ABERCROMBIE ARCHITECTURAL FIRM

Network Design and Upgrade Proposal

Abercrombie Architectural Firm:

Network Design and Upgrade Proposal

Executive Abstract

Elite Networking received a Request for Proposal (RFP) from Abercrombie Architectural Firm, the request states several sites located internationally are to have networks built and/or to have existing infrastructure updated. This proposal specified requirements for the following:

- Design and build networks for sites in Virginia Beach, San Diego, Buenos Aires, and Leeds (See Appendix A)
- Upgrade the existing headquarters of Spokane , Washington, USA (See Appendix B)

Keywords: Network architecture, IDS, IPS, cost analysis, network security

Table of Contents

Scope of Work

Abercrombie Architectural Firm has request proposal for deigning and upgrading 4 sites located internationally, and upgrading their existing headquarters. Requirements must be met including but not limited to ensuring network security meets industry standards, providing network availability across all sites, providing cross domain support (the ability to access the resources of a remote site from the users current site), installing state-of-the-art hardware and software, and providing training to oncoming staff in the maintenance and operation of the new network. Abercrombie Architectural Firm has requested consultation and documentation regarding all provided network technologies as well as operational and policy documents for the operation of the network.

A comprehensive list of all deliverables, technical designs and specifications, cost analysis, and scheduling have been provided. Elite Networking has included performance reviews of all servers, the computers that manage access to resources, these performance reviews have included a margin of error to reflect changes from the prototype network to the physical network. In addition to completing a DRP (Disaster Recovery Plan) a comprehensive penetration test of the prototype network has been completed and the results are available for your review. The results of this test provide a view into the risks associated with the proposed network as well as mitigation techniques.

Technical Design

Internet services have been provided by Ground Control Satellite Solutions to accommodate the web and cross domain networking needs. Ground Control Satellite Solutions will function as the primary ISP, they have been contracted in order to provide reliable connections across the various sites. They specialize in satellite connected internet, meaning in the event of a natural disaster you will never lose connectivity at your site. In the event of loss of connectivity to a site Abercrombie Architectural Firm

must contact this ISP in order to have services restored, Elite Networking does not provide the means to restore such services. All sites have been interconnected with each other in order to provide reliable access to all features. The prototype network has proven resilient in the event of single or even multiple site failure (See Appendix C). In the event a single site were to lose connectivity all other sites will still maintain communications with each other, the proposed network which will differ from the prototype will prove even more resilient than the prototype in the event of loss of connectivity(See Appendix D). The proposed network will each have a connection directly to the internet, instead of a single connection through Spokane, Washington.

Several hardware and software items such as IDS, IPS, HIPS, and antivirus solutions have been added to the network to help provide several layers of security. These devices will provide information to the company's network security team in the event of an attack or for basic network analysis. In addition to hardware and software solutions, policies have been enacted to provide additional security thus helping to ensure data integrity and availability.

Outside contractors have been leveraged to provide the client with cloud services, IAAS, SAAS, and PAAS. These contractors will provide the client access to virtual systems across the internet such as virtual desktops, software, data storage, and database management. This will allow Abercrombie Architectural Firm to access from anywhere, important data and services, this gives the client incredible flexibility when on travel, working from a remote location like the site of project, and when sharing ideas and information with others across the company.

Network Architecture

Your new network will be accommodated according to the RFP, including Windows clients and servers, and Linux clients and servers. Cross domain connectivity has been provided and intranetworking speeds are established at no less than 100Mbps. The IP schema for the network has been constructed in

such a way as to provide services for the current number or requested devices and has the ability to expand and upgrade the network as needed. All hardware will have secured protocols, ports and firewall rules to allow authorized traffic in your network. A WSUS server will be implemented to keep all of your clients updated while maintaining good network performance. The network would be set to allow all external servers and websites accessible to your clients by placing them in a DMZ so there will be protection to your intranet. As mentioned an IDS will be placed behind the firewall to monitor traffic in and out of your network. We have also place a web filter, to insure you have the maximum control over your employees internet usage, it will also allow spam, malware, spyware and virus protection. Not only will we develop a network that meets or exceeds your operational needs but one will be developed that provides security and peace of mind.

General Configuration

Each site will include service provided by Windows Server 2012 or Fedora, depending upon the requirements of the specific site. These sites are being equipped with 8 physical servers each. 7 of these physical servers will host their own services: Directory, email, log, database, web, application, and a backup domain controller. 1 physical server per site will host two virtual servers, one being print services and the other being file services, and this will minimize the need for additional hardware while still keeping the two services separate. The virtual systems sharing a physical server have been chosen based upon function, bandwidth, and system resources required for operation, thus ensuring peak performance across the intranet. The servers with a dedicated physical server were chosen because of their need for system resources, the impact to the network in the event of hardware failure, and the security risks of having certain services coupled together. The servers will be configured with the following services:

Table 1: Basic Network Services

Virtualization Y/N	# of Virtual Servers	Service 1	Service 2
N	0	Log	
N	0	Database	
N	0	Web Hosting	
Y	2	Print	File Share
N	0	Domain Controller	
N	0	Application	
N	0	Email	
N	0	Backup Domain Controller	

The sites have all been planned with routers and layer 2 switches, these devices will be configured with VLAN (Virtual Local Area Network), this feature is setup in such a way as to prevent users from accessing information stored within various departments to which they are not assigned. Also included to facilitate security will be IDS and IPS (Intrusion Detection System and Intrusion Prevention System). Respectively these will provide data to the log server and prevent attacks or block malicious traffic (See Appendix E). IDS will be placed in front of the DMZ in order to track attacks attempting to come into the network even if they are not successful, this will give the IA team a detailed information of the type of attack the company receives on a daily basis and a manner with which to proactively block future attacks. The IPS will be configured inside the DMZ in order to block network traffic deemed malicious. The network has also been configured with access via VPN giving secure access to those working remotely and giving administrators a means to isolate areas of the network, in the event public access or WiFi is provided.

Sites

Each site will adhere to the standard network architecture mentioned in the proposal as well as the general configuration. These sites will however be customized based on the specifications mentioned in the RFP. Spokane will be upgraded to Windows Server 2012 Standard and the clients will be upgraded to Windows 8.1. Being newer operating system they will continue to be supported by the vendor Microsoft for several more years in the future. Windows 8.1 will also provide greater protection against threats than earlier Windows versions and will have the capability to run newer more secure software than its predecessors. Servers in Virginia Beach, Buenos Aires and select servers and clients in San Diego will follow suit with these operating systems and versions. Fedora 22 will be installed on servers at Leeds as well as select servers and clients in San Diego. Fedora 22 is the latest release for this Linux build.

As mentioned the infrastructure will match the specifications in the general configuration. Each site will be equipped with web services positioned outside the DMZ along with and IPS for logging traffic attempting to access the network and traffic leaving the network. Behand the DMZ will be positioned an IPS meant to block traffic deemed malicious, by the administrators. Also behind the DMZ is located the primary and backup domain controllers, email, print, database, file, application, and log servers. To save resources, maximize efficiency, and reduce overall maintenance costs print and file services will be installed on virtual servers, located on the same physical server. All network equipment, servers, DMZ, IPS, IDS, will copy their log periodically to the log server. Administrators will be able to utilize this log server to as a means to track anomalies and unauthorized activities, in addition to assure integrity of the information originally recorded by said devices. The network layout is designed to provide adequate network in addition to proper enterprise hardware security (See Appendix E)

Active Directory

Active Directory will be implemented on all sites running Microsoft Windows Server 2012. Active Directory will house all objects on the network; Printers, plotters, users, computers, servers. Each site will have a separate domain established within the same forest. The forest itself will function as the entire network and the domain will separate each site. This will provide greater functionality and relative ease of management.

Domains

A forest has been created for the network and within the forest a domain has been created for each site. Each site will house its own server hosting its domain. It will also be provided with a backup server in the event of failure of the primary. Each domain will house accounts for the users located at each site, as well as all clients, printers, groups, and distributions lists. Each domain will provide the other domains access to its resources and data. This will provide the users within the network the ability to easily communicate and share files, thus giving departments a way to easily manage their resources. Groups will be established to give the administrators the ability to establish role and rule based access across their domain. Distribution lists have also been created to facilitate communications among users.

Security

Detailed security plan (See Attached: Security Policies).

Hardware

Several forms of hardware based security has been implemented to ensure proper operation of the network:

- IDS – An IDS has been placed outside the DMZ. IDS was chosen to provide record of all traffic entering and exiting the network. This device will record it the traffic even in the event said traffic was blocked by a firewall, antivirus, or router.

- IPS – An IPS has been placed within the DMZ. The device can have parameters set that will allow administration to block any traffic they deem to be malicious or that can generate risk. The IPS was placed within the DMZ to block unsafe traffic not caught by the router or firewall.
- ASA – An ASA was installed on the network in front of the public facing router. This will allow administration to block traffic to the router and objects outside the DMZ deemed risky.
- Firewall – The firewall was placed on the backend of the router, allowing the DMZ to function separately from the internal network.
- VLAN – Separate VLAN were established on each switch, one for each department. This will help to ensure the integrity of a departments files by limited access to users who have no role allowing them to access another departments files.
- ACL – The router has been configured with a comprehensive ACL (Access Control List). The list limits access to and from certain IP addresses. The ACL was configured to allow PC's access to departments, services, and/or information deemed necessary by administration.

Software

Each PC, and server (Including virtual Server) will have Norton Antivirus installed. Norton will be provided initially by Elite Networking but a subscription will be required to renew services in the future, this subscription will be provided by the vendor.

Policies

Group policies have been established across the network. These will ensure limited access to certain features within the operating systems as well as limited access across the network. Users will be required to change their password periodically and those passwords must adhere to complexity requirements. Users will be prevented from accessing tools such as RegEdit, UNC, Remote Desktop, and system files.

Administrators will be required to obtain two accounts, one administrator and one user. Administrator rights will be limited to administrator accounts furthermore, administrator accounts will be prohibited from typical user access. Administrator accounts will be prohibited from accessing the internet and from sending/receiving email. This will be done in order to prevent malware from using administrator rights to execute.

Schedule

We have organized our teams so that the project should be completed in an estimated 54 days (See Attached: Project Schedule). The tasks performed will include backing up Spokane, upgrading the site then performing a retrieval of all backup information. Each site will be built at the same time as the others. This is possible by establishing team leaders at each site that will oversee work being conducted in their specialized area. Each site will have a network and server team, and a contractor hired to deliver and install the clients. The team leaders will ensure their members complete their objectives within the allotted time, and will report to the project manager in the event resources to reallocate.

The work will be arranged as to provide optimal up time for existing employees. As the contractors begin installing hardware the server team will begin remotely installing software. This will be done through the use of the application server and will present minimal interruption of services to employees. Each site will be completed at differing times, this is based on varying need of clients at the different sites.

Network infrastructure and security devices will be the first tasks to be completed, once the security devices are in place we can begin connecting servers and clients to the internet. The ISP has been contacted and services will be provided at the time the network is ready to connect. Cloud services will also be available at this time, this will ensure employees will have a greater range of capabilities early in the project. While the servers are being brought online the contractors hired to install the client

hardware will begin rendering their services. After the domain controllers are established said contractor will connect these devices to the network and the server team will begin updating software.

Our testing and technical writing specialist will begin establishing a DRP, operational documentation, and performing penetrations tests (See attached: DRP). The penetration test will provide the network and server teams with a thorough analysis of network vulnerabilities, when completed these teams will begin closing these gaps.

Cost Analysis

After a thorough cost analysis t is estimated the project will reasonably cost $8,853,759.00. This price is broken down into two major categories materials, services, and labor. The cost is further separated by site (See attached: Cost Analysis). This number will alter depending upon you cloud computing needs. At the moment cloud services will be provided by Microsoft through the use of One Drive, and Office 365, and by Oracle data services. The price will change depending as you assess your ever changing needs. ISP will vary per site, the network will use a combination of Cox, Virgin, and Telecom. Materials make the bulk of the order with some sites exceeding some 500 clients. We have managed to keep labor at a minimum (See attached: Project Cost – Labor Estimate) by utilizing contractors to work in coordination with the rest of the team and properly utilizing a combination of application server to push software and GPO’s to configure the clients.

Reference List

Cox Communications. (Oct 10, 2015). Professional communication

Cisco. (Oct 15, 2015). Retrieved from http://www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/index.html-tab-Switches

Dell. (Oct 17, 2015). Retrieved from http://www.dell.com/us/business/p/servers

Microsoft. (Oct 20, 2015). Retrieved from http://www.microsoft.com/en-us/server-cloud/products/windows-server-2012-r2/

Telecom. (Oct 10, 2015). Professional communication

Virgin. (Oct12, 2015). Professional communication

Appendix A: Request for Proposal RFP-12-0017

Request for Proposal

REQUEST FOR PROPOSAL RFP-12-0017

Information Technology Infrastructure Expansion

I. BACKGROUND

a. History. The Abercrombie Architectural Firm (AAF) is a privately owned company, which was incorporated in 2005. The main office is in Spokane Washington and has 2,700 employees. This site is currently running Windows 2000 Advanced Server and a mixture of client operating systems. AAF's business has increased dramatically over the past two years and the company will be expanding to four more locations and hiring additional employees for these sites during the next year. The four sites and the number of employees to be hired for these sites are

i. Leeds, England (1,200 employees)

ii. Buenos Aires, Argentina (540 employees)

iii. Virginia Beach, Virginia (2,100 employees)

iv. San Diego, California (1,435 employees)

b. General Site Requirements. These sites will be using a combination of operating systems, based upon their local needs (see specifications in section III below). The sites are also to be networked (see specifications in section V below). The sites will require new computer and networking hardware (see specifications in sections IV and V below). The sites should leverage important networking and system resources through virtualization, cloud, and storage technologies including SAAS, IAAS, and PAAS, as appropriate. The sites will deploy information assurance (IA) and network security in accordance with industry standard practices

c. General RFP Requirements. To setup these four new sites, this request for proposal includes:

i. Providing all computer and networking hardware and software

ii. Performing the integration and installation of these components

iii. Providing documentation for operations, including security, and disaster recovery

II. DELIVERY REQUIREMENTS
All hardware and software are to be shipped to the appropriate AAF site, with costs being F.O.B.

III. COMPUTER SOFTWARE REQUIREMENTS

a. General. All software licenses are to be provided as part of the final delivery of specified software, along with one set of documentation for each software item per site.

b. Operating Systems. The following operating system software will be provided for each site:

i. Leeds, England - Linux Servers and Clients

ii. Buenos Aires, Argentina - Windows Server w/ Windows clients

iii. Virginia Beach, Virginia - Windows Server w/ Windows clients

iv. San Diego, California - Linux Servers w/ Linux Clients and Windows Clients

c. Application Software. The following applications software will be provided for each site: (All software should be appropriate to that site's OS requirements.)

CAD Program

Office Productivity Software

E-mail Services/Clients

Web Services

Database Services

IV. COMPUTER HARDWARE REQUIREMENTS

a. General. All maintenance agreements are to be provided as part of the final delivery of specified hardware, along with one set of documentation for each hardware item per site.

b. Site Requirements. The following computer hardware will be provided:

i. Each site will have the following servers/services available:

General File Servers

CAD

Mail

Web

Database

ii. Leeds, England

1000 Workstations

Three High-End Plotters

Five Color Printers

10 Laser Printers

iii. Buenos Aires, Argentina

500 Workstations

One High-End Plotter

Two Color Printers

Five Laser Printers

iv. Virginia Beach, Virginia

2000 Workstations

Five High-End Plotters

Five Color Printers

20 Laser Printers

v. San Diego, California

1400 Workstations

Three High-End Plotters

Five Color Printers

10 Laser Printers

V. NETWORK REQUIREMENTS
All software licenses are to be provided as part of the final delivery of any provided network software, along with one set of documentation for each network item per site.

a. Site Intranetworking Requirements. All sites should be configured with a high-speed reliable network with the ability to be readily expanded/upgraded. The network should provide at least 100Mbps workstation speeds and appropriate backbone speeds. Other requirements as follows:

i. Leeds, England - Six story building w/ approximately 20,000 square feet per floor

ii. Buenos Aires, Argentina - Three story building w/ approximately 15,000 square feet per floor

iii. Virginia Beach, Virginia - Two neighboring buildings, five story buildings w/ approximately 25,000 square feet per floor

iv. San Diego, California - Four story building w/ approximately 30,000 square feet per floor

b. Company Internetworking Requirements. The contractor will provide for secure internetworking between the five (5) AAF sites, so that company proprietary data can be safely and confidentially shared among the sites.

VI. PROPOSAL SUBMISSION

a. Date, Time, and Place of Proposal Submission. The response to this RFP shall be delivered NLT 5:30pm on 5 Dec 2012 to the following address:

Abercrombie Architectural Firm, Inc.

Room 422

ATTN: Milton Abercrombie

b. Proposal Format:

i. Two (2) bound hardcopies of the written proposal shall be provided, and shall be organized into the following sections:

Technical Design – all network drawings shall also be provided electronically in Visio format

Installation/Integration Schedule – all project schedules shall also be provided electronically in Microsoft Project format

Cost Data – cost data for each proposed hardware and software item shall also be provided electronically in a Microsoft Access

ii. An executive-level website shall be developed by the contractor providing access to the proposal. This website shall be available for viewing by other AAF evaluation officials for one (1) week after the close of this solicitation.

iii. A prototype network shall also be provided by the bidder. This prototype shall demonstrate an implementation of all technologies described within the proposed solution and will be subject to an evaluation by a panel composed of members of the IT department of AAF.

Last modified: Monday, November 26, 2012, 7:21 PM

Appendix B: Request for Proposal RFP-12-0017 – Addendum

RFP Addendum

REQUEST FOR PROPOSAL RFP-12-0017 – Addendum

Information Technology Infrastructure Expansion

I. UPGRADE OF HOME OFFICE

The main office in Spokane Washington has 2,700 employees. This site is currently running Windows 2000 Advanced Server and a mixture of client operating systems. This site will be upgraded to be compatible with the additional sites being added in the original RFP-12-0017.

II. COMPUTER REQUIREMENTS

a. Operating Systems. The following operating system software will be provided for the site - Windows Servers and Clients

b. Servers/Hardware. The site currently has the following available:

1. Servers/services:

General File Servers

CAD

Mail

Web

Database

2. Hardware:

2500 Workstations

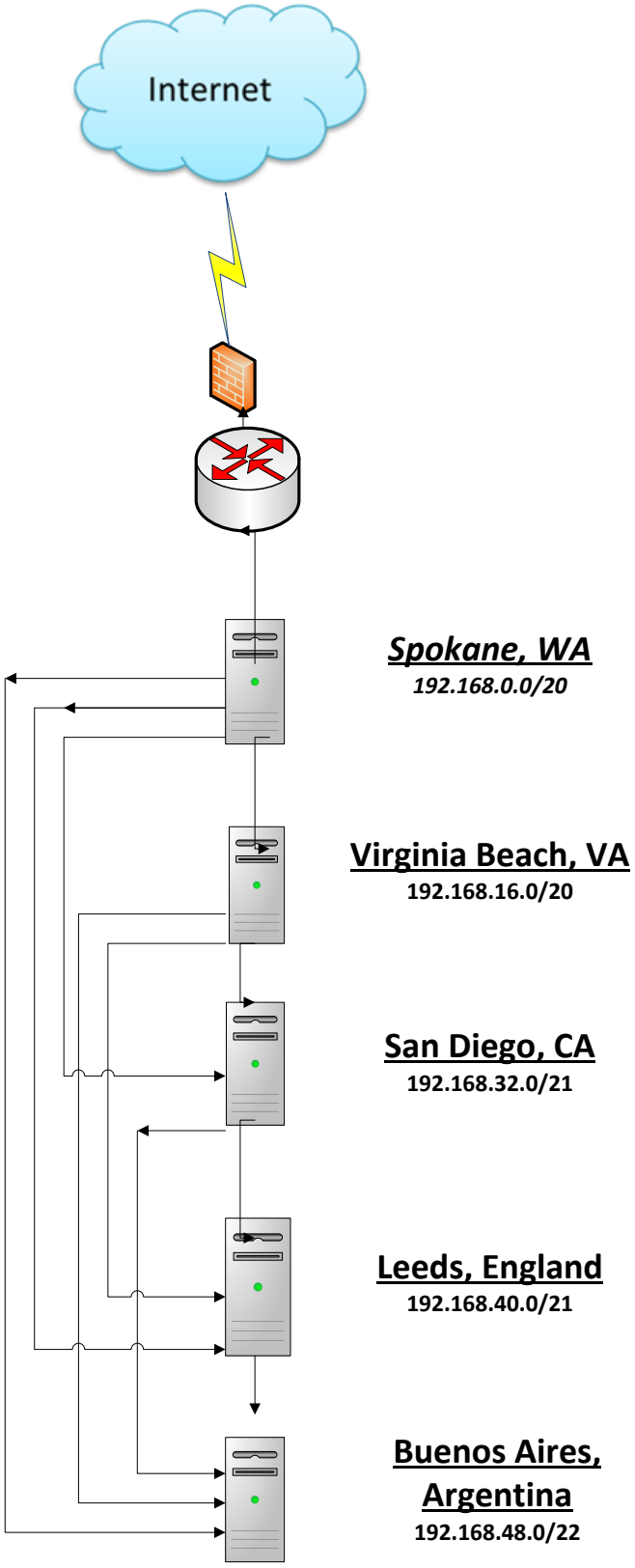
Ten High-End Plotters

Twenty-five Color Printers

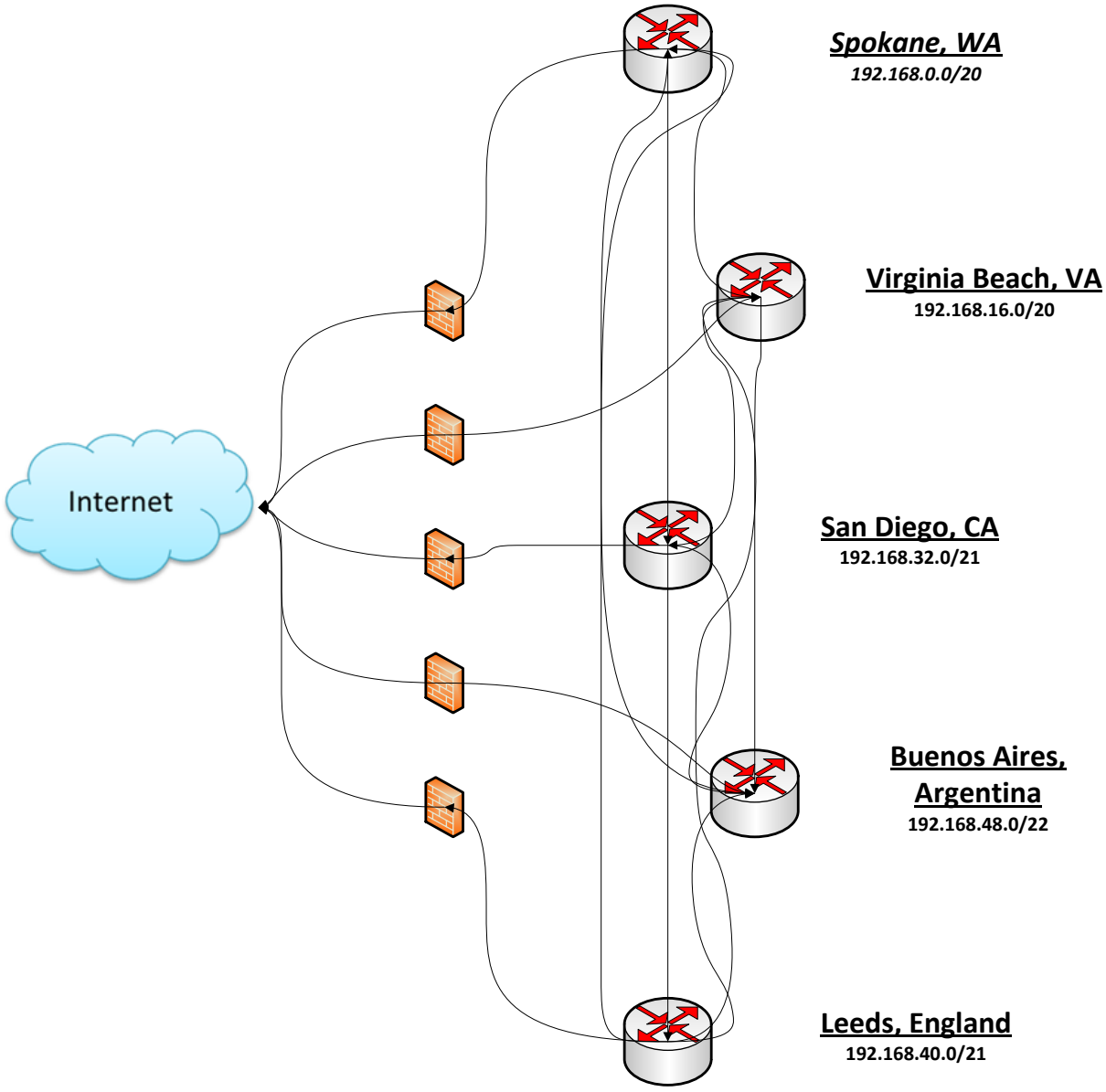
Thirty Laser Printers

Last modified: Monday, November 26, 2012, 7:22 PM

Appendix C: Prototype Network Diagram



Appendix D: Proposed Network Diagram



Appendix E: Detailed Network Diagram