

Final Project: Scenario 3

Caroline Artz & Ina Drew

Northwestern University

Table of Contents

Network Legend.....3

Local Area Network.....4

Wide Area Network.....5

Capacity & Future Growth Plan.....6

Security8

Business Environment & Threat Assessment..... 8

Planning 9

Protecting..... 11

Responding 11

Integrated LAN & WAN Diagram12

Budget.....13

Recommendations.....13

Staffing 13

Redundancy 14

Remote Users, VPN & Security 14

Spare Equipment..... 14

References15

Tables.....16

Final Project: Scenario 3

Scenario 3 charged us with configuring LANs for ABC Consulting’s two new locations in Atlanta and Cleveland. The Cleveland site must accommodate 38 users while the larger Atlanta site must maintain an initial 50 person staff while also preparing to scale up to 70 employees. To accomplish our task, we were given a budget of \$288,000.

Network Legend

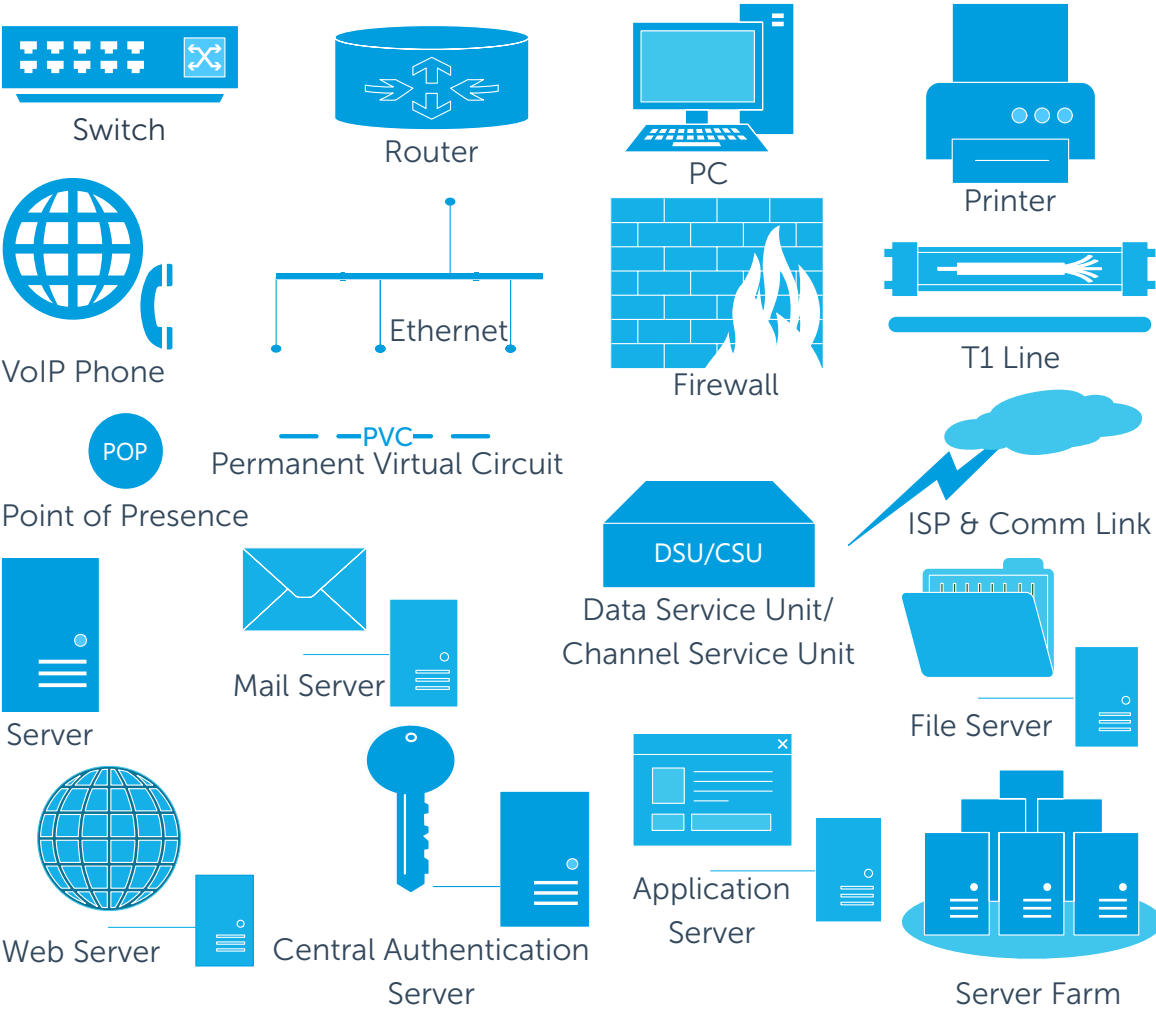


Figure 1. Network Legend. See Appendix A for legend in table format.

Local Area Network

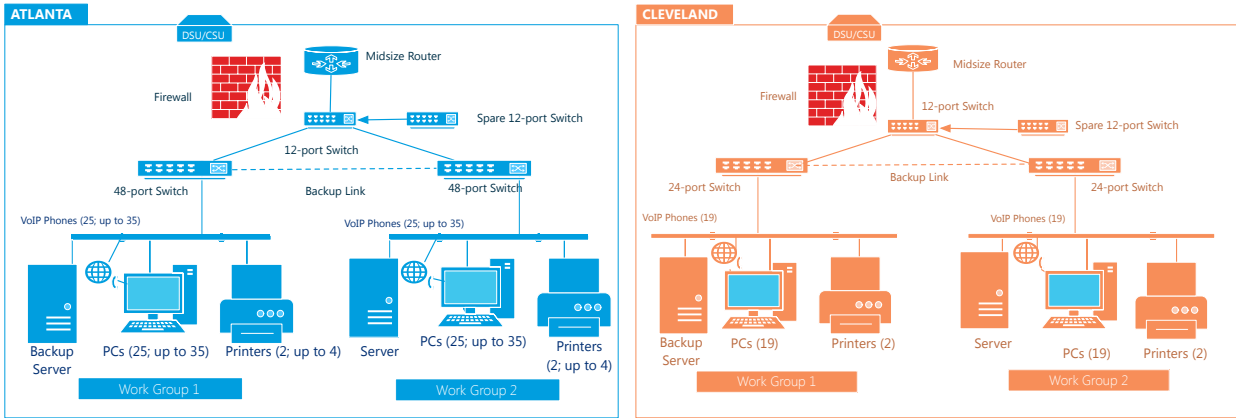


Figure 2. Local Area Networks (LAN). See Appendix B for larger diagram.

For ABC Consulting’s expansion we designed a switched Ethernet local area network (LAN; Appendix B) at the new site locations in Atlanta and Cleveland. Our configuration for both is hierarchical and includes logical bus topology. We opted for a switched Ethernet environment without the integration of hubs so that users have the maximum use of bandwidth. For both locations, each host is connected via standard 4-pair UTP Ethernet cable. We deployed optical fiber cords with 2 Gbps of trunk capacity connecting the 1000BASE-SX switches. We ensure that each host has a dedicated port in order to optimize speed.

Building for availability and high performance, both new sites have at least four switches and one router at the border of the network. To ensure access to the server in the event of failure at one of the workgroup switches, we installed a backup link connecting the two 48-port switches at Atlanta and two 24-port switches at Cleveland. This link is disabled by default to avoid network loops but automatically activates in the event of a failure at an adjacent primary switch under the Spanning Tree Protocol/Rapid Spanning Tree Protocol (STP/RSTP). Implementing

this design and protocol adds redundancy and effectively enhances network reliability at our new sites (R. R. Panko & Panko, 2013).

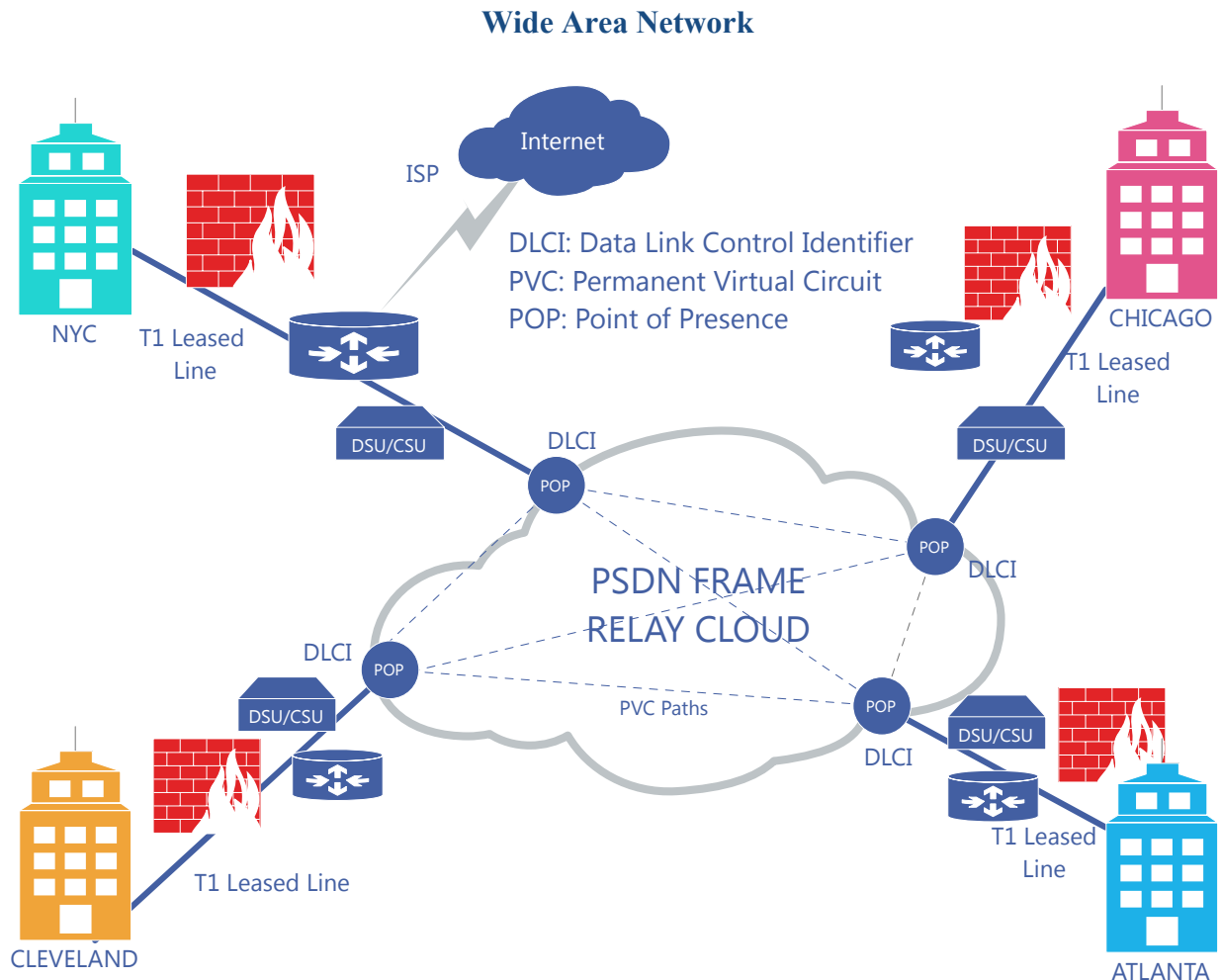


Figure 3. Wide Area Network (WAN). See Appendix C for larger diagram.

Our wide area network (WAN; Appendix C) connects via T1 leased line access to a Frame Relay public switched data network (PSDN) cloud with Internet available through WAN access to the New York ISP. Frame Relay is standardized for WAN technology that specifies the logical link layers of digital telecommunications channels using packet switched network methodology. This development in public switched network technology offers higher performance and greater transmission efficiency than the original PSDN standard, X.25. An

advantage of a public switched network is that customers save money by avoiding the cost of laying out and/or maintaining a resource-heavy network relying on site-to-site physical leased line connectivity (R. R. Panko & Panko, 2013). To aid network management ABC plans to procure Internet and Frame Relay services from the same telecommunications company.

Each of our locations has a border router and one leased T1 line serving as the access link to then WAN network core. The private T1 leased line transmits over 2-Pair Data-Grade UTP and run a physical connection from each site location to their nearest PSDN point-of-presence (POP). Our Frame Relay network core transmits data between the sites' POPs via pre-specified permanent virtual circuits (PVCs). The PVCs provide bi-directional communication paths between data terminating devices across all four sites and are uniquely identified by a Data Link Control Identifiers that also function to assign frames to the specified PVC. We opted for a full mesh configuration of PVCs between the POPs for added redundancy and therefore reducing the chances of network downtime during failures.

The use of PVCs eliminates the need for real time switching decisions dictating the frames' paths through the mesh PSDN core and results in reduced costs. This technique accommodates more flexibility and makes more efficient use of bandwidth (R. R. Panko & Panko, 2013). As a result, this type of technology poses an efficient, cost effective option that is likely to meet ABC Consulting's network requirements.

Capacity & Future Growth Plan

In light of this expansion and the desire and potential for additional future growth, extra hardware (one 12-port switch) has been allocated for Atlanta, which also serves as backup in the event of failure. With decided to include the same additional hardware at Cleveland with the primary purpose of backup.

With Frame Relay, network capacity concerns are important to consider, especially in light of inevitable increase in bandwidth needs over time. The Frame Relay techniques such as variable length packets and statistical multiplexing that allow for many of the advantages of Frame Relay (e.g., low cost and ability to use any unused bandwidth) are possible, in part, due to the PSDN sharing between a provider's customers. Consequently, this results in concerns around slow speeds and packet loss due to an overly congested network and ensuring quality of service. ABC Consulting's service provider guarantees them a portion of bandwidth when they negotiate their Committed Information Rate (CIR) and Committed Burst Size (Bc; greatest amount of consecutive bits they will carry without discarding), but traffic in excess becomes at risk for being discarded. To address congestion in Frame Relay Forward Explicit Congestion Notifications (FECN) and Backward Explicit Congestion Notifications (BECN) header bit messages function as requests to reduce the speed of traffic between sources (SearchNetworking, 2008).

It is important that ABC assess their network usage activities upon the expansion in order to appropriately adjust their CIR and Bc rates with their provider. Internet bandwidth is needed to support high-bandwidth business applications including VoIP calling and video conferencing. ABC will purchase Internet bandwidth from their ISP (also their Frame Relay provider), but not to the full capacity of their T1 Frame port since some of the PVCs only exist to provide branch-to-branch traffic (Cisco, n.d.).

To address QoS, it would be advantageous to enable Frame Relay Traffic Shaping on the virtual circuit interface and ultimately configure Resource Reservation Protocol (RSVP) Support for Frame Relay (Cisco, n.d.). Further, employing hardware load balancing devices (routers)

would also be helpful to optimize bandwidth, minimize downtime, facilitate traffic prioritization, and potentially add security (Caforio, n.d.).

One advantage of Frame Relay is that it is easily scalable. If additional bandwidth is needed from the ISP it can be procured at a cost. If ABC Consulting expands beyond this development, additional sites can be networked to the Frame Relay Cloud with relative ease via access lines to a nearby POP (R. R. Panko & Panko, 2013).

Security

ABC Consulting takes networking and data security very seriously making every effort to achieve comprehensive security. However, ABC must leverage risk analysis when budgeting for security needs. Based on characteristics of their operations ABC must select and prioritize types and levels of protection sufficient to protect their assets so that the total amount spent on security does not exceed that of the potential damage (R. R. Panko & Panko, 2013).

Keeping in mind that security measures will fail, even with the best planning, ABC strives to build successive layers of defense mechanisms so that a single break point does not result in full penetration of their network. With personnel expanding to locations across 4 states, factors such as access control are of particular importance to both the management of security operations and the protection against threats.

Business Environment & Threat Assessment

While some of ABC's six departments are located exclusively at the New York City headquarters branch (Finance and Business Development; See Table 1), most departments will have at least one representative on staff at each location. Members departments spread across locations (e.g., Management, IT, Human Resources) will regularly depend on network resources to communicate with colleagues (VoIP, email, WebEx). Departments that are localized (i.e.,

consulting divisions) still require reliable daily access to networked resources (e.g., WebEx, VoIP, Email needed for preliminary meetings with potential clients conducted and to conduct ongoing business with existing clients).

Data & assets. ABC Consulting must manage both client and company data. Considering each type of data within these two broad categories when assessing the threat environment and planning for network security is important. Relating to clients, assets include the proprietary business data they may provide during the course of rendered services as well as an encompassing client database with identifying details, historical records, and contractual information. On the internal side, assets include human resources databases storing sensitive personnel information. Business development and financial information is housed on a server at the NYC HQ. Company process and procedural information is also stored on a central server accessible by employees for training, ongoing development, and reference purposes.

ABC's business operations gives insight into the specific network requirements and resulting potential weak points for building a strong network security. Table 2 summarizes the processes and assets ABC must protect.

Planning

In an effort maintain our network security goals and reduce the risk of threats to the network, ABC will provision policies accompanied by implementation guidance such that all members of ABC Consulting are actively involved in the process. The central IT department will conduct mandatory virtual Security Lunch & Learn sessions out of the NYC HQ office. These periodic sessions will serve as a source of training (e.g., the importance of strong and complex passwords), implementation guidance, and an avenue for peers to provide support in how to maintain an acceptable balance of convenience and security. Further, IT management will

regularly schedule and execute oversight tasks including period audits, log file review, and vulnerability testing.

IT personnel will configure hardware and software to address security threats and end-point protection that includes enforcing reasonably strong password generation. A central authentication service housed on a server at the NYC HQ will provide directory service and credential management for networked applications. Workstations will be configured to automatically log users out after idling for more than 10 minutes with password authentication required to regain access. As email is an important form of communication for ABC, to protect against propagation vectors attacking through email attachments, spam-filtering and anti-virus software will be installed on the mail server. To provide layered protection, ABC will also install antivirus software such as Norton™ Protection Systems on all servers and user devices and set virus definitions to update automatically. ABC will ensure Service Pack II is installed on each computer for proactive protection against malicious code blocking exploits in addition to patching known vulnerabilities (Microsoft, n.d.). Branch IT personnel will periodically review all machines to make sure that they are fully updated.

While shared training resources are of a relatively less sensitive nature than other corporate assets and access requires less stringent forms of authentication, stricter access control is necessary for staff members and departmental management requiring access to sensitive data. Such requests will require rigorous authentication methods including digital certificate authentication for offsite personnel and access cards for onsite personnel who must pass the layers of physical security.

LAN Border stateful packet inspection firewalls provide ingress and egress filtering of all transmitted packets at each location. Connection seeking packets are compared against access

control list (ACL) rules and only allowed to connect when criteria are met. Connection requests deemed as potentially unsafe and known attack packets are dropped but logged for oversight review. An additional firewall module provides an extra layer of malware protection via web-content filtering to prevent users from accessing restricted, blacklisted or potentially malicious websites (R. R. Panko & Panko, 2013). Despite firewall protection, LAN servers must be backed up to protect against data loss in the event an attack does occur. ABC's plan includes backing up all data at 2:00 a.m. and restores the data at 4:00 a.m. daily. This process will ensure that user data is either stored on the server or copied across regularly prior to backups.

Protecting

ABC Company's Security Protection Plan (SPP) provides a unifying framework that integrates a range of efforts designed to enhance the safety of the complete infrastructure. The IT Network administrator will use strong encryption to encode data and prevent unauthorized parties from viewing or modifying any stored data. Further, all portable devices require encryption (i.e. smartphones, laptops, tablets) in order to access the company network and data. Encryptions will also prevent inappropriate access to networked documents and e-mail messages.

Responding

Our response to network intrusions involves strengthening our infrastructure and disrupting any immediate threat to the system. Our plan is to detect, stop, repair and punish violators according to ABC Policy (R. R. Panko & Panko, 2013). ABC has a one-hour response policy during office hours and otherwise three-hours for serious incidents such as virus infections. Should a threat come to fruition as an actual attack, ABC will first isolate the incidents or compromises to protect against any further damage. Second, we will enforce immediate password change based on the incident protocol as well as monitor and tighten all

entry points. We will handle internal violations according to our breach plan which includes the potential for termination based on the management’s discretion. We will prosecute external intruders according to state law respective to location.

Although no network is ever completely secure as long as there is access to the Internet, ABC will continue to improve upon their practices towards an increasingly robust security system by preventing, deterring, neutralizing, or mitigating the effects of incidents, compromises or natural disasters (R. R. Panko & Panko, 2013).

Integrated LAN & WAN Diagram

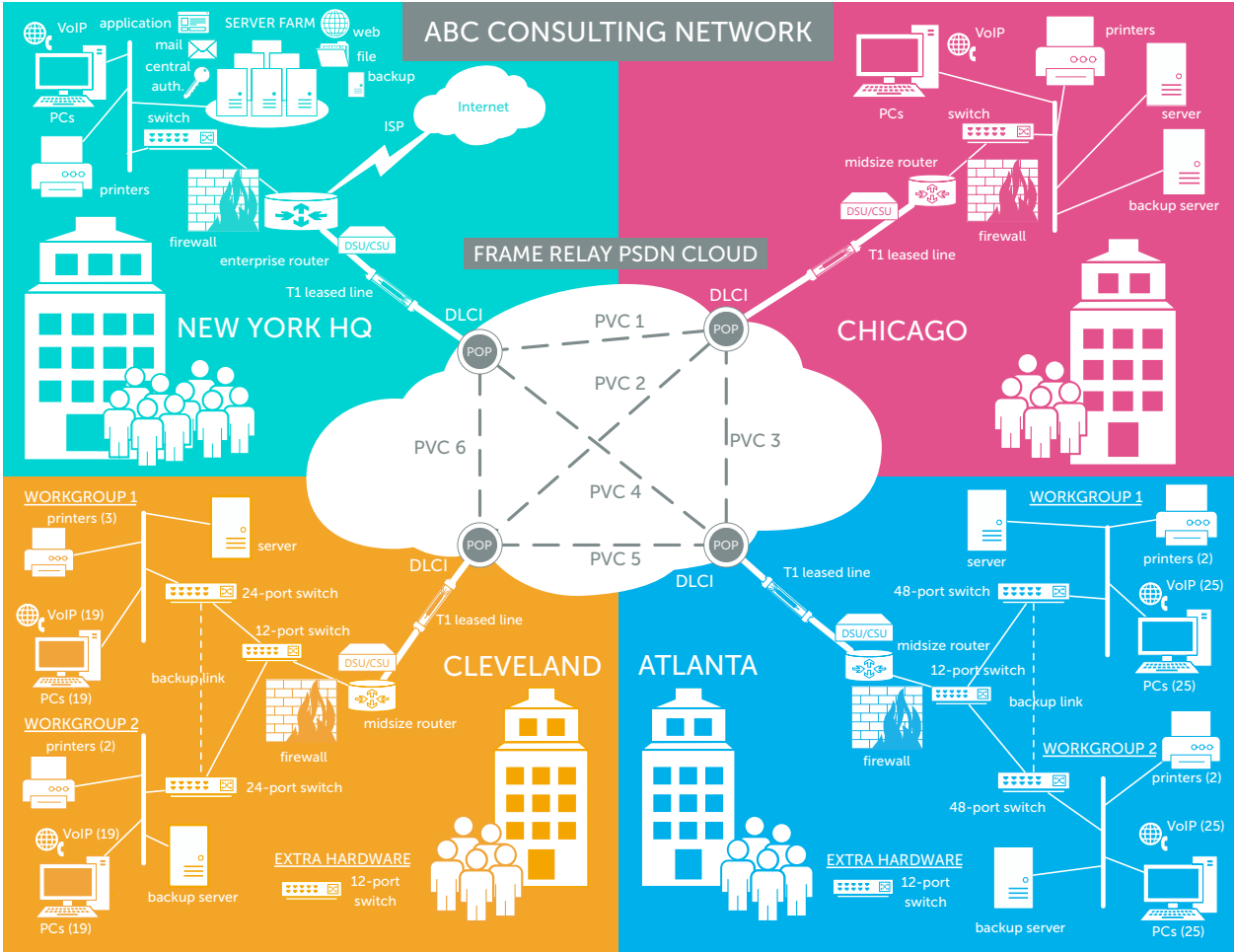


Figure 4. Integrated LAN & WAN Diagram. See Appendix D for larger diagram.

Budget

ABC Consulting Expansion Budget: \$288,000 Limit

ITEM	SCENARIO 3: BUDGET		
	AMOUNT	# NEEDED	TOTALS
Midsized Router	\$5,000.00	3	\$15,000.00
Enterprise Router	\$9,000.00	1	\$9,000.00
Switch (12-port)	\$1,000.00	4	\$4,000.00
Switch (24-port)	\$1,900.00	2	\$3,800.00
Switch (48-port)	\$2,900.00	2	\$5,800.00
Frame Relay Circuits (per PVC)	\$600.00	6	\$3,600.00
Server	\$5,500.00	4	\$22,000.00
Firewall	\$5,000.00	4	\$20,000.00
ISP Connection	\$700.00	1	\$700.00
LAN Cabling	\$38,000.00	2	\$76,000.00
PC Costs	\$500.00	88	\$44,000.00
Printer	\$100.00	9	\$900.00
TOTAL PROJECT			\$204,800.00

Figure 5. Budget. See Appendix E for excel file.

Recommendations

ABC’s expansion as outlined and supported over the course of this quarter more than accommodates a working network including security practices beyond basic needs. However, the significant amount of money under budget at project completion must be addressed. Our recommendations for additional hardware, staffing, and network components reflect this budgetary discrepancy with the excess funds migrating directly to projects implementing these enhancements.

Staffing

As part of the LAN and WAN initiative, ABC should allocate funds for hiring staff members at the Atlanta and Cleveland locations. We recommend staffing one mid-level network administrator and one PC level II technician for each location outside of the NYC HQ branch. These teams of network specialists would work together supporting hardware and software issues on-site. We hiring a Senior Network Engineer, Chief Information Officer and/or Chief Security Officer to maintain the IT department and work with other ABC departments on

management issues (e.g., implementing staff security training). All branch IT staff would report to the New York Senior IT department for all major network matters including asset procurement requests (CCNA, n.d.).

Redundancy

To add additional redundancy, we recommend an additional backup ISP link. We advise having the second ISP also at the NYC HQ location to reduce any management concerns. The NYC Firewall would require build-in multipath routing logic so that in the event of failover, the traffic would be routed to an alternate gateway.

Remote Users, VPN & Security

To address the glaring need for a virtual private network (VPN) enabling secure remote user access to the network for team members traveling and working remotely, we recommend upgrading all sites to Cisco ASA firewalls. In addition to VPN functionality, the Firewall would still provide the stateful packet inspection while also providing enhanced Intrusion Detection Services and many additional network-based security controls (Cisco, n.d.).

Spare Equipment

To supplement the spare hardware previously allocated to the 2 new sites (additional 12-port switches), we recommend all sites have spare configured routers to use in the event of failure. We would advise allocating additional switches two Atlanta if and when they acquire 20 additional staff members.

References

Caforio, J. R. (n.d.). What is hardware load-balancing device (HLD)? *SearchNetworking*.

Retrieved June 3, 2013, from <http://searchnetworking.techtarget.com/definition/hardware-load-balancing-device>

CCNA, N. (n.d.). Frame Relay. *NetCert CCNA*. Retrieved May 13, 2013, from

<http://netcert.tripod.com/ccna/wan/frelay.html>

Cisco. (n.d.). Frame Relay. *Cisco DocWiki*. Retrieved May 13, 2013, from

http://docwiki.cisco.com/wiki/Frame_Relay

Cisco. (n.d.). Part 5: Signalling - Signalling Overview. *Cisco*. Retrieved June 3, 2013, from

http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfsig.html#wp1004438

Cisco. (n.d.). Cisco ASA 5500 Series Firewall Solution Overview. *Cisco*. Retrieved June 3,

2013, from

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_brochure0900aecd8048dba8.html

Microsoft. (n.d.). Here's why SP2 is such an important update for WindowsXP. *Microsoft*

Technet. Retrieved May 26, 2013, from [http://technet.microsoft.com/en-](http://technet.microsoft.com/en-us/library/bb457009%28d=printer%29.aspx)

[us/library/bb457009%28d=printer%29.aspx](http://technet.microsoft.com/en-us/library/bb457009%28d=printer%29.aspx)

Panko, R. R., & Panko, J. L. (2013). *Business Data Networks & Security* (9 ed., pp. 1–560).

Upper Saddle River: Prentice Hall.

SearchNetworking. (2008). FECN/BECN. *SearchNetworking*. Retrieved June 4, 2013, from

<http://searchnetworking.techtarget.com/definition/FECN-BECN>

Tables

Table 1.
ABC Firm Organization Structure

ABC Consulting Firm




















Department	Location
Upper Management	Primarily at NYC HQ; Each location has 1 Branch Manager
Consulting Teams & Divisions	At all locations but divisions are generally not split across multiple locations
Business Development: Marketing, Sales, Research	NYC HQ
Finance	NYC HQ
IT	Primary location at NYC HQ; <i>See Recommendations section for our assessment of IT staff hiring and allocations.</i>
Human Resources	Primary location at NYC HQ; Each location has 1 HR Rep

Table 2.

ABC Asset Summary

Communication		Shared Resources	Data	
Corporate	Client		Corporate	Client
<ul style="list-style-type: none"> • WebEx • VoIP • Email 	<ul style="list-style-type: none"> • WebEx • VoIP • Email 	Procedural resources and information	<ul style="list-style-type: none"> • Human resources (personnel) • Business Development • Financial 	<ul style="list-style-type: none"> • ID, Records, Contractual info • Proprietary business data

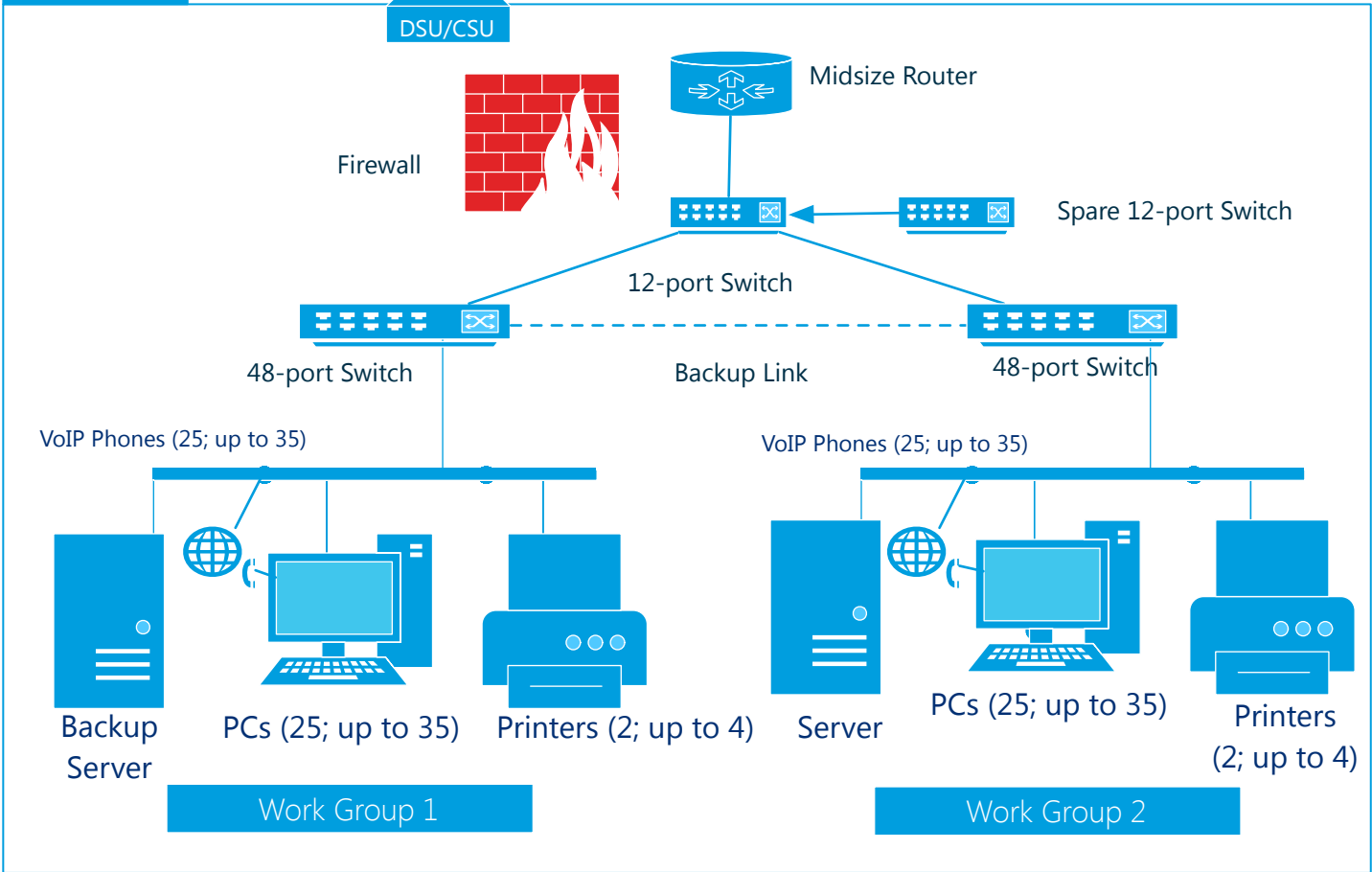
APPENDIX A: NETWORK LEGEND

SYMBOL	DESCRIPTION
	Switch
	Router
	Internet & ISP Comm Link
	PC
	Printer
	Firewall
	Ethernet
	Permanent Virtual Circuit
	T1 Leased Line
	VoIP Phone
	Data Service Unit/Channel Service Unit
	Point of Presence
	Server
	Server Farm
	Mail Server
	Web Server
	Application Server
	Central Authentication Server
	File Server

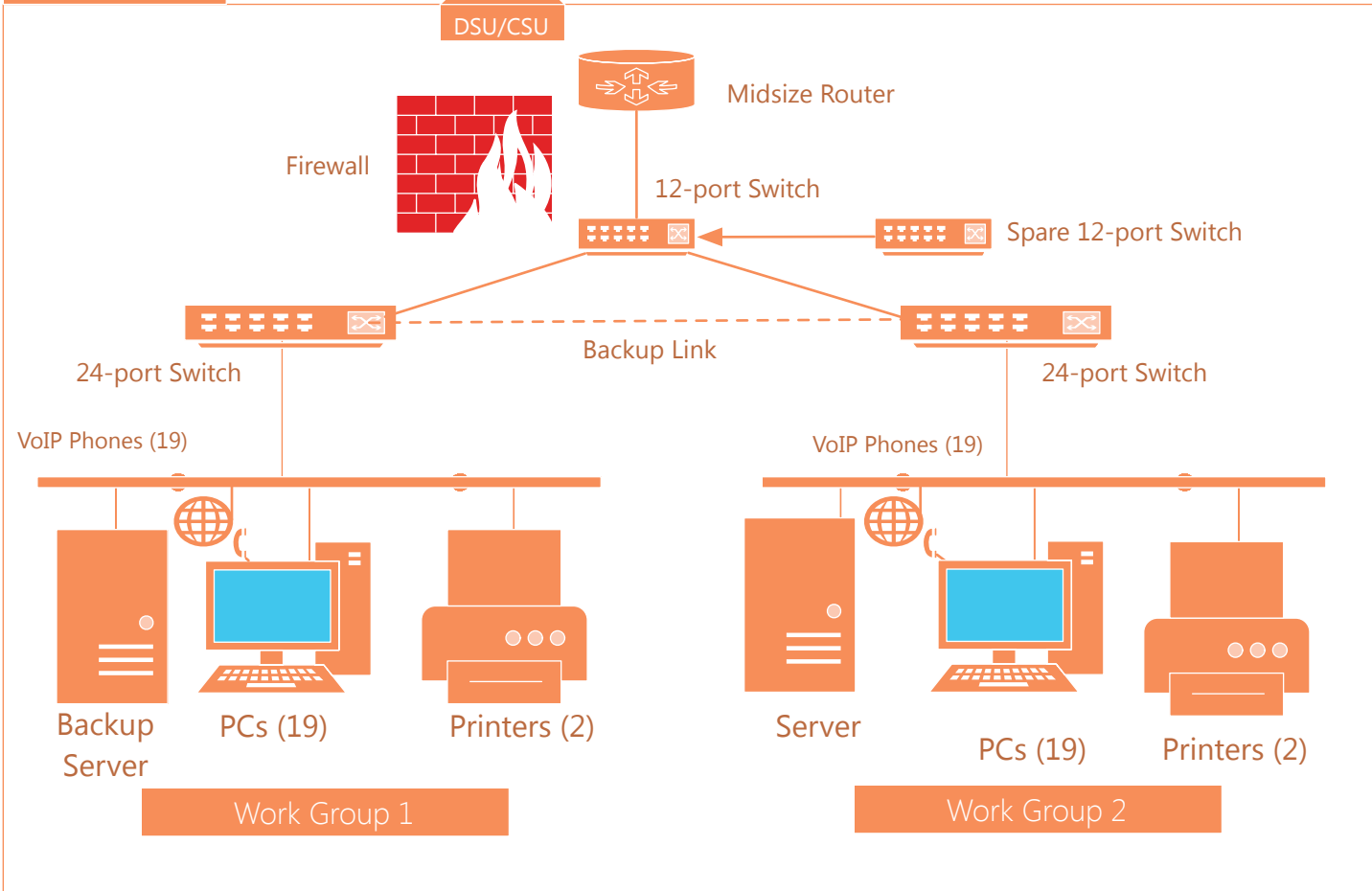
APPENDIX B: ABC CONSULTING SITES

LOCAL AREA NETWORKS (LAN)

ATLANTA

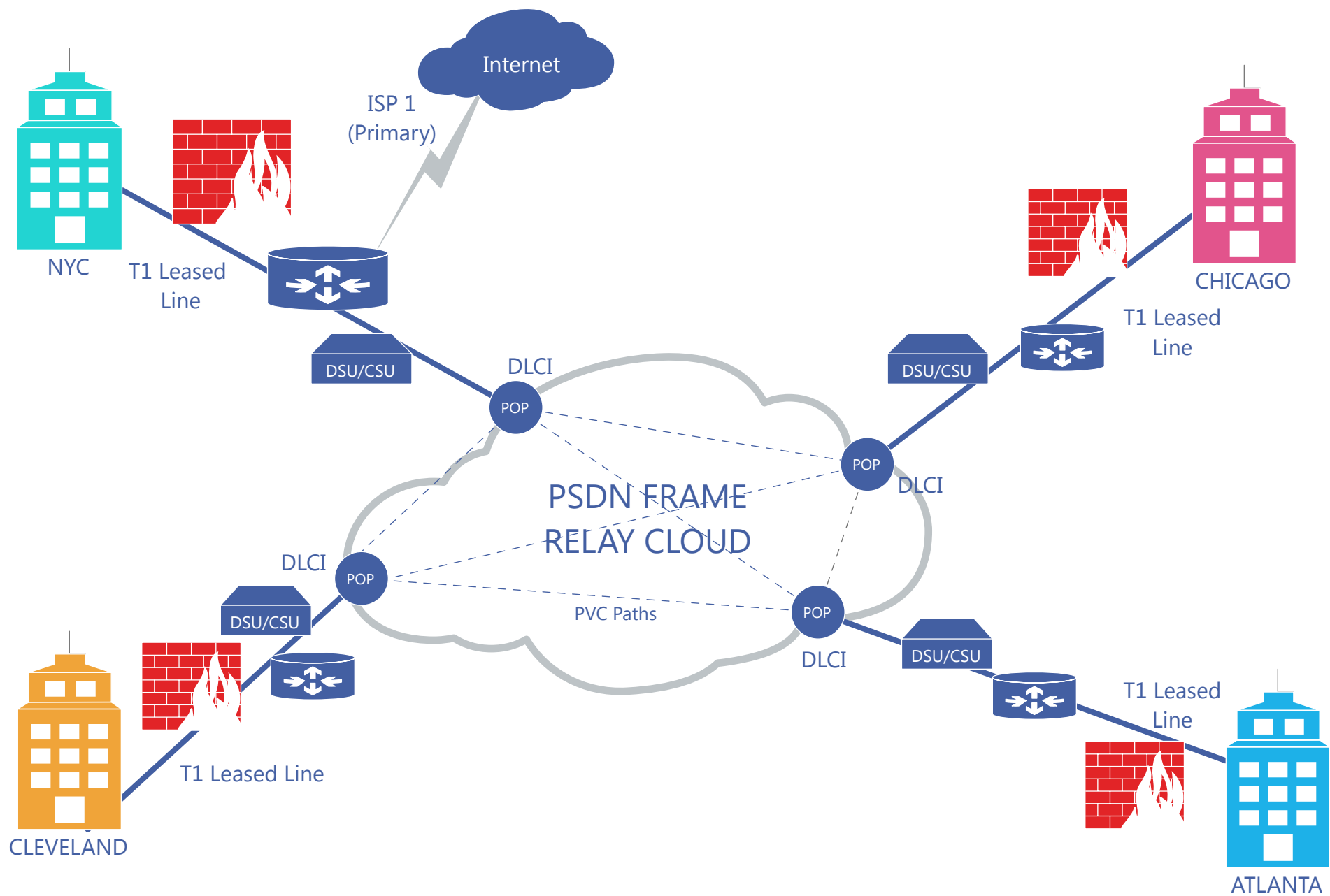


CLEVELAND



APPENDIX C: ABC CONSULTING WIDE AREA NETWORK (WAN)

DLCI: Data Link Control Identifier
PVC: Permanent Virtual Circuit
POP: Point of Presence



APPENDIX D: ABC CONSULTING NETWORK DIAGRAM

Artz & Drew, CIS 313, 2013

