
permit ip 10.0.0.0 0.0.15.255 10.0.0.0 0.0.15.255
permit ip 10.0.0.0 0.0.15.255 10.0.16.0 0.0.7.255
permit udp 10.0.0.0 0.0.15.255 10.0.16.0 0.0.7.255 eq 514
permit ip 10.0.0.0 0.0.15.255 10.0.24.0 0.0.7.255
permit ip 10.0.0.0 0.0.15.255 10.0.32.0 0.0.0.127
permit ip 10.0.0.0 0.0.15.255 10.0.32.128 0.0.0.15
permit ip 10.0.0.0 0.0.15.255 10.0.32.144 0.0.0.15
permit ip 10.0.0.0 0.0.15.255 10.0.32.160 0.0.0.15
permit tcp 10.0.0.0 0.0.15.255 180.145.22.0 0.0.0.255 eq 143
permit tcp 10.0.0.0 0.0.15.255 180.145.22.0 0.0.0.255 eq pop3
permit tcp 10.0.0.0 0.0.15.255 180.145.22.0 0.0.0.255 eq smtp
deny tcp 10.0.0.0 0.0.15.255 194.123.88.0 0.0.0.255 eq 20
deny udp 10.0.0.0 0.0.15.255 194.123.88.0 0.0.0.255 eq 20
deny tcp 10.0.0.0 0.0.15.255 194.123.88.0 0.0.0.255 eq ftp
deny tcp 10.0.0.0 0.0.15.255 194.123.88.0 0.0.0.255 eq www
deny tcp 10.0.0.0 0.0.15.255 194.123.88.0 0.0.0.255 eq 443
deny ip 10.0.0.0 0.0.15.255 200.200.200.0 0.0.0.255
deny udp 10.0.0.0 0.0.15.255 206.206.83.0 0.0.0.255 eq 194
deny tcp 10.0.0.0 0.0.15.255 206.206.83.0 0.0.0.255 eq 194
deny udp 10.0.0.0 0.0.15.255 206.207.82.0 0.0.0.255 eq 194
deny tcp 10.0.0.0 0.0.15.255 206.207.82.0 0.0.0.255 eq 194
deny udp 10.0.0.0 0.0.15.255 206.207.83.0 0.0.0.255 eq 194
deny tcp 10.0.0.0 0.0.15.255 206.207.83.0 0.0.0.255 eq 194
deny udp 10.0.0.0 0.0.15.255 206.207.84.0 0.0.0.255 eq 194
deny tcp 10.0.0.0 0.0.15.255 206.207.84.0 0.0.0.255 eq 194
deny udp 10.0.0.0 0.0.15.255 206.207.85.0 0.0.0.255 eq 194
deny tcp 10.0.0.0 0.0.15.255 206.207.85.0 0.0.0.255 eq 194
deny ip any any

Chicago Main Out

remark ACL for outbound Access VLAN
permit ospf any any
permit icmp any any ttl-exceeded
permit ip 199.199.199.0 0.0.0.255 10.0.0.0 0.0.15.255
permit tcp 180.145.22.0 0.0.0.255 10.0.0.0 0.0.15.255 eq smtp established
permit tcp 180.145.22.0 0.0.0.255 10.0.0.0 0.0.15.255 eq 143 established
permit tcp 180.145.22.0 0.0.0.255 10.0.0.0 0.0.15.255 eq pop3 established
permit tcp 209.123.234.4 0.0.0.3 10.0.0.0 0.0.15.255 established
permit ip 10.0.0.0 0.0.15.255 10.0.0.0 0.0.15.255
permit ip 10.0.16.0 0.0.7.255 10.0.0.0 0.0.15.255
permit ip 10.0.24.0 0.0.7.255 10.0.0.0 0.0.15.255
permit ip 10.0.32.0 0.0.0.127 10.0.0.0 0.0.15.255
permit ip 10.0.32.128 0.0.0.15 10.0.0.0 0.0.15.255
permit ip 10.0.32.144 0.0.0.15 10.0.0.0 0.0.15.255
permit ip 10.0.32.160 0.0.0.15 10.0.0.0 0.0.15.255
deny ip any any

Chicago Admin In

```
remark ACL for inbound Admin VLAN
permit udp any any eq bootps
permit udp any any eq domain
permit tcp any any eq domain
permit udp any any eq snmp
permit ip 10.0.32.0 0.0.0.127 199.199.199.0 0.0.0.255
permit tcp 10.0.32.0 0.0.0.127 200.200.200.0 0.0.0.255 eq 1234
permit ip 10.0.32.0 0.0.0.127 209.123.234.4 0.0.0.3
permit ip 10.0.32.0 0.0.0.127 10.0.0.0 0.0.15.255
permit ip 10.0.32.0 0.0.0.127 10.0.16.0 0.0.7.255
permit udp 10.32.0.0 0.0.0.127 10.0.16.0 0.0.7.255 eq 514
permit ip 10.0.32.0 0.0.0.127 10.0.24.0 0.0.7.255
permit ip 10.0.32.0 0.0.0.127 10.0.32.0 0.0.15.255
permit tcp 10.0.32.0 0.0.0.127 180.145.22.0 0.0.0.255 eq 143
permit tcp 10.0.32.0 0.0.0.127 180.145.22.0 0.0.0.255 eq pop3
permit tcp 10.0.32.0 0.0.0.127 180.145.22.0 0.0.0.255 eq smtp
deny tcp 10.0.32.0 0.0.0.127 194.123.88.0 0.0.0.255 eq 20
deny udp 10.0.32.0 0.0.0.127 194.123.88.0 0.0.0.255 eq 20
deny tcp 10.0.32.0 0.0.0.127 194.123.88.0 0.0.0.255 eq ftp
deny tcp 10.0.32.0 0.0.0.127 194.123.88.0 0.0.0.255 eq www
deny tcp 10.0.32.0 0.0.0.127 194.123.88.0 0.0.0.255 eq 443
deny udp 10.0.32.0 0.0.0.127 206.206.83.0 0.0.0.255 eq 194
deny tcp 10.0.32.0 0.0.0.127 206.206.83.0 0.0.0.255 eq 194
deny udp 10.0.32.0 0.0.0.127 206.207.82.0 0.0.0.255 eq 194
deny tcp 10.0.32.0 0.0.0.127 206.207.82.0 0.0.0.255 eq 194
deny udp 10.0.32.0 0.0.0.127 206.207.83.0 0.0.0.255 eq 194
deny tcp 10.0.32.0 0.0.0.127 206.207.83.0 0.0.0.255 eq 194
deny udp 10.0.32.0 0.0.0.127 206.207.84.0 0.0.0.255 eq 194
deny tcp 10.0.32.0 0.0.0.127 206.207.84.0 0.0.0.255 eq 194
deny udp 10.0.32.0 0.0.0.127 206.207.85.0 0.0.0.255 eq 194
deny tcp 10.0.32.0 0.0.0.127 206.207.85.0 0.0.0.255 eq 194
deny ip any any
```

Chicago Admin Out

```
remark ACL for outbound Admin VLAN
permit ospf any any
permit icmp any any ttl-exceeded
permit ip 199.199.199.0 0.0.0.255 10.0.32.0 0.0.0.127
permit tcp 200.200.200.0 0.0.0.255 10.0.32.0 0.0.0.127 eq 1234
permit tcp 180.145.22.0 0.0.0.255 10.0.32.0 0.0.0.127 eq smtp established
permit tcp 180.145.22.0 0.0.0.255 10.0.32.0 0.0.0.127 eq 143 established
permit tcp 180.145.22.0 0.0.0.255 10.0.32.0 0.0.0.127 eq pop3 established
permit tcp 209.123.234.4 0.0.0.3 10.0.32.0 0.0.0.127 established
permit ip 10.0.0.0 0.0.15.255 10.0.32.0 0.0.0.127
permit ip 10.0.16.0 0.0.7.255 10.0.32.0 0.0.0.127
permit ip 10.0.24.0 0.0.7.255 10.0.32.0 0.0.0.127
permit ip 10.0.32.0 0.0.0.127 10.0.32.0 0.0.0.127
permit ip 10.0.32.128 0.0.0.15 10.0.32.0 0.0.0.127
permit ip 10.0.32.144 0.0.0.15 10.0.32.0 0.0.0.127
permit ip 10.0.32.160 0.0.0.15 10.0.32.0 0.0.0.127
deny ip any any
```

Rome In

remark ACL for inbound Access VLAN
permit udp any any eq bootps
permit udp any any eq domain
permit tcp any any eq domain
permit udp any any eq snmp
permit ip 10.0.24.0 0.0.7.255 199.199.199.0 0.0.0.255
permit tcp 10.0.24.0 0.0.7.255 194.123.88.0 0.0.0.255 eq 20
permit udp 10.0.24.0 0.0.7.255 194.123.88.0 0.0.0.255 eq 20
permit tcp 10.0.24.0 0.0.7.255 194.123.88.0 0.0.0.255 eq ftp
permit tcp 10.0.24.0 0.0.7.255 194.123.88.0 0.0.0.255 eq www
permit tcp 10.0.24.0 0.0.7.255 194.123.88.0 0.0.0.255 eq 443
permit tcp 10.0.24.0 0.0.7.255 180.145.22.0 0.0.0.255 eq 143
permit tcp 10.0.24.0 0.0.7.255 180.145.22.0 0.0.0.255 eq pop3
permit tcp 10.0.24.0 0.0.7.255 180.145.22.0 0.0.0.255 eq smtp
permit ip 10.0.24.0 0.0.7.255 209.123.234.4 0.0.0.3
permit ip 10.0.24.0 0.0.7.255 10.0.0.0 0.0.15.255
permit ip 10.0.24.0 0.0.7.255 10.0.16.0 0.0.7.255
permit udp 10.0.24.0 0.0.7.255 10.0.16.0 0.0.7.255 eq 514
permit ip 10.0.24.0 0.0.7.255 10.0.24.0 0.0.7.255
permit ip 10.0.24.0 0.0.7.255 10.0.32.0 0.0.0.127
permit ip 10.0.24.0 0.0.7.255 10.0.32.128 0.0.0.15
permit ip 10.0.24.0 0.0.7.255 10.0.32.144 0.0.0.15
permit ip 10.0.24.0 0.0.7.255 10.0.32.160 0.0.0.15
deny udp 10.0.24.0 0.0.7.255 206.206.83.0 0.0.0.255 eq 194
deny tcp 10.0.24.0 0.0.7.255 206.206.83.0 0.0.0.255 eq 194
deny udp 10.0.24.0 0.0.7.255 206.207.82.0 0.0.0.255 eq 194
deny tcp 10.0.24.0 0.0.7.255 206.207.82.0 0.0.0.255 eq 194
deny udp 10.0.24.0 0.0.7.255 206.207.83.0 0.0.0.255 eq 194
deny tcp 10.0.24.0 0.0.7.255 206.207.83.0 0.0.0.255 eq 194
deny udp 10.0.24.0 0.0.7.255 206.207.84.0 0.0.0.255 eq 194
deny tcp 10.0.24.0 0.0.7.255 206.207.84.0 0.0.0.255 eq 194
deny udp 10.0.24.0 0.0.7.255 206.207.85.0 0.0.0.255 eq 194
deny tcp 10.0.24.0 0.0.7.255 206.207.85.0 0.0.0.255 eq 194
deny ip 10.0.24.0 0.0.7.255 200.200.200.0 0.0.0.255
deny ip any any

Rome Out

remark ACL for outbound Access VLAN
permit ospf any any
permit icmp any any ttl-exceeded
permit ip 199.199.199.0 0.0.0.255 10.0.24.0 0.0.7.255
permit tcp 194.123.88.0 0.0.0.255 10.0.24.0 0.0.7.255 eq 20
permit udp 194.123.88.0 0.0.0.255 10.0.24.0 0.0.7.255 eq 20
permit tcp 194.123.88.0 0.0.0.255 10.0.24.0 0.0.7.255 eq ftp
permit tcp 194.123.88.0 0.0.0.255 10.0.24.0 0.0.7.255 eq www
permit tcp 194.123.88.0 0.0.0.255 10.0.24.0 0.0.7.255 eq 443
permit tcp 180.145.22.0 0.0.0.255 10.0.24.0 0.0.7.255 eq smtp established
permit tcp 180.145.22.0 0.0.0.255 10.0.24.0 0.0.7.255 eq 143 established
permit tcp 180.145.22.0 0.0.0.255 10.0.24.0 0.0.7.255 eq pop3 established
permit tcp 209.123.234.4 0.0.0.3 10.0.24.0 0.0.7.255 established
permit ip 10.0.0.0 0.0.15.255 10.0.24.0 0.0.7.255
permit ip 10.0.16.0 0.0.7.255 10.0.24.0 0.0.7.255
permit ip 10.0.24.0 0.0.7.255 10.0.24.0 0.0.7.255
permit ip 10.0.32.0 0.0.0.127 10.0.24.0 0.0.7.255
permit ip 10.0.32.128 0.0.0.15 10.0.24.0 0.0.7.255
permit ip 10.0.32.144 0.0.0.15 10.0.24.0 0.0.7.255
permit ip 10.0.32.160 0.0.0.15 10.0.24.0 0.0.7.255
deny ip any any

Figures 5 and 6 show how an ACL works on the network. Figure 5 is for traffic entering the network and figure 6 is for traffic exiting the network.

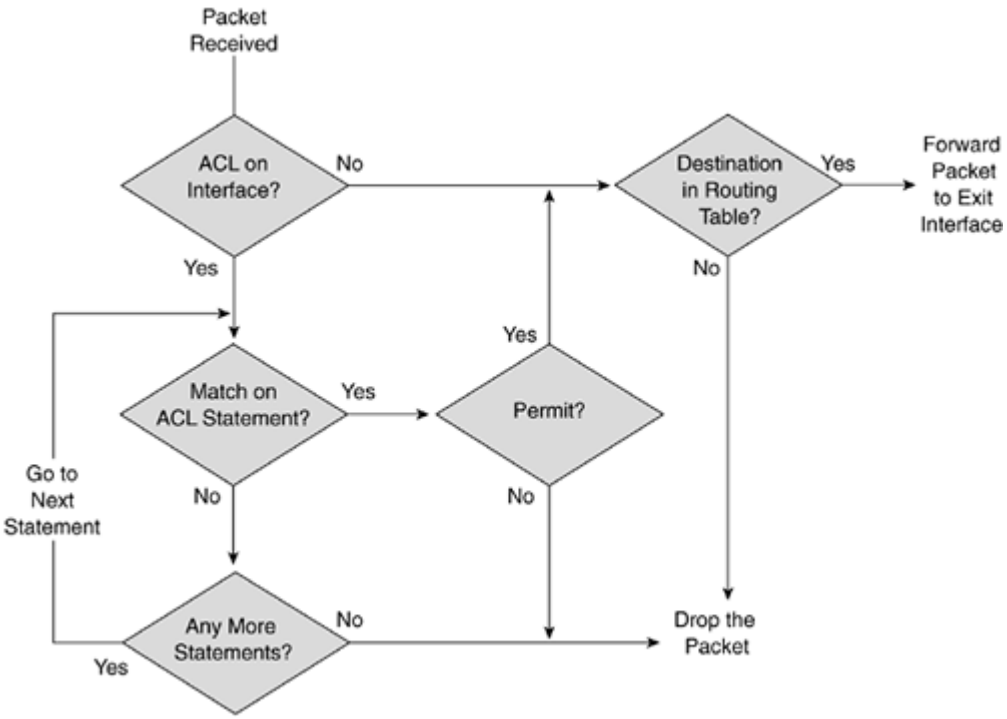

Figure 5 - Entry into the network (ACL IN)

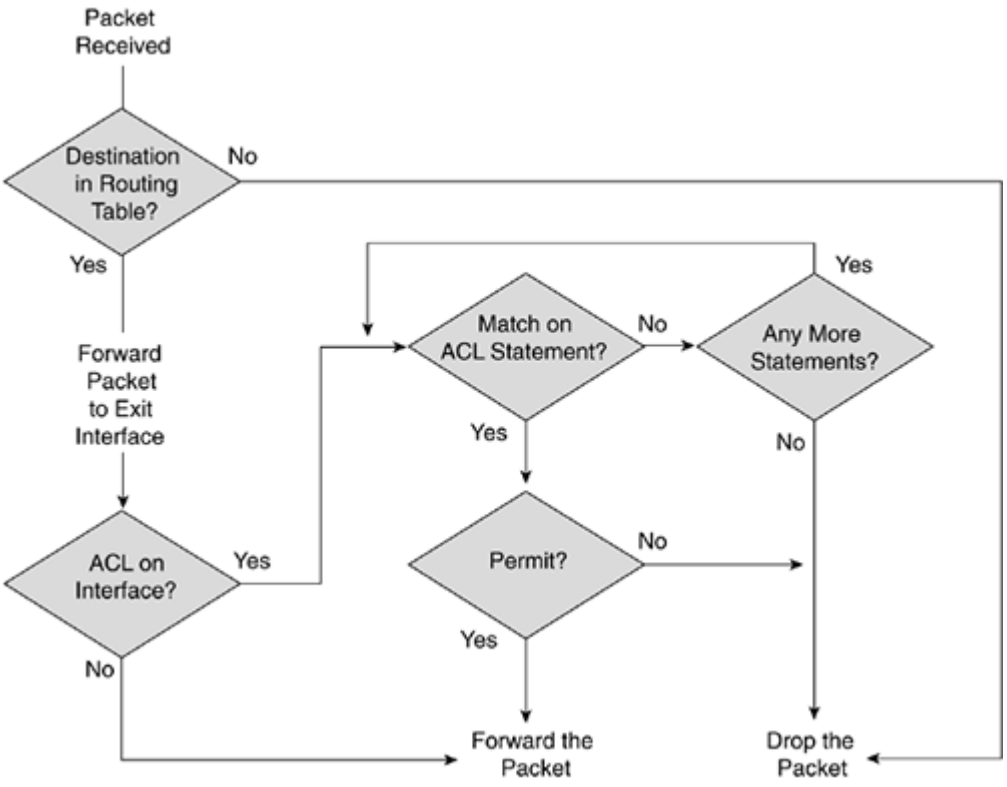

Figure 6 - Exit out of the network (ACL OUT)

The established keyword ensures that only connections initiated from inside the network can send data back into the network. This ensures no outside connection can penetrate the network whether inadvertently or maliciously.

In a real world networked environment, this would be implemented using the reflect keyword on both the inbound and outbound ACLs. This is useful if access is allowed through ports that are dynamic.

Appendix 2 – DNS & Mail Server

The DNS server is hosted at address 10.0.16.253

This server handles the translating of the research database web server to http://intranet.

It also allows for the address mail.dipoff.com to be forwarded to the IP address of the mail server.

Appendix 3 – Packet Tracer Limitations

Finance Server

It is important to note here that it is not possible to have a TCP service running on port 1234 on the finance server as Packet Tracer does not allow this feature. When the network is implemented in real world, the finance server will be running an ASP on TCP port 1234, thus allowing the ACL to be fully and properly implemented.

For the purposes of demonstrating this to the organisation, it will be necessary to use a complex PDU in Packet Tracer to show how this done. However, the packet will come back as a fail and state there is no service running on that port.

Mail Server

The simulation in Packet Tracer does not allow the mail server to be utilised as it would be in a real world networked environment. Packet Tracer randomly assigns a port to the email program on each PC and increases by 1 every time it is used. This does not allow mail to be sent using the program.

However, a complex PDU utilising port 25 will allow the ACL to be tested. The ACL cannot be written to allow random port access and this is why it would fail using the email program.

The same is the case for receiving mail utilising POP and also for sending and receiving mail utilising IMAP.

Research Database

It is not possible to show the access via FTP, HTTP and HTTPS as Packet Tracer randomly assigns a port number greater that 1025 to initiate connections. It is, therefore, only possible to do this using a complex PDU.

Frame Relay

Due to the limitations of Packet Tracer, a representation of the ISP utilising frame relay to the network is not achievable. It is, therefore, only possible to show this by representing the ISP with a router and corresponding serial connection to Cambridge.

Test Log

DHCP

Source		Destination			
Network	IP	Name	IP	Result	Corrective Action
Cambridge	10.0.16.0	DHCP Server	10.0.16.254	P	--
Chicago M	10.0.0.0	DHCP Server	10.0.16.254	F	Allowed DHCP via ACL IN
Chicago A	10.0.15.0	DHCP Server	10.0.16.254	F	Implemented VLAN 20
Rome	10.0.24.0	DHCP Server	10.0.16.254	F	Allowed DHCP via ACL IN

Syslog

Source		Destination			
Network	IP	Name	IP	Result	Corrective Action
Cambridge	10.0.16.0	Syslog Server	10.0.16.253	P	--
Chicago M	10.0.0.0	Syslog Server	10.0.16.253	F	Allowed syslog via Cambridge ACL OUT
Chicago A	10.0.15.0	Syslog Server	10.0.16.253	F	Allowed syslog via Cambridge ACL OUT
Rome	10.0.24.0	Syslog Server	10.0.16.253	F	Allowed syslog via Cambridge ACL OUT

Routers

Source		Destination			
Name	IP	Name	IP	Result	Corrective Action
Cambridge S0/0/0	10.0.32.177	Rome S0/0/1	10.0.32.178	P	--
Cambridge S0/0/1	10.0.32.181	Chicago S0/0/1	10.0.32.182	P	--
Chicago S0/0/0	10.0.32.186	Rome S0/0/0	10.0.32.185	P	--
Chicago S0/0/1	10.0.32.182	Cambridge S0/0/01	10.0.32.177	P	Note: Fails when ACL is implemented on port
Rome S0/0/0	10.0.32.185	Chicago S0/0/0	10.0.32.186	P	--
Rome S0/0/1	10.0.32.178	Cambridge S0/0/1	10.0.32.181	P	--

Servers

Mail

Source		Destination			
Network	IP	Name	IP	Result	Corrective Action
Cambridge	10.0.16.0	Mail Server	180.145.22.33	P	--
Chicago M	10.0.0.0	Mail Server	180.145.22.33	F	Allowed via ACL OUT
Chicago A	10.0.15.0	Mail Server	180.145.22.33	F	Allowed via ACL OUT
Rome	10.0.24.0	Mail Server	180.145.22.33	F	Allowed via ACL OUT

Finance

Source		Destination			
Network	IP	Name	IP	Result	Corrective Action
Cambridge	10.0.16.0	Finance Server	200.200.200.200	P	Note: Required block
Chicago M	10.0.0.0	Finance Server	200.200.200.200	P	Note: Required block
Chicago A	10.0.15.0	Finance Server	200.200.200.200	F	Allowed via ACL IN
Rome	10.0.24.0	Finance Server	200.200.200.200	P	Note: Required block

Data Centre

Source		Destination			
Network	IP	Name	IP	Result	Corrective Action
Cambridge	10.0.16.0	Data Centre	199.199.199.199	P	--
Chicago M	10.0.0.0	Data Centre	199.199.199.199	P	--
Chicago A	10.0.15.0	Data Centre	199.199.199.199	F	Implemented VLAN 20
Rome	10.0.24.0	Data Centre	199.199.199.199	P	--

Research Database

Source		Destination			
Network	IP	Name	IP	Result	Corrective Action
Cambridge	10.0.16.0	Research DB	194.123.88.99	P	--
Chicago M	10.0.0.0	Research DB	194.123.88.99	P	Note: Required block
Chicago A	10.0.15.0	Research DB	194.123.88.99	P	Note: Required block
Rome	10.0.24.0	Research DB	194.123.88.99	P	--

Spanning Tree

There were issues between the switches in Chicago that caused a broadcast storm to occur. The root bridge was not able to be selected due to this storm occurring. It was required to manually set the bridge ID to enable the root bridge to be selected.

Bibliography

Cisco, n.d. *Cisco Support Community - Technical Support Forum.* [Online]
Available at: https://supportforums.cisco.com/index.jspa
[Accessed 10 03 2013].

Lewis, W., 2008. *LAN Switching and Wireless: CCNA Exploration Companion Guide.* Indianapolis: Cisco Press.

networking-forum.com, n.d. *networking-forum.com - Cisco Networking.* [Online]
Available at: http://www.networking-forum.com/viewforum.php?f=50
[Accessed 10 03 2013].

TechExams.net, n.d. *TechExams.net.* [Online]
Available at: http://www.techexams.net/forums/
[Accessed 10 03 2013].

Vachon, B. & Graziani, R., 2008. *Accessing the WAN: CCNA Exploration Companion Guide.* Indianapolis: Cisco Press.