Kerberos Consulting
March 5, 2008

243 S Wabash Ave
Chicago, IL 60604
Tel: (312) 968-4225
Fax: (312) 968-9225

Security and Network Design Proposal

PAUL RECOVERY AND TREATMENT CENTER

Prepared for: Paul Recovery and Treatment Center

Prepared By: Joseph Aguirre, Matthew Babich, Mike Dadouche, Gregori Jenkins, and Chris Robinson

Description: This is a proposal submission for the Paul Recovery and Treatment Center based in Beverly Hills, California. In this proposal is a comprehensive network and security design made by our nationally-known consultants . We are confident that our solution will meet PRTC's needs for today's and future growth.

Table of Contents

1. Executive Summary 10

2. WAN Design 11

2.1.Overview 11
2.2.Equipment 12
2.3.Configuration 12
2.4.Internet Connectivity 13
2.5.Security 17
2.6.Equipment Maintenance and replacement 18
2.7.Pricing 19

3. LAN Design 20

3.1. Infrastructure 20
3.1.1. Data Center Core Switching 20
3.1.1.1.Catalyst 6509E 20
3.1.1.1.1.Modules 20
3.1.1.1.2.Wiring 21
3.1.1.1.3.Warranty 22
3.1.1.1.4.Diagram 23
3.1.2. Closet Access Switching 23
3.1.2.1.Cisco 3750 23
3.1.2.1.1.Wiring 23
3.1.2.1.2.Warranty 25
3.1.2.1.3.Logical Core Switching Diagram 26
3.2.IP Addressing 26
3.2.1.VLANs 27
3.2.2.DHCP 28
3.2.3.Statically Addressed Devices 29
3.2.4.Network Equipment 30
3.3.Pricing 30
3.3.1. Overview 30
3.3.2.Pricing Matrix 30

4. Data Center 31

4.1.Overview 31
4.2.Technical Solutions 31
4.2.1.Servers 31
4.2.1.1.HP Proliant DL360 G5 31
4.2.1.1.1.Services Provided 31
4.2.1.1.1.1. Active Directory/DNS – PRTCDC01 &PRTCDC02 31
4.2.1.1.1.2. Exchange – PRTCEXCH01 & PRTCEXCH02 32
4.2.1.1.1.3. File and Print Services – PRTCFILE01 & PRTCFILE02 32
4.2.1.1.1.4. Vontu – PRTCVONTU01 32
4.2.1.1.1.5. GFILANGuard – PRTCESAFE01 33
4.2.1.2.HP Proliant DL380 G5 34
4.2.1.2.1.Services Provided 36
4.2.1.3.HP Proliant DL580 G5 36
4.2.1.3.1.Services Provided 36
4.2.1.4.Warranty for HP Servers 36
4.2.2. Server IP Addresses 36
4.2.3. Storage Solution 36
4.2.3.1. IBM SAN 37
4.2.3.1.1.Partitions 39
4.2.4. Server Network Connections 39
4.2.5. KVM 40
4.2.5.1.Raritan KX2-232 IP 40
4.2.5.2. Redundancy 40
4.2.5.3. Cables 40
4.2.5.4. Warranty 40
4.2.6. Racks 40
4.2.6.1. HP 10842 Wide Rack 40
4.2.7. UPS 41
4.2.7.1. APC Symmetra PX 40KW 41
4.3. Licensing 41
4.3.1. Operating System 41
4.3.1.1. Microsoft 41
4.3.2. SQL Server 42
4.3.2.1. Microsoft 42
4.3.3. Virtual Infrastructure 42
4.3.3.1. VMWare ESX Server 43
4.3.4. Client Access License 43
4.3.4.1.Microsoft 43

4.3.5.Email Server 43
4.3.5.1.Microsoft Exchange Server 43
4.4.Network Cabling 43
4.4.1.Fiber Runs 43
4.4.2.Cat5e UTP Runs 45
4.4.3.Cat6 UTP Runs 45
4.4.4.Patch Panel Wiring 45
4.4.5.Patch Cables 46
4.5.Cable Management 47
4.5.1.Ladder Rack System 47
4.6.Domain Names 48
4.7.Monitoring 48
4.7.1.Network 48
4.7.1.1.Microsoft Operations Manager 48
4.8.Diagrams 50
4.8.1.Data Center 50
4.8.1.1.Wiring 50
4.8.1.2.Cable Management 51
4.8.2.Data Center Racks 52
4.8.3.Floor Network Jack Locations 58
4.8.3.1. First Floor 58
4.8.3.2. Second Floor 59
4.8.3.3. Third Floor 60
4.8.4. IDF Closets 61
4.9. Doctor Access 64
4.9.1.Tablet PCs 64
4.9.2. Security 64
4.9.2.1. Encryption SafeBoot 64
4.9.2.2. Sticky MAC 64
4.10. Recommendations 66
4.10.1. Staffing 66
4.10.2. Training 66

5. IP Addressing 67

5.1.Overview 67
5.2.IP Address Matrices 67

6. Physical Security 69

6.1.Overview 69

6.2.Physical Security Concerns **69**
6.2.1.Perimeter Entry 69
6.3.Designated Access Area **70**
6.3.1. First Floor 70
6.3.2.Second Floor 71
6.3.3. Third Floor 71
6.4.Access Points **72**
6.4.1.First Floor 72
6.4.2.Second Floor 74
6.4.3. Third Floor 75
6.5.Access Level Rules **76**
6.5.1.Definition of Access Levels 77
6.5.1.1.Specific Rules on Access Levels 77
6.6.Equipment **79**
6.6.1. Hartman Controls 79
6.6.1.1. Door Proximity Access Control Panel 79
6.6.1.2.HCEC-8 Option 80
6.6.1.3.RF101 Keypad/Proximity Reader 80
6.6.1.4.RF10 Proximity Reader 81
6.6.1.5.RS485 to TCP/IP Converter 81
6.6.1.6.Badge Type Proximity Card 81
6.6.2. AlarmLock **82**
6.6.2.1.RRPM1200P AK Magnetic Lock with Remote Control 82
6.7.Training **82**
6.7.1.General 82
6.7.2.Trainer 83
6.7.3.Programmer 84
6.8.Pricing **84**
6.8.1.Overview 84
6.8.2.Pricing Matrix 84

7. Virtual Security **85**

7.1.Overview **85**
7.2.Anti- Virus, Spam, Spyware **85**
7.3.Network Authentication, Auditing, and Scanning **86**
7.3.1.Authentication 86
7.3.2.Auditing and Scanning 87
7.4.Data Loss Prevention **87**
7.5.Web Security **88**
7.6.Backup **89**

7.7.Recommended Utilities **90**
7.8.Cisco Secure ACS **91**
7.8.1.Overview 91
7.8.2.Equipment 91
7.8.3.Configuration 91
7.9.Cisco Secure MARS **92**
7.9.1.Overview 92
7.9.2.Equipment 93
7.9.3.Configuration 93
7.10.Equipment Maintenance and Replacement **94**
7.10.1.Software 94
7.10.2.Hardware **94**
7.11.Pricing **95**
7.12.Pricing (Part Two) **96**

8. Security Assessment **97**

8.1.Overview **97**
8.2.Current Approach of the Risk Assessment **97**
8.2.1.Technique in Gathering Information 97
8.3.System Characterization **98**
8.3.1.System-Related Information 98
8.3.2.Operational Environment 98
8.4.Threat Identification **99**
8.4.1.Physical Threats 102*
8.5.Vulnerability Identification **105**
8.6.Security Requirements **108**
8.6.1.Control Analysis 109
8.6.2.Control Methods 109
8.6.3.Likelihood Determinations 109
8.6.4.Impact Analysis 109
8.6.5.Magnitude of Impact Definitions 111
8.7.Risk Assessment **111**
8.8.Assets **120**

9. Security Policy **122**

9.1.Physical Access **122**
9.1.1.Overview 122
9.1.2.Scope 122
9.1.3.Policy 122

9.1.3.1.Employee Requirements 122
9.1.3.2.PRTC Required Action 122
9.1.3.3.Appropriate Measures for Physical Access 123
9.1.4. Enforcement 123
9.1.5.Definitions 123
9.2.**Data Access** 124
9.2.1.Overview 124
9.2.2.Scope 124
9.2.3.Policy 124
9.2.3.1.Employee Requirements 124
9.2.3.2. PRTC Required Action 124
9.2.3.3.Appropriate Measures for Data Access 124
9.2.3.4.Enforcement 125
9.2.3.5.Definitions 125
9.3.Data Retention 126
9.3.1.Overview 126
9.3.2.Scope 126
9.3.3.Policy 126
9.3.3.1.Employee Requirements 126
9.3.3.2.PRTC Required Action 126
9.3.3.3.Appropriate Measures for Sensitive Data 126
9.3.3.4.Appropriate Measures for Non-Sensitive Data 127
9.3.4.Enforcement 127
9.3.5.Definitions 127
9.4. Data Destruction 128
9.4.1.Overview 128
9.4.2.Scope 128
9.4.3.Policy 128
9.4.3.1.Employee Requirements 128
9.4.3.2.PRTC Required Action 128
9.4.3.3.Appropriate Measures for Sensitive Paper Documents 128
9.4.3.4.Appropriate Measures for Electronic Media 129
9.4.4.Enforcement 129
9.4.5.Definitions 130
9.5. **Network Appliance** 131
9.5.1.Overview 131
9.5.2.Scope 131
9.5.3.Policy 131
9.5.3.1.Employee Requirements 131
9.5.3.2.PRTC Required Action 131
9.5.3.3.Appropriate Measures for Network Appliances 131

9.5.4.Enforcement 132
9.5.5.Definitions 132
9.6. Workstations 133
9.6.1.Overview 133
9.6.2.Scope 133
9.6.3.Policy 133
9.6.3.1.Employee Requirements 133
9.6.3.2.PRTC Required Action 133
9.6.3.3.Appropriate Measures for Physical Access 133
9.6.4.Enforcement 134
9.6.5.Definitions 134
9.7. **Servers 135**
9.7.1.Overview 135
9.7.2.Scope 135
9.7.3.Policy 135
9.7.3.1.Employee Requirements 135
9.7.3.2.PRTC Required Action 135
9.7.3.3.Appropriate Measures for Servers 135
9.7.4.Enforcement 136
9.7.5.Definitions 136
9.8. Anti-Virus 137
9.8.1.Overview 137
9.8.2.Scope 137
9.8.3.Policy 137
9.8.3.1.Employee Requirements 137
9.8.3.2.PRTC Required Action 137
9.8.3.3.Appropriate Measures for Anti-Virus 137
9.8.4.Enforcement 138
9.8.5.Definitions 138
9.9. Acceptable Use 139
9.9.1.Overview 139
9.9.2.Scope 139
9.9.3.Policy 139
9.9.3.1.Employee Requirements 139
9.9.3.2.PRTC Required Action 139
9.9.3.3.Appropriate Measures for Acceptable Use 139
9.9.4.Enforcement 140
9.9.5.Definitions 140
9.10. Auditing 141
9.10.1.Overview 141
9.10.2.Scope 141

9.10.3.Policy 141
9.10.3.1.Employee Requirements 141
9.10.3.2.PRTC Required Action 141
9.10.3.3.Appropriate Measures for Auditing 141
9.10.4.Enforcement 142
9.10.5.Definitions 142
9.11.Awareness Training 143
9.11.1.Overview 143
9.11.2.Scope 143
9.11.3.Policy 143
9.11.3.1.Employee Requirements 143
9.11.3.2.PRTC Required Action 143
9.11.3.3.Appropriate Measures for Awareness Training 143
9.11.4.Enforcement 144
9.11.5.Definitions 144

10. Total Cost 145

10.1.Overview 145
10.2.Pricing Matrices 145

11. Implementation Plan 146

11.1.Overview 146
11.2.Implementation Matrices 146

12. Assumptions 154

1. Executive Summary

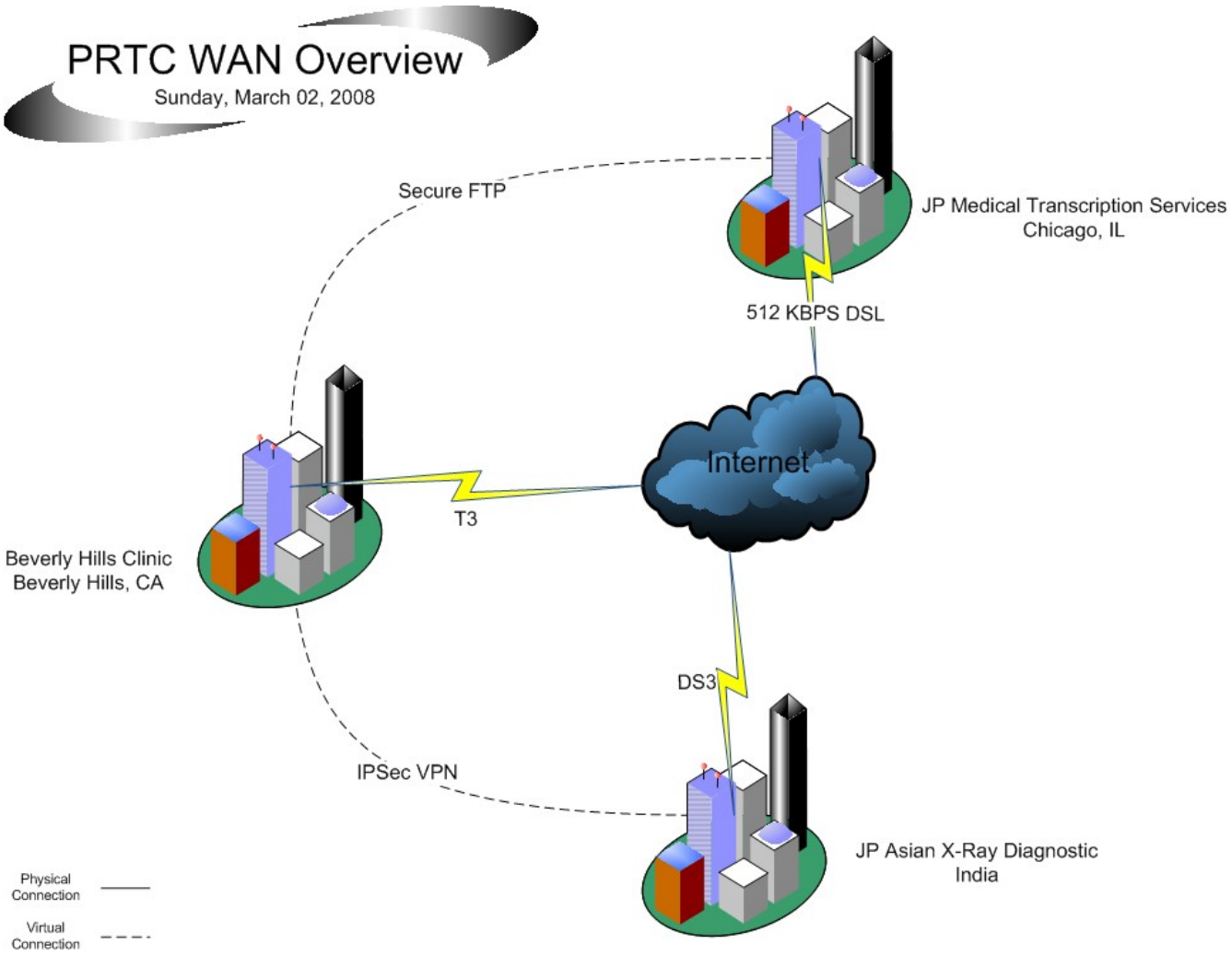
As a startup healthcare company, Paul Recovery and Treatment Center (PRTC), is presented with many challenges with deciding on a network and security infrastructure. Compliance and security are a necessity for companies in today's world that deal with patient records and data. If not given the appropriate attention, security breaches can cause a disruption of service or a compromise of information; each of which will ultimately cause a financial loss. Because PRTC is a new company, they have an excellent opportunity to choose a secure and compliant network solution that will provide a fully secure network infrastructure that will remain serviceable for years to come. We at Kerberos Consulting realize the threats that are out there and strive to bring each client a fully customized network and security infrastructure design based on their needs. We have prepared this design to be compliant and efficient for both the company and customers.

2. WAN Design

2.1. Overview

As a new startup clinic in Beverly Hills, Paul Recovery and Treatment Center (PRTC) has the opportunity to invest in a strong infrastructure that will support the company for years to come. PRTC has a number of demands that must be met that are directly involved with the Wide Area Network configuration (WAN): must connect to Internet, transfer large X-ray images to JP X-Ray Asian Diagnostic, and transfer of data to JP Medical Transcription Service. These are only a few of the practical demands placed on the network that are easily realized. The most important demand which is often taken for granted is that of security. It is this that will make or break the design put forth by Kerberos Consulting, and as a result, it has been well applied throughout the design of PRTC's network.

The heightened emphasis on security given the sensitive nature of clinic's position means that extreme consideration must be placed on the overall protection of PRTC. Constant attempts to harvest information about clients past and to come as well as numerous other threats demands that an active prevention scheme be in place. The WAN is essentially the front line of defense against most virtual threats. That being so, some very powerful security tools have been placed to defend against them.


PRTC WAN Overview
Sunday, March 02, 2008
Secure FTP
JP Medical Transcription Services
Chicago, IL
512 KBPS DSL
Internet
T3
Beverly Hills Clinic
Beverly Hills, CA
DS3
IPSec VPN
JP Asian X-Ray Diagnostic
India
Physical Connection
Virtual Connection

2.2.Equipment

The following is a list of equipment that will be ordered for PRTC:

First Line of Defense:

- Cisco 3845 Integrated Service Router Model# 3845 – x1
- Cisco Advanced Security for 3845 ISR Model# CD384-AISK9 – x1
- Certified Flash Memory 64 MB for 3800 ISR Model# MEM3800-64CF - x1
- Cisco 2811 Integrated Service Router Model# 2811 – x1
- Cisco Advanced Security for 2811 ISR Model# CD28N-ASK9 - x1
- Certified Flash Memory 64 MB for 2800 ISR Model# MEM2800-64CF - x1
- Cisco T3/E3 Network Module Model# NM-1T3/E3 - x2

Second Line Of Defense:

- Cisco Adaptive Security Appliance 5510 with SSM-AIP-10 Module
  Model# ASA5510-AIP10-K9 – x2

Main WAN Switch

- Cisco Catalyst Express Model# CE500GTC – x1

Backup Power
APC UPS Model# SUA2200 - x1

2.3.Configuration

The WAN configuration is optimized to handle large file transmissions at extremely fast rates. For this we have selected a T3 Internet connection and a ½ T3 connection as backup from JPTelco. PRTC's T3 connection will terminate at the primary router (3845 ISR). This will provide the main Internet connection for the company. A secondary ½ T3 line will go to the secondary router (2811 ISR) which will become the backup Internet connection. This will allow PRTC to failover to the secondary line should the primary Internet connection fail. After the first line of defense we have the Security Appliances which are the main points of threat mitigation.

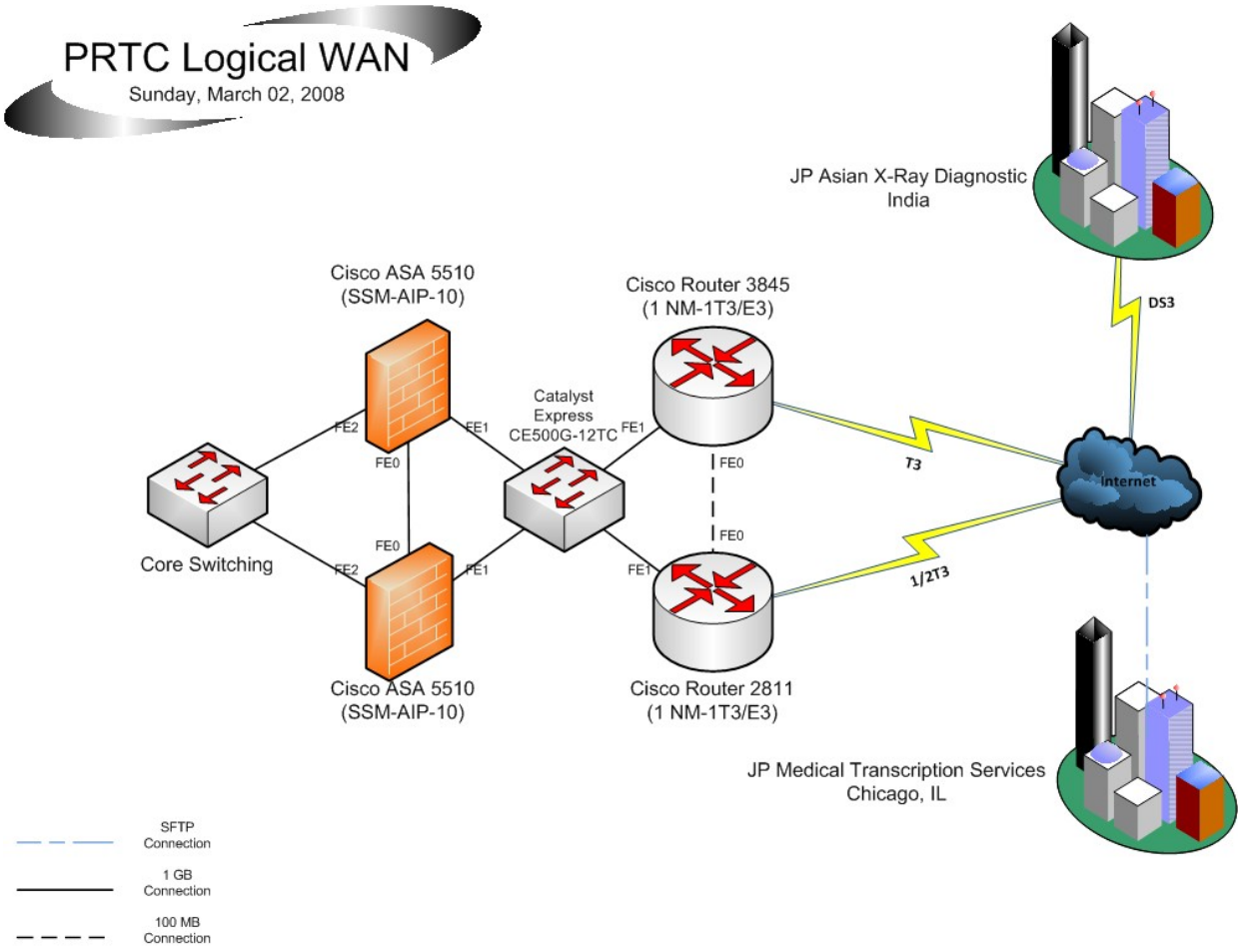
Both Adaptive Security Appliances (ASA) provide the second line of defense which makes up the bulk of defense against external and internal threats. The appliances' security configuration will be covered in the security subsection. As for physical Ethernet configuration, both Adaptive Security Appliances have a connection to the Catalyst Express switch for WAN device interconnectivity. That will allow connectivity to the routers. There is a physical Ethernet connection between two Adaptive Security Appliance to allow polling of status for the two devices. One

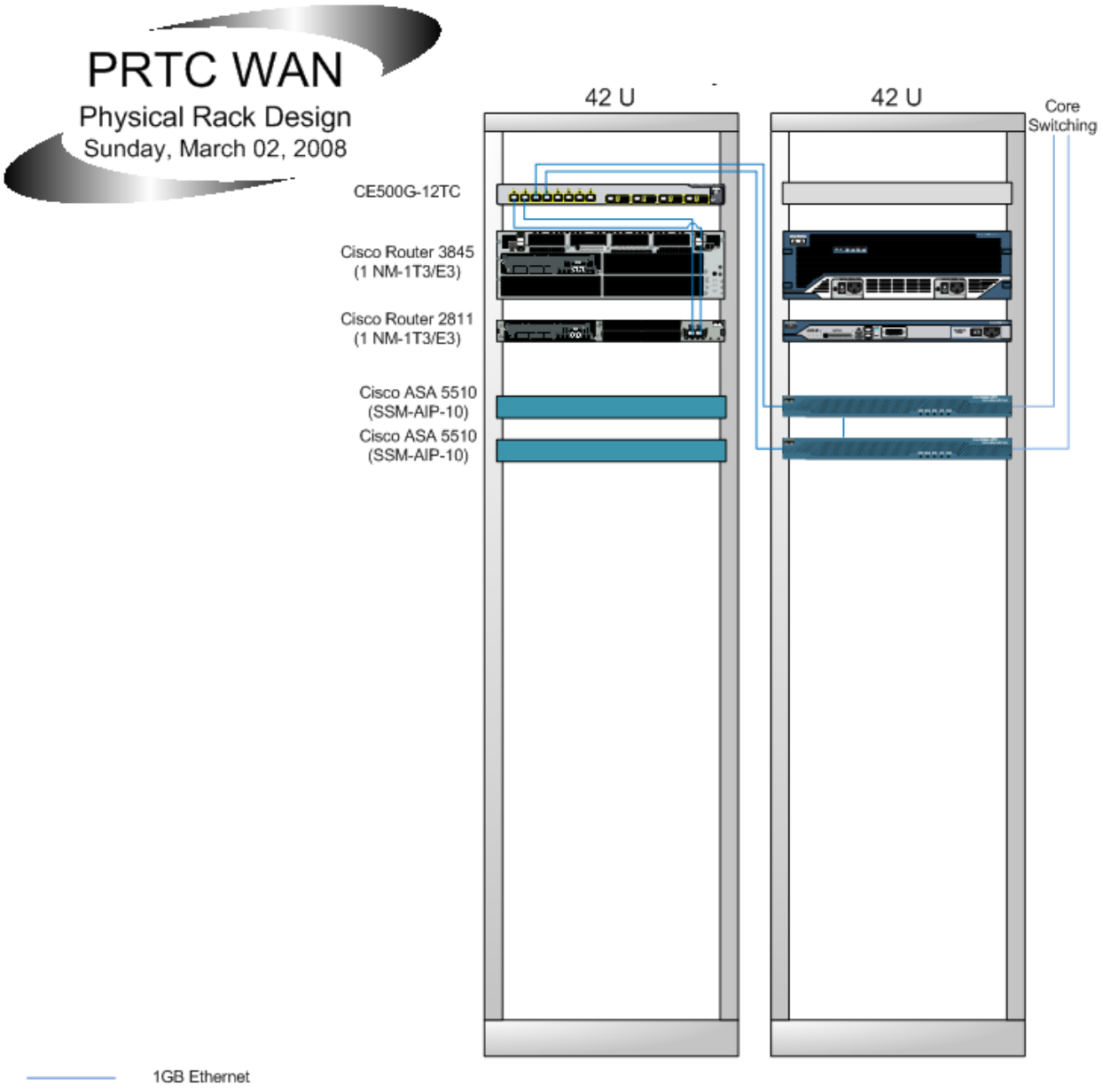
Adaptive Security Appliance will be active while the other is standby. This allows failover should one device fail. The third Ethernet connection goes to core switching.

2.4.Internet Connectivity

PRTC in is need of a substantial amount of bandwidth in order to transfer numerous files that are few in number but large in size. These files will typically be X-Rays of patients. Knowing that a doctor will need an analysis of these x-rays within a matter of minutes, a full T3 connection was selected to accommodate those results. It is possible to use a T3 connection to the Internet for this purpose as well as furnish an responsive Internet connection to internal computer users. This connection is terminated at the primary router Cisco 3845 IST which can handle such speeds.

For backup, we have selected a ½ T3 connection which will be terminated at the Cisco 2811 ISR. The purpose for this backup line is to allow a degraded Internet connection service in the even of a failure in T3 service to the main router. The ½ T3 will no be as responsive as the regular T3 connection but it will allow work to continue at an acceptable speed.
Using these connections data will be transferred to JP Asian X-Ray Diagnostic and JP Medical Transcription Service as well as provide Internet connectivity to internal users. The average user will use about 50 Kbps for email, web surfing, and other lightweight services like FTP. A T3 connection will be sufficient enough to accommodate these demands.


PRTC Logical WAN
Sunday, March 02, 2008
JP Asian X-Ray Diagnostic
India
DS3
Cisco ASA 5510
(SSM-AIP-10)
Cisco Router 3845
(1 NM-1T3/E3)
Catalyst
Express
CE500G-12TC
FE2
FE1
FE0
FE1
FE0
T3
internet
Core Switching
FE0
FE2
FE1
FE1
FE0
1/2T3
Cisco ASA 5510
(SSM-AIP-10)
Cisco Router 2811
(1 NM-1T3/E3)
JP Medical Transcription Services
Chicago, IL
SFTP
Connection
1 GB
Connection
100 MB
Connection


PRTC WAN
Physical Rack Design
Sunday, March 02, 2008
42 U
42 U
Core Switching
CE500G-12TC
Cisco Router 3845 (1 NM-1T3/E3)
Cisco Router 2811 (1 NM-1T3/E3)
Cisco ASA 5510 (SSM-AIP-10)
Cisco ASA 5510 (SSM-AIP-10)
1GB Ethernet

2.5.Security

WAN devices are separated into two parts in terms of security: the first line of defense are the advanced security features of the routers. These security features include Virtual Private Networking (VPN), Intrusion Protection, Firewall, Network Access Control, and more. Much of our data will be headed towards external recipients in JP X-Ray Asian Diagnostic and JP Medical Transcription Service so action must be taken to protect that data. An IPSec VPN will be created between headquarters and JP X-Ray Asian Diagnostic to ensure safe and uncompromisable delivery. IPSec VPN provide rugged encryption techniques to ensure data integrity between the two sites. As for connecting to JP Medical Transcription Service, a secure file transfer protocol (SFTP) service will be set in headquarters to protect the data being sent there. These VPN and SFTP options are purely to protect data that is being transmitted across the Internet to external computer networks. Protection from attacks on the first line of defense occurs at the Intrusion Protection System (IPS).

The IPS is designed to detect and prevent traffic that is deemed malicious. Based on IPS configuration, the system will decide on how to handle questionable traffic by either dropping the traffic, sending alerts to administrators and operators, not responding, or resetting the connection. A basic setup of an IPS will be configured on the Main and Standby routers. Implementing a basic setup in the routers while having IPS configured on the Security Appliances, but in a more fine tuned manner, will help mitigate attacks on the network in the first and second line of defense (the security appliances).

2.6.Equipment Maintenance and replacement

Maintaining WAN equipment is essential to day-to-day operations at PRTC. Not only must the network avoid all outages but we have to make sure that the equipment does not fail. To prepare for such situations, supplemental warranty and support products were purchased for the WAN equipment. This supplemental warranty package is called Smartnet. It is a service provided by Cisco to support Cisco hardware and software. This includes phone support, web knowledge base access, technical support, parts replacement. The following table lists the devices covered by Smartnet and the features offered.

Device	Support Model Number	Quantity	Features
Cisco 3845 ISR	CON-SNT-3845	3	Extended Service Agreement Replacement 1 Year On-Site 8x5 Support Next Business Day
Cisco 2811 ISR	CON-OS-2811	3	Extended Service Agreement Replacement 1 Year On-Site 8x5 Support Next Business Day
Cisco ASA 5510	CON-SUO1-AS1A10K9	6	Extended Service Agreement Replacement 1 Year On-Site 8x5 Support Next Business Day
Cisco Catalyst Express 500G-12TC	CON-SNT-CE5G12TC	6	Extended Service Agreement Replacement 1 Year 8x5 Support Next Business Day
APC UPS SUA2200	SUA2200	1	Technical Support Phone Consulting

			3 Years 24x7

2.7.Pricing

Retailer	Product Type	Manufacturer	Model		Price	Quantity	Total
Main Router							
Hardware.com	3845 ISR	Cisco		3845	$7,645.00	1	$7,645.00
Hardware.com	IOS Adv Sec	Cisco	CD384-ASK9		$1,260.00	1	$1,260.00
Hardware.com	Flash Memory Card 64 MB	Cisco	MEM3800-64CF		$140.00	1	$140.00
Hardware.com	Network Expansion Module	Cisco	NM-1T3/E3		$5,135.00	1	$5,135.00
CDW.com	Smartnet 1YR	Cisco	CON-SNT-3845		$1,586.99	3	$4,760.97
Total							$18,940.97
Standby Router							
Hardware.com	2811 ISR	Cisco		2811	$1,425.00	1	$1,425.00
Hardware.com	IOS Adv Sec	Cisco	CD28N-ASK9		$840.00	1	$840.00
Hardware.com	Flash Memory Card 64 MB	Cisco	MEM2800-64CF		$140.00	1	$140.00
Hardware.com	Network Expansion Module	Cisco	NM-1T3/E3		$5,135.00	1	$5,135.00
CDW.com	Smartnet 1YR	Cisco	CON-OS-2811		$551.99	3	$1,655.97
Total							$9,195.97
Main and Standby Security Appliances							
Hardware.com	Security Appliance w/ Adv Inspe	Cisco	ASA5510-AIP-K9		$4,635.00	2	$9,270.00
CDW.com	Smartnet 1YR	Cisco	CON-SUO1-AS1A10K9		$1,649.99	6	$9,899.94
Total							$19,169.94
Main Switch							
Hardware.com	Network Switch	Cisco	WS-CE500GTC		$1,137.11	2	$2,274.22
CDW.com	Smartnet 1YR	Cisco	CON-SNT-CE5G12TC		$154.99	6	$929.95
Total							$3,204.17
Backup Power							
CDW.com	Uninterpretable Power Supply	APC	SUA2200		$834.99	1	$834.99
CDW.com	UPS Support	APC	WBEXTWAR3YR-SP-03		$116.99	1	$116.99
Total							$951.98
Services							
JPTelco	T3 Internet Service 1 YR	JPTelco	T3 Internet		$4,000.00	36	$144,000.00
JPTelco	½ T3 Internet Service 1 YR	JPTelco	½ T3 Internet		$3,800.00	36	$136,800.00
Total							$280,800.00
Grand Total							$332,263.03

3. LAN Design

3.1.Infrastructure

3.1.1.Data Center Core Switching

3.1.1.1.Catalyst 6509E

The Cisco 6509E core switch will provide all core switching throughout the facility. This 9-slot chassis provides stability, redundancy and scalability to PRTC for many years of expansion if needed. The 6509E will provide connection from our internal network to the external network.

3.1.1.1.1.Modules

Cisco Supervisor Engine 720-3BXL - control processor

The 6509E's core switching ability will come from the Supervisor 720 module installed in slot 6 of the chassis. The Supervisor Engine 720 delivers scalable-performance, intelligence, and a broad set of features to address the needs of the most demanding service provider and enterprise deployment requirements for building modular, resilient, scalable, and secure layer 2 or layer 3 solutions by:

- Delivering scalable forwarding Performance: up to 400 Mpps IPv4 and 200 Mpps IPv6 with dCEF
- Multi Protocol Label Switching support (MPLS) in hardware: enabling the use of VPNs and layer 2 tunneling while improving traffic engineering for QoS
- Delivering up to 40 Gbps per slot of switching capacity; 720 Gbps aggregate bandwidth
- Providing support for new high performance next generation gigabit and 10Gigabit interfaces
- Protecting customer's investment, supporting all three generations of Catalyst 6500 series interfaces and service module configurations
- Supporting all 3 generations of Catalyst 6500 series interfaces, services modules and WAN interfaces
- Enabling an increase in chassis interface port density and services module configurations

Catalyst 6500 48-Port Gig Ethernet Modules

The other modules that will be installed are the 48-port Ethernet switches for data center LAN connections. There will be two Cisco Catalyst 6500 48-Port 10/100/1000 Ethernet Module s installed into slots one and two of the chassis. This dual setup will provide redundancy for all servers in the data center.

Cisco Catalyst 6500 (WS-X6724-SFP) (WSX6724SFPRF) Expansion Module

These mixed media modules contain 24 port fiber optic connections. The main use of these will be to connect the core switching equipment to the access layer switching equipment on each of the floors. The two modules will provide redundancy in case of failure. Each floor switch cluster will connect to both modules via fiber optics. These modules will be installed in slots five and six of the chassis.

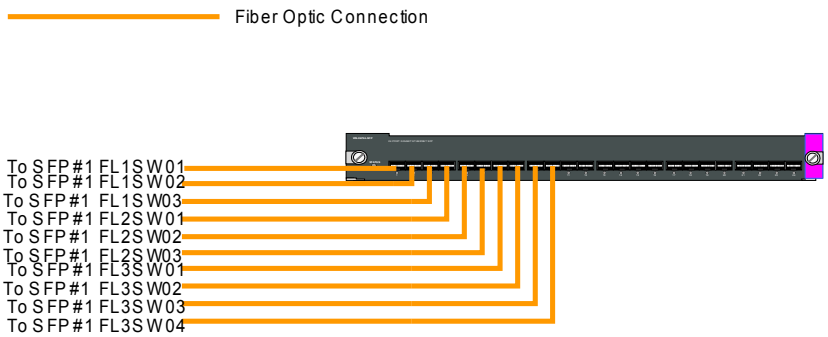
Cisco WS-CAC 8700W Power Supply

The power for the 6500 chassis will be provided with dual 8700W hot swap power supplies installed in each bay. These power supplies provide the ability to remotely cycle power the chassis and the following features:

- hot-plug / redundant (plug-in module)
- AC 100-240 V
- 8.7 kW

3.1.1.1.2.Wiring

There are two main wiring sections on the 6509E; the access layer switch connection, and the datacenter network connection. The access layer switch connection is provided through fiber optic cables into a 24 port SFP switch installed into the chassis. There will be two SFP switch modules to provide redundancy for communications to the access layer switches. The wiring for each module looks like the following:



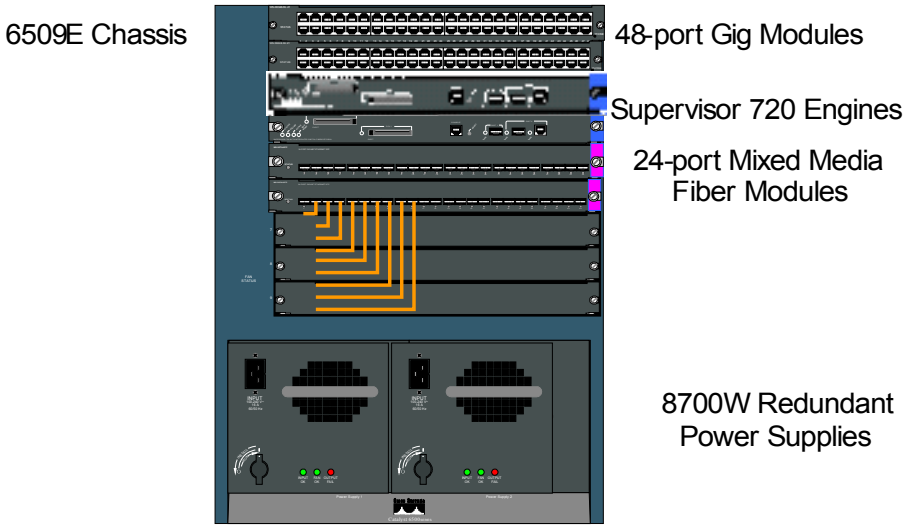
The wiring scheme for the core switch to the IDF switches is as follows:

Source Host	Source Interface	Destination Host	Destination Interface	Cable Type
PRTCCORESWTCH01	SFP#1 GE0/1	PRTCFL1SW01	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#1 GE0/2	PRTCFL1SW02	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#1 GE0/3	PRTCFL1SW03	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#1 GE0/4	PRTCFL2SW01	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#1 GE0/5	PRTCFL2SW02	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#1 GE0/6	PRTCFL2SW03	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#1 GE0/7	PRTCFL3SW01	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#1 GE0/8	PRTCFL3SW02	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#1 GE0/9	PRTCFL3SW03	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#1 GE0/10	PRTCFL3SW04	SFP GE0/1	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/1	PRTCFL1SW01	SFP GE0/2	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/2	PRTCFL1SW02	SFP GE0/2	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/3	PRTCFL1SW03	SFP GE0/2	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/4	PRTCFL2SW01	SFP GE0/2	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/5	PRTCFL2SW02	SFP GE0/2	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/6	PRTCFL2SW03	SFP GE0/2	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/7	PRTCFL3SW01	SFP GE0/2	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/8	PRTCFL3SW02	SFP GE0/2	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/9	PRTCFL3SW03	SFP GE0/2	Fiber Optic
PRTCCORESWTCH01	SFP#2 GE0/10	PRTCFL3SW04	SFP GE0/2	Fiber Optic

3.1.1.1.3.Warranty

Cisco products will be covered by SmartNet warranty plan in case of failure that includes three years on site replacement of failed parts. The warranty comes with 24 hour seven day support with a four hour on-site response time. This also includes full access to Cisco Connection Online (CCO) support forums for additional support.

3.1.1.1.4.Diagram



3.1.2.Closet Access Switching

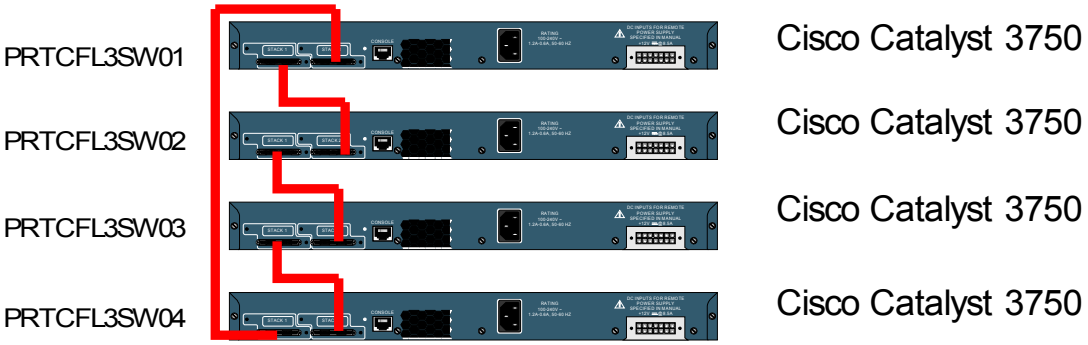
Each floor of the facility will have a dedicated Intermediate Distribution Facility that will house the access layer switching equipment as well as the patch panels. The patch panels will be the termination point for all of the network cable pulls throughout the floor. The Cisco 3750 switches will be setup as a stack and will act as one switch to control switching for the floor.

3.1.2.1.Cisco 3750

The Cisco Catalyst 3750 switch is a 48-port 100Base-TX fast Ethernet unit. This switch also contains four SFP ports that will be used for fiber connection to the core switch on the third floor.

3.1.2.1.1.Wiring

Each floor will have multiple 3750 switches that will be linked together to work as a stack. This means they will act as one switch with many ports. The wiring for each floor will look like the following (*Switch names and number of switches for each floor will vary depending on floor*):

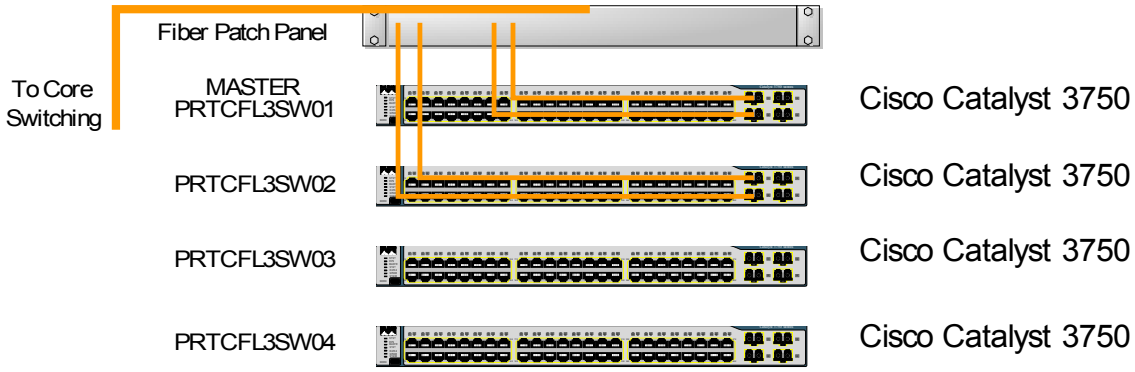


These connections will be made with StackWise cables that are included with each switch.

The wiring of the stacks is as follows:

Source Host	Source Port	Destination Host	Destination Port	Cable Type
Floor 1				
PRTCFL1SW01	Stack 1	PRTCFL1SW02	Stack 2	StackWise
PRTCFL1SW02	Stack 1	PRTCFL1SW03	Stack 2	StackWise
PRTCFL1SW03	Stack 1	PRTCFL1SW01	Stack 2	StackWise
Floor 2				
PRTCFL2SW01	Stack 1	PRTCFL2SW02	Stack 2	StackWise
PRTCFL2SW02	Stack 1	PRTCFL2SW03	Stack 2	StackWise
PRTCFL2SW03	Stack 1	PRTCFL2SW01	Stack 2	StackWise
Floor 3				
PRTCFL3SW01	Stack 1	PRTCFL3SW02	Stack 2	StackWise
PRTCFL3SW02	Stack 1	PRTCFL3SW03	Stack 2	StackWise
PRTCFL3SW03	Stack 1	PRTCFL3SW04	Stack 2	StackWise
PRTCFL3SW04	Stack 1	PRTCFL3SW01	Stack 2	StackWise

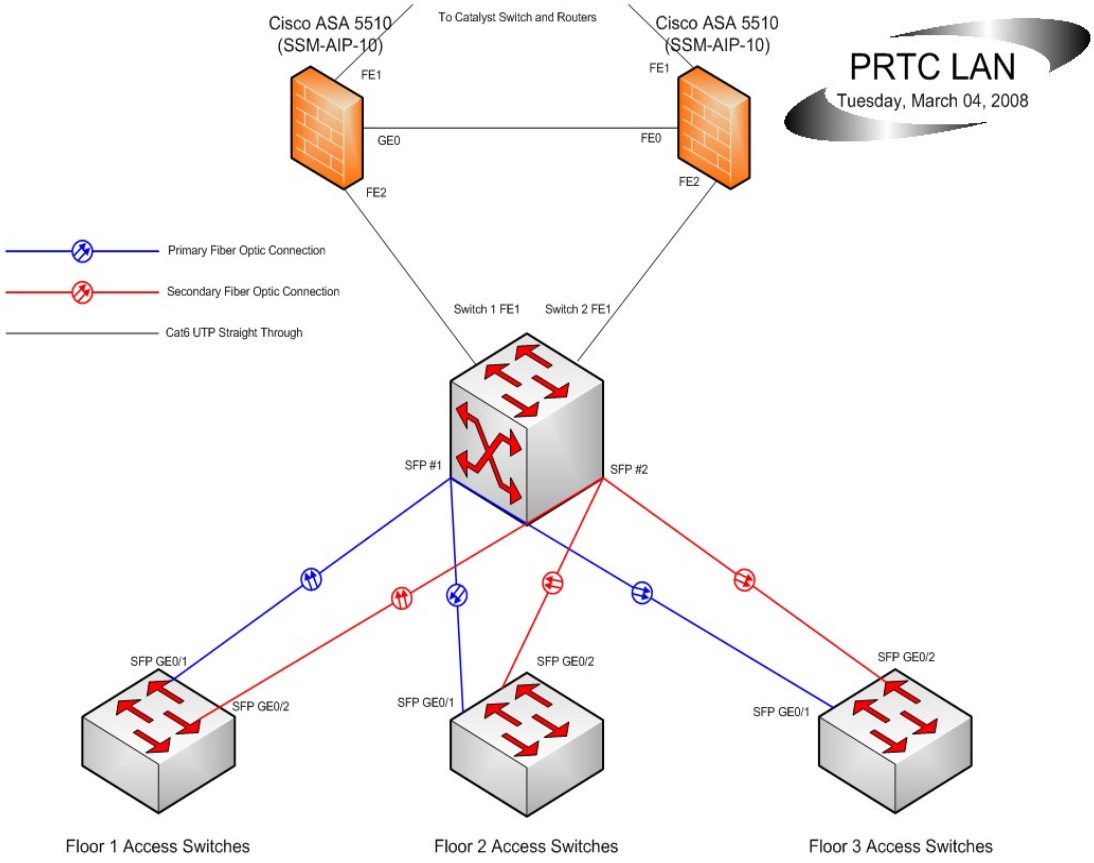
The Connections to the core switch will be made via fiber optics. A 6 strand MMF run will be run from the core switching area to each floor IDF rack and terminated in a fiber patch panel with port numbers 1-6. A dual redundant connection will be completed with two switches being connected to two SFP modules housed in the core switch. Switch 1 will have SFP port #1 and port #2 connected to SFP Module 1 Port 1 and SFP Module 2 Port 1 respectively. The following diagram displays a sample floor's switch wiring to the core layer:



3.1.2.1.2.Warranty

The Cisco Catalyst 3750 switch will be covered by SmartNet warranty plan in case of failure that includes three years on site replacement of failed parts. The warranty comes with 24 hour seven day support with a four hour on-site response time. This also includes full access to Cisco Connection Online (CCO) support forums for additional support.

3.1.2.1.3.Logical Core Switching Diagram



3.2.IP Addressing

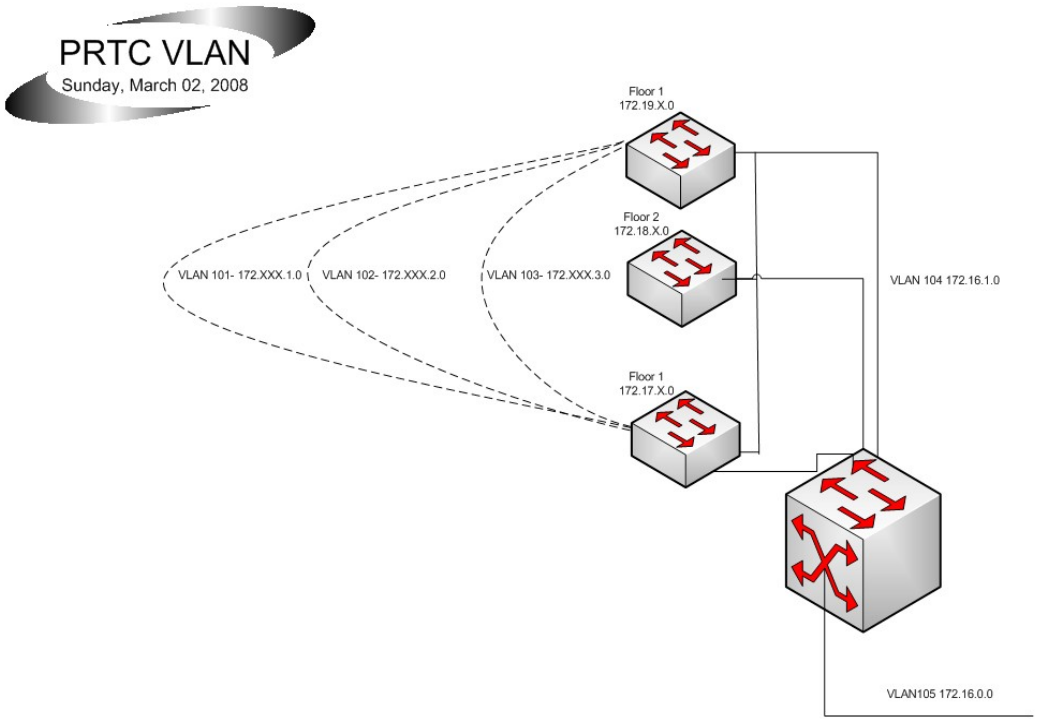
The IP addressing scheme for the LAN will consist of a class B private address range that will have different subnets and Virtual LAN's to separate floors and devices. The scheme will follow the 172.XXX.YYY.ZZZ. The XXX part of the address will be the subnet of the floor that the network is on. The YYY will be the Virtual LAN that the network is on. And the ZZZ will be the host address.

3.2.1.VLANs

PRTC will be designated six different VLAN's for separation. VLAN's will separate PC's, Printers, and Phones (Optional). The last three will be for the IT department, data center servers, and switches. The next table shows the VLAN specifications:

VLAN NAME	Description	Network	Subnet	Location
VLAN101	PC Vlan	172.XXX.1.0	255.255.255.0	All Floors
VLAN102	Printer Vlan	172.XXX.2.0	255.255.255.0	All Floors
VLAN103	Optional Phone Vlan	172.XXX.3.0	255.255.255.0	All Floors
VLAN104	Core Switch	172.16.1.0	255.255.255.0	Core Switch to Floor Switches
VLAN105	Server Vlan	172.16.0.0	255.255.255.0	Data Center

The following diagram shows the logical diagram of the VLAN's:



3.2.2.DHCP

All of the PC's on the network will be given an address dynamically. Utilizing the Dynamic Host Control Protocol, PRTC can save time deploying new equipment and have a better record of the already deployed equipment. DHCP address will be handed out using a DHCP server that will be located within PRTCDC02. Each floor will be given a different subnet network address dynamically according to the following table:

DHCP Server PC Vlan	Scope	Start Address	End Address	Subnet Mask	Default Gateway	DNS Servers
PRTCDC02	172.17.1.0	172.17.1.10	172.17.1.250	255.255.255.0	172.17.0.1	172.16.0.2/3
PRTCDC02	172.18.1.0	172.18.1.10	172.18.1.250	255.255.255.0	172.18.0.1	172.16.0.2/3
PRTCDC02	172.19.1.0	172.19.1.10	172.19.1.250	255.255.255.0	172.19.0.1	172.16.0.2/3

3.2.3.Statically Addressed Devices

DHCP will not be utilized to address the servers in the datacenter. These devices will be given static (non-changing) address manually due to the servers needing to be access constantly. A static address will allow other devices on the network to find the host because the address will never change. The following table describes the address scheme that is being used for each server in the data center:

Hardware	Server Name	IP Address ETH0/0	IP Address ETH0/1	Subnet Mask	Default Gateway	DNS Server	Secondary DNS
Raritan KX2-232	PRTCKVM01	172.16.0.4	172.16.0.24	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
Raritan KX2-232	PRTCKVM02	172.16.0.5	172.16.0.25	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCDC01	172.16.0.2	172.16.0.22	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCDC02	172.16.0.3	172.16.0.23	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL580 G5	PRTCSQL01	172.16.0.6	172.16.0.26	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL380 G5	PRTCSQL02	172.16.0.7	172.16.0.27	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL380 G5	PRTCSQL03	172.16.0.8	172.16.0.28	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL380 G5	PRTCSQL04	172.16.0.9	172.16.0.29	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL580 G5	PRTCESX01	172.16.0.10	172.16.0.30	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCEXCH01	172.16.0.11	172.16.0.31	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCEXCH02	172.16.0.12	172.16.0.32	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCFILE01	172.16.0.13	172.16.0.33	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCFILE02	172.16.0.14	172.16.0.34	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCVONTU01	172.16.0.15	172.16.0.35	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCESAFE01	172.16.0.16	172.16.0.36	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCAV01	172.16.0.17	172.16.0.37	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
VMWare VM	PRTCBADGE01	172.16.0.18	172.16.0.38	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
VMWare VM	PRTCTIGER01	172.16.0.19	N/A	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
VMWare VM	PRTCLOG01	172.16.0.20	N/A	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
Cisco ACS	PRTCACS01	172.16.0.39	172.16.0.40	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
Iprism	PRTCIPRISM01	172.16.0.41		255.255.255.0	172.16.0.1		
VMWare VM	PRTCWUS01	172.16.0.42		255.255.255.0	172.16.0.1	172.16.0.0	172.16.0.3

3.2.4.Networking Equipment

The switching equipment will also have static addresses for devices to locate them automatically and proper routing to take place. The next table dictates addresses for the LAN equipment:

Hardware	Host Name	IP Address	Subnet Mask	Default Gateway
Cisco 6509 Switch TOP	PRTCCORESWTCH01	172.16.0.1	255.255.255.0	172.16.0.50 172.16.0.51
Cisco 3750 Stack FL1	PRTCFL1SW01-03	172.17.0.1	255.255.255.0	172.16.0.1
Cisco 3750 Stack FL2	PRTCFL2SW01-03	172.18.0.1	255.255.255.0	172.16.0.1
Cisco 3750 Stack FL3	PRTCFL3SW01-04	172.19.0.1	255.255.255.0	172.16.0.1

3.3. Pricing

3.3.1. Overview

The following image is the pricing spreadsheet for the DataCenter.

3.3.2.Pricing Matrix

Product Type	Manufacturer	Model	DescriptiorPrice	Quantity	Total
Building Cabling					
Network Drop Dual	JPTelco	Cat5e	$125.00	108	$13,500.00
Network Drop Dual	JPTelco	Cat5e	$125.00	108	$13,500.00
Fiber Run	JPTelco	MMF 6 strand	$1,200.00	6	$7,200.00
Network Drop	JPTelco	Cat6 Datacenter	$150.00	144	$21,600.00
Fiber Run	JPTelco	MMF 6 strand Datacenter SAN	$1,200.00	2	$2,400.00
Cable Management	DataCenter Depot	DA-LR1024 10ftL x 2ftW	$116.81	5	$584.05
Patch Cable	CDW	Cat5e 3' Blue	$2.99	25	$74.75
Patch Cable	CDW	Cat5e 7' Blue	$2.99	100	$299.00
Patch Cable	Tripp Lite	Cat5e 5' Blue	$4.99	50	$249.50
Patch Cable	CDW	Cat5e 3' Black	$2.99	25	$74.75
Patch Cable	Tripp Lite	Cat5e 5' Black	$4.99	50	$249.50
Patch Cable	Tripp Lite	Cat5e 7' Black	$4.99	100	$499.00
Total					$60,230.55
Core Switching Hardware					
Core Switch	Cisco	Catalyst 6509E	$6,959.99	1	$6,959.99
Warranty	Cisco	Smartnet	$6,659.99	3	$19,979.97
Switch Module	Cisco	6500 series	$9,399.99	2	$18,799.98
Mixed Media Module	Cisco	WS-X6724-SFP	$11,869.42	2	$23,738.84
Supervisor Engine	Cisco	720*3BXL	$28,806.99	2	$57,613.98
Power Supply	Cisco	WS-CAC-8700W	$5,429.99	2	$10,859.98
Total					$137,952.74
Access Switching Hardware					
Floor Switches	Cisco	catalyst 3750	$6,113.99	10	$61,130.99
Warranty	Cisco	Smartnet	$1,059.99	30	$31,799.70
Network Module	Cisco	1000BASE-SX SFP	$379.99	12	$4,559.88
Total					$97,490.57
End-User Hardware					
Tablet PC	HP	Compaq Tablet PC tc4400	$1,975.99	20	$39,519.50
Docking Station	HP	Advanced Docking Station	$229.99	48	$11,039.52
Warranty	HP	3 year Pickup and Return	$189.99	20	$3,799.80
Total					$14,839.32
Data Integrity					
Encryption	Safeboot	Content Encryption Package	$33.00	20	$660.00
RSA Keys	RSA	SID800- 3 year 25-pack	$1,647.76	1	$1,647.76
Total					$2,307.76

4. DATA CENTER

4.1. Overview

In order to provide the much needed capabilities that PRTC needs, a state of the art data center has been designed with a two thoughts in mind; security and expandability. Every essential piece of the network is setup to have redundancy ensuring a high percentage of network uptime and the data center has been designed that if expansion in the future is needed, there is plenty of room and backbone network pieces to welcome the expansion.

4.2. Technical Solutions (Hardware)

4.2.1. Servers

4.2.1.1. HP Proliant DL360 G5

The HP Proliant DL360 G5 is a versatile 1U server which will house a number of PRTC's core services. This server provides dual GB network links for quick access and redundancy. Other features of this server include:

- 1 x Quad-Core Xeon E5335 / 2 GHz
- RAM 2 GB
- Hot-swap 2.5
- CD-RW / DVD
- ATI ES1000
- Power supply - hot-plug 700W

These servers will be customized with dual hot-swap 146GB SAS hard drives to provide both speed and redundancy in case of failure. The drives will be configured with a RAID1 array to provide a mirrored effect. This will increase redundancy because if one drive fails the other will take over after a reboot. The failed drive can be replaced and will automatically be replicated from the drive that is currently in working order.

4.2.1.1.1. Services Provided

4.2.1.1.1.1. Active Directory/DNS- PRTCDC01 & PRTCDC02

PRTC will have two servers setup as domain controllers as well as have Active Directory. This will provide redundancy in case of failure and allow us to provide more services spread across two servers than just one. These servers will provide the structure for all users and policies implemented at the clinic. More on the policies and AD services will be touched upon later in this document.

DNS services will also be installed on the two domain controllers and these will take care of all of the DNS records as well as forwarding DNS lookups to the internet. The domain name chosen for the clinic is PRTC.com. All DNS entries will be as follows; *ServerName.*PRTC.com.

DHCP services will provide a dynamic IP address server for hosts on the network using the dynamic host control protocol; this will mainly include PC's.

4.2.1.1.1.2.Exchange- PRTCEXCH01 & PRTCEXCH02

Two DL360's have been designated as email servers that will house account information and policies. The two servers will provide redundancy so that email will be available in the event of a failure. Due to the large amount of space that email can take up, the stores for exchange will be housed on the Storage Area Network (SAN) in its own partition. The two servers will be configured specially with fiber optic NIC cards. These fiber cards will be the connection to the SAN for quick response and transfer time of email. More on the configuration will be listed in the SAN section of this document. A global Internet domain name of PRTC.com will be used to direct all email messages from the Internet to the internal servers. The email policies will be discussed in the policy section of this document.

4.2.1.1.1.3.File and Print Services- PRTCFILE01 & PRTCFILE02

Two DL360's will be used as file and print servers. These servers will house the structure for all files and folders created by business processes. The dual servers will provide redundancy Due to the large amount of data that will be housed here; the actual storage will be on the SAN in a file partition. These servers will each have two fiber optic NIC cards installed to provide connection to the SAN for file access and transfer. The SAN section will provide more information on this configuration.

4.2.1.1.1.4.Vontu- PRTCVONTU01

Data protection is vital to this corporation due to the extreme confidentiality needed with its patients as well as the strict compliance it must follow including HIPAA. In order to help meet compliance and keep our customers assured that their identity is kept private; a data protection appliance must be put into place. Vontu is a leading company at helping companies meets compliance by following three simple rules; Data at Rest, Data in Motion, and Data at the Endpoint. Vontu does this by using the following technologies:

Vontu solutions provide comprehensive HIPAA data loss prevention for any organization that stores and/or transmits PHI. Advantages include:

- Pre-defined HIPAA Policy Template with Vontu's TrueMatch™ detection suite for the highest accuracy in the industry and over 24,000 keywords

- Discover and protect PHI data exposed on file servers, databases, Microsoft SharePoint®, Lotus Notes®, Documentum®, LiveLink®, web servers, Microsoft Exchange®, and other data repositories
- Monitor and prevent PHI loss on the network including email, IM, Web, Secure Web (HTTP over SSL), FTP, P2P, and generic TCP
- Discover PHI data stored on the endpoint, such as desktops and laptops, and prevent this data from being inappropriately used, sent out, or copied to storage devices such as USB drives, CD/DVDs, or iPods
- Comprehensive audit support through HIPAA compliance reports and role-based dashboards
- Automatically enforce PHI data security policies with a centralized platform for detection accuracy, policy management and automated incident response, notification, workflow and compliance reporting, to help organizations change employee behavior and pinpoint compliance gaps in existing business processes
- Role-Based Access Control enables business units and departments to review and remediate only those PHI incidents relevant to their role and privileges.

4.2.1.1.1.5.GFILanguard- PRTCESAFE01

See GFILanguard section for complete details on use

4.2.1.2. HP Proliant DL380 G5

The DL380 G5 is a more powerful server than the DL360. It contains two processors and more memory. These servers will handle more process intensive services that the clinic will need. Some of the key features of the DL380's chose are:

- Two 2.33GHz Intel Quad-Core Xeon E5345 Processor
- 2-Way
- 16MB Cache
- 4GB RAM
- SAS Drive
- Hot-Swap 2.5
- CD-RW/DVD-ROM
- 2- 10/100/1000 Ethernet

These servers will be customized with dual fiber optic NIC's to provide fast connection to the SAN for storage needs. They will also have dual 146GB SAS hard drives configured in RAID1 mode to provide redundancy and hot-swap capabilities.

4.2.1.2.1. Services Provided

The servers that will be housed in the DL380 platform are the SQL servers that will house the primary medical record databases that will be comprised of all the patient data and billing. These SQL servers will not actually house the databases; they will house the SQL applications with the databases stored on the SAN on their own separate encrypted partition. This will allow PRTC to meet compliance and have backups done daily to ensure no data is lost. The DNS names of these servers are PRTCSQL01, PRTCSQL02, PRTCSQL03, and PRTCSQL04 respectively.

4.2.1.3.HP Proliant DL580 G5

The Proliant DL580 G5 server is an extremely powerful and expandable server. This server will house our VM environment which will contain servers in our network. The DL580 contains the following hardware:

- Dual Quad Care Intel Xeon 2.13GHz processors
- 32GB PC2-5300 RAM
- 6- 146GB Hot Plug SAS 10,000rpm hard drives
- RAID1 Configuration
- HP Fire Channel 4GB Dual Channel
- 2 HP 1200W Hotpluggable power supplies

4.2.1.3.1.Services Provided

The DL580 server will come preinstalled with VMWare's ESX server operating system which will be our VM environment. Virtual servers provide a cost effecting and space saving way to build up a network. The VMWare section of this document will explain virtual servers in more detail and how VMWare accomplishes this.

4.2.1.4.Warranty for HP Servers

The warranties provided for the HP servers are all inclusive (meaning additional hardware) and are for a period of three years. The warranties provide 24 hours a day seven days a week The service provides four hour on-site replacement with parts and labor included. This means that in the even of a failure, and HP representative will be out to fix the problem in four hours. The pricing for the warranties is in the pricing section of this document.

4.2.2.Server IP Addresses

All servers will have 255.255.255.0 (/24) subnet mask as well as a default gateway address of 172.16.0.1. This is the address of the Core Switch module that the servers NIC cards connect to. The DNS Servers will be

Hardware	Server Name	IP Address ETH0/0	IP Address ETH0/1
HP Proliant DL360 G5	PRTCDC01	172.16.0.2	172.16.0.22
HP Proliant DL360 G5	PRTCDC02	172.16.0.3	172.16.0.23
HP Proliant DL580 G5	PRTCSQL01	172.16.0.6	172.16.0.26
HP Proliant DL380 G5	PRTCSQL02	172.16.0.7	172.16.0.27
HP Proliant DL380 G5	PRTCSQL03	172.16.0.8	172.16.0.28
HP Proliant DL380 G5	PRTCSQL04	172.16.0.9	172.16.0.29
HP Proliant DL580 G5	PRTCESX01	172.16.0.10	172.16.0.30
HP Proliant DL360 G5	PRTCEXCH01	172.16.0.11	172.16.0.31
HP Proliant DL360 G5	PRTCEXCH02	172.16.0.12	172.16.0.32
HP Proliant DL360 G5	PRTCFILE01	172.16.0.13	172.16.0.33
HP Proliant DL360 G5	PRTCFILE02	172.16.0.14	172.16.0.34
HP Proliant DL360 G5	PRTCVONTU01	172.16.0.15	172.16.0.35
HP Proliant DL360 G5	PRTCESAFE01	172.16.0.16	172.16.0.36
HP Proliant DL360 G5	PRTCAV01	172.16.0.17	172.16.0.37
VMWare VM	PRTCBADGE01	172.16.0.18	172.16.0.38
VMWare VM	PRTCTIGER01	172.16.0.19	N/A
VMWare VM	PRTCLOG01	172.16.0.20	N/A
Cisco ACS	PRTCACS01	172.16.0.39	172.16.0.40
Iprism	PRTCIPRISM01	172.16.0.41	
VMWare VM	PRTCWUS01	172.16.0.42	

4.2.3.Storage Solution

In order to efficiently and safely store data, a Storage Area Network will be placed in the data center to provide all storage of files and databases. A SAN is a centrally managed storage center that is expandable and upgradeable. The SAN that was chosen is from IBM

4.2.3.1.IBM SAN

The IBM SAN consists of four different parts; the storage bays, the storage volume controllers, the SFP switch, and the UPS battery backup.

DS4800 Disk Storage Bay

The IBM System Storage DS4800 is a midrange disk system that will provide enough storage space and expandability for years to come as the business grows. Benefits of this system are

- 4 Gbps Fibre Channel interface technology
- Up to 1600 MBps bandwidth for high throughput applications
- Fibre channel and SATA hard disk drives supported
- Includes IBM DS4000 Storage Manager to help centrally manage the DS4000 series
- Eight host channels for increased connectivity

This system is expandable to 112TB of storage with flexible disc sizes and types supported.

SAN Volume Controller Storage Engine 2145 Model 8F4
The SVC 2145-8F4 contains specialized software, storage engines, a master console, and external UPS'. Two controllers must be purchased to have a master and a slave to provide redundancy. The controllers have 4-GBPS NIC cards installed to access the servers across the datacenter.

SAN32-B-3 Fabric Switch
This switch provides up to 4GBPS auto-sensing links to each device plugged into it. This will be the core switch for the SAN environment and will encompass the SQL, File, and Exchange server fiber links.

Hardware Summary: (ibm.com)

- Base switch includes 16 ports activated, Advanced Zoning, Fabric Watch, Web Tools and redundant hot-swappable power/fan modules in an efficient, compact enclosure
- Each port can auto-negotiate to 4, 2 or 1 Gbps link speeds depending on the speed of the device at the other end of the link
- 8-Port Activation feature allows "pay as you grow" scalability from 16 to 24 or 32 active ports
- Non-blocking architecture enables up to 256 Gbps throughput with a 32-port configuration
- Shortwave and longwave Small Form-factor Pluggable (SFP) optical transceivers are available
- Optional advanced security, performance monitoring and ISL trunking features provided enhanced capabilities needed in larger and extended distance SAN configurations

4.2.3.1.1.Partitions

The SAN will have different partitions to keep data separate. Each partition will be setup as a RAID 1 to provide a mirrored redundancy in order to ensure data is not lost. 20 300GB disks will be placed in each storage unit for a total of 12 terabytes of storage. These disks are hot-swap 15krpm hard drives with a 4GB Fibre Channel interface to provide maximum transfer rates. Figure # shows the partition table:

Partition	Size	Description
I:	1 TB	Personal Drives for Employees
X:	500 GB	Outgoing XRAY Files
Y:	1 TB	SQL Databases
W:	1 TB	Email
V:	500GB	VM Backups

4.2.4.Server Network Connections

Each server has two gigabyte NIC cards that support cat5e or cat6 UTP Ethernet cable. Both NIC cards will be connected for redundancy to ensure availability of servers at all times. In each rack there is a 48 port patch panel that will be used for all IP connectivity. Each rack will have a letter to identify which patch panel belongs to which rack. The connectivity for servers is as follows:

Server	ETH 0/0	ETH 0/1	KVM
PRTCSQL01	A-001	A-002	A-025
PRTCSQL02	A-003	A-004	A-026
PRTCSQL03	A-005	A-006	A-027
PRTCSQL04	A-007	A-008	A-028
PRTCESX01	A-009	A-010	A-029
PRTCDC01	B-001	B-002	B-025
PRTCDC02	B-003	B-004	B-026
PRTCEXCH01	B-005	B-006	B-027
PRTCEXCH02	B-007	B-008	B-028
PRTCFILE01	B-009	B-010	B-029
PRTCFILE02	B-011	B-012	B-030
PRTCVONTU01	C-001	C-002	C-025
PRTCESAFE01	C-003	C-004	C-026
PRTCAV01	C-005	C-006	C-027
PRTCSAN01	D-001	D-002	D-025
PRTCSAN02	D-003	D-003	D-026

4.2.5.KVM

4.2.5.1.Raritan KX2-232 IP

To support all systems in the PRTC Data Center, an IP based KVM will be used. This solution will provide access to each server from either the console in the data center, or through the network at a workstation. The Raritan model that was chosen provides 32 ports for 32 servers to be monitored. These models come complete with dual redundant power supplies, a console port, and four IP based consoles for monitoring.

4.2.5.1.1.Redundancy

In the case of a failure and immediate access is needed; a backup KVM will be in place to support each server on standby. At the time of failure, cables will have to be manually unplugged from the master KVM and plugged into the slave KVM. Although it is highly unlikely one of these will fail, we still recommend dual KVM switches in case of expansion.

4.2.5.1.2.Cables

Each server will be connected to the KVM via IP. Each server has a standard VGA and PS/2 ports for console connection so a KVM cable for each server is needed to complete the connection.

4.2.5.1.3.Warranty

The guardian support services gold package three year service will be chosen for warranty protection of the KVM switches. This support package provides 24 hour availability for phone consulting, technical support, and email consulting. If the event of a failure occurs the KVM will be replaced within 24 hours.

4.2.6.Racks

4.2.6.1.HP 10842 Wide Rack

The Racks chosen for the data center are the HP 10842 racks. They have a wide design to provide excellent cooling and cable management for the enterprise. The 10842 is a standard 42U rack with a size of 19inches. These racks meet RoHS compliance standards.

Specifications:

- Height- 42U
- Material- Metal
- Rack Size- 19”
- Weight Limit- 2000lbs
- Depth- 39.8 inches
- Height- 78.7 inches
- Weight- 295.4lbs
- Width- 31.5 inches

The racks will be used both in the data center and in the IT staging room for all rack mounted servers.

4.2.7. UPS

4.2.7.1. APC Symmetra PX 40Kw

The PRTC facility already has a generator in place in case of a power failure, but this generator does not provide power at the moment of failure. Due to this fact a battery backup system is needed to provide power for all of the major systems during a power failure before the generator kicks in. The APC Symmetra PX-40Kw has the following input and output specs:

Input

- Built-in Static Bypass
- 208V 3PH Normal Input Voltage
- 50/60 Hz +/- 5Hz Input Frequency
- Hard Wire 5-wire Input Connections
- Input voltage range of 177-240V

Output

- 90% efficiency at full load
- 40kW / 40kVA output power capacity

This system uses four battery modules to provide the power and can power 20,000 Watts (half of its capable load) for 13.9 minutes. In the event of more power needed, four additional slots are available for expansion.

4.3. Licensing

4.3.1. Operating System

4.3.1.1. Microsoft

The operating systems being used on almost all of the servers is Microsoft Windows Server 2003 R2 Enterprise Addition. The data center will need 14 licenses for each of the servers running Windows. Server 2003 R2 is Microsoft's latest build of its proven server operating system with features including:

- Active Directory
- File and Print Server
- DNS services
- Easy to use management tools

Servers Using This Software:

- PRTCDC01
- PRTCDC02
- PRTCSQL01
- PRTCSQL02
- PRTCSQL03
- PRTCSQL04
- PRTCEXCH01
- PRTCEXCH02
- PRTCFILE01
- PRTCFILE02
- PRTCVONTU01
- PRTCESAFE01
- PRTCAV01
- PRTCBADGE01
- PRTCLOG01
- PRTCWUS01
-

4.3.2.SQL Server

In addition to the operating system software needed, PRTC will also need a database software that will manage and control all databases used at the clinic.

4.3.2.1.Microsoft

The database software that will be installed on each of the SQL servers is Microsoft's SQL Server Standard 2005 Edition. Features of SQL Server include:

- Data Mining Tools
- Easy to use GUI
- Integration into Server 2003
- Increased availability with failover clustering and database mirroring

Servers Using This Software:

- PRTCSQL01
- PRTCSQL02
- PRTCSQL03
- PRTCSQL04

4.3.3.Virtual Infrastructure

A virtual infrastructure of servers provides a scalable single server that can house numerous servers to save money and space. The product we chose for our VM environment is VMWare's ESX Server. This is a Linux based operating system with

an IP GUI to handle all the user interaction with servers and maintenance.

4.3.3.1. VMWare ESX Server

The licensing for an ESX server consists of a per processor license. In the case of the dual processor server we are using, a standard two processor license is needed. After this is installed, each server needs its own server license; this is accounted for in the Microsoft section of licensing for operating systems.

4.3.4. Client Access License

4.3.4.1. Microsoft

In order for each employee to have access to the network systems, Client Access Licenses (CAL) must be purchased. These CAL's get installed on the domain controller servers to provide each user a license to have a network account. PRTC has approximately 100 employees so it is recommended that 125 user CAL's be purchased. The reason for extra is in case of new hires or any consultants that might be working at the facility with short notice. Fines and penalties can be high if compliance with user CAL's is not met.

4.3.5. Email Server

4.3.5.1. Microsoft Exchange Server

Microsoft Exchange Server 2007 will provide email services for PRTC. This software provides seamless integration with Windows 2003 Active Directory for easy manageability. Exchange also provides a web interface for employees to access email securely from anywhere there is an Internet connection. This feature will not be part of this design but the system is capable of having this option down the line. This software will be installed on the two exchange servers.

Servers Using This Software:

- PRTCEXCH01
- PRTCEXCH02

4.4. Network Cabling

All cabling that is needed to run throughout the building will be supplied by JPTelco. This includes fiber optic runs, UTP network cable runs and all supplied patch panel terminations.

4.4.1.Fiber Runs

Fiber optic runs include 6 strands in each run and will be used for connection between the Storage Area Network (SAN) with accessing servers and between the core switch and the floor switch stacks. In total six fiber optic MultiMode Fiber runs are needed to complete the fiber optic network. One run from each floor IDF to the data center core switch rack is needed totaling three for the switching equipment. The last three are all data center internal to and from the SAN. The two server racks that will need to access storage on the SAN are the SQL/VM rack and the domain/email/file rack. These are the servers that have stores on the SAN and will need fiber optic connections due to the high amount of transfer speed needed.

4.4.2.Cat5e UTP Runs

Each floor will need to have Cat5e network cable run from each IDF closet to each desk/access area throughout the floor. Each termination will have a total of four network jacks for connections to the network. One jack is for the PC, one jack is for an optional printer, one for a VoIP phone when implemented, and one for a spare/optional fax machine. A total of 108 runs of four wires are needed to complete network connections for all stations and rooms needing access to the network. A diagram of each network jack location is located later in this document.

4.4.3.Cat6 UTP Runs

In the data center, the wiring will be a higher category standard to provide gigabit connections between the server and the switching equipment to make communications quick. Each rack will have a 48-port patch panel at the top that will consist of 48 individual Cat6 runs from the rack to the patch panel rack next to the core switch rack.

4.4.4.Patch Panel Wiring

A dedicated patch panel rack will reside next to the core switching equipment rack. This group of six 48-port RJ45 patch panels will provide connection to each individual rack for both network and IP KVM connections. Each rack will be designated a letter and each port will be designated a number. Rack A's first port will be designated by "A-001" and Rack A's 48th port will be named "A-048". This will provide easy tracing of wires if need be. The connections will be from the server/host port to the rack port. The rack port will be connected to the corresponding patch panel port via a Cat6 cable run. The patch panel port will then be connected to the designated switch port. The wiring scheme for both the KVM and Server connections are detailed in the table on the next page.

Server	ETH 0/0	ETH 0/1	KVM
PRTCSQL01	A-001	A-002	A-025
PRTCSQL02	A-003	A-004	A-026
PRTCSQL03	A-005	A-006	A-027
PRTCSQL04	A-007	A-008	A-028
PRTCESX01	A-009	A-010	A-029
PRTCDC01	B-001	B-002	B-025
PRTCDC02	B-003	B-004	B-026
PRTCEXCH01	B-005	B-006	B-027
PRTCEXCH02	B-007	B-008	B-028
PRTCFILE01	B-009	B-010	B-029
PRTCFILE02	B-011	B-012	B-030
PRTCVONTU01	C-001	C-002	C-025
PRTCESAFE01	C-003	C-004	C-026
PRTCAV01	C-005	C-006	C-027
PRTCACS01	c-007	c-008	c-028
PRTCSAN01	D-001	D-002	D-025
PRTCSAN02	D-003	D-003	D-026

4.4.5.Patch Cables

In addition to the cable runs, patch cables are needed to connect hosts to patch panels. These patch cables will be purchased in bulk in the following denominations. Different colors and different sizes are needed for connectivity and to distinguish different items. Blue cables will designate a server, and black cables will designate a KVM connection. The following table shows denominations of cables:

Description	Size/Color	Quantity
Patch Cable	Cat5e 3' Blue	25
Patch Cable	Cat5e 7' Blue	100
Patch Cable	Cat5e 5' Blue	50
Patch Cable	Cat5e 3' Black	25
Patch Cable	Cat5e 5' Black	50
Patch Cable	Cat5e 7' Black	100

4.5. Cable Management

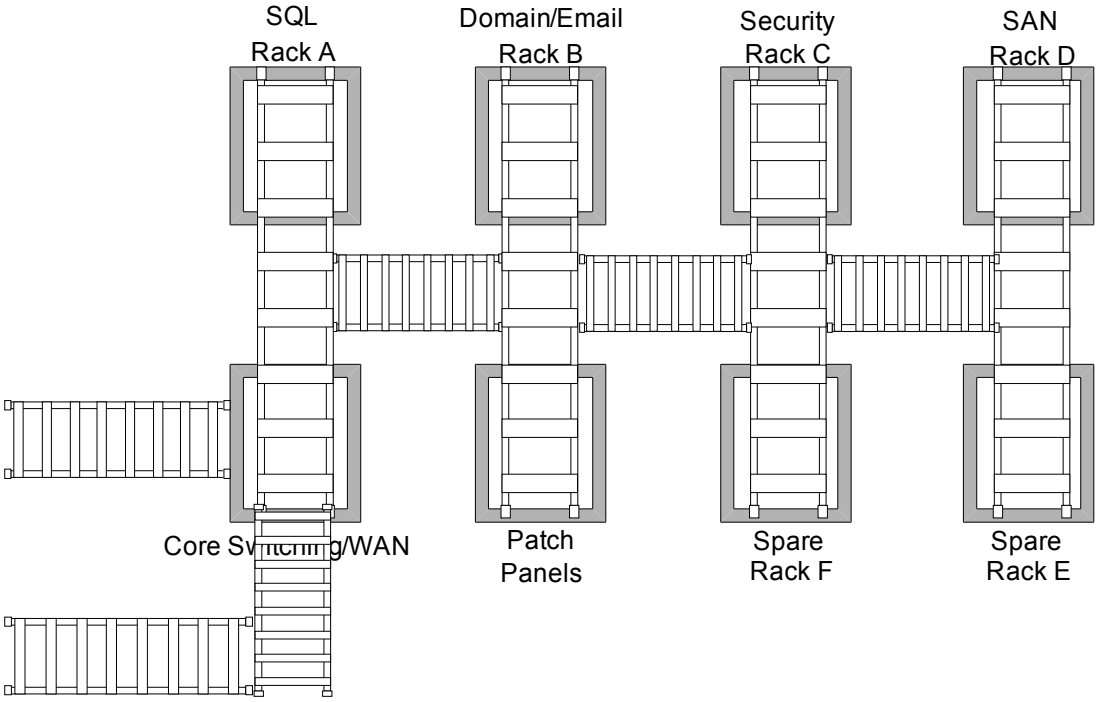
The datacenter will have a lot of wiring running in out and around it and therefore will have to have a cable management system to keep wires neat and out of the way to prevent problems. The cable management chosen for the datacenter and IDF rooms is a ladder rack system. A ladder rack system provides overhear ladders for wires to run on.

4.5.1. Ladder Rack System

The ladder rack system will be setup in an H formation with access to each rack as well as access to the outside cabling. This cabling will include the IDF fiber connections as well as the telecommunication WAN connections. The ladder rack system comes in variable lengths and will be cut to specific size and connected with included connector pieces. This system can be expanded at any time for additional cable runs. Some specifications of the system are as follows:

- 24" Wide x 10 foot long Ladder Racks
- Easily attaches to enclosure or server rack
- Ladder Rack is category 5 and 6 compliant and meets TIA-569A standards
- Made of 16 gauge tubular steel, finished with a durable, non-corrosive powder coat

A diagram of the ladder rack system in the data center:



4.6. Domain Names

In order to keep track of users, promote policies, support email and network related problems; a domain will be created to centralize the management. The domain name chosen for the internal network is PRTC.com. This will ensure all devices are part of the same network and can all be monitored and accessible. PRTCDC01 and PRTCDC02 servers will be the designated domain controllers where the Active Directory, DNS, DHCP, File, and Printer servers will be located. The two servers will be setup so that if one fails the entire domain does not go down. The domain table shows the different Organizational Groups and Security Groups that will be created to separate groups within the clinic:

Type	Name	Members
Organization Unit	PRTC_USERS	All users/Security Groups
Security Group	Doctors	All Doctors
Security Group	IT	IT employees
Security Group	Nurses	All Nurses
Security Group	PRTC	All Employees
Security Group	Administrative/Operations	Admin/Operation Employees
Security Group	Office Assistants	All Office Assistants
Security Group	Mailroom	All Mailroom employees

4.7. Monitoring

In order to have an efficient network, a monitoring scope will be created in order to visually monitor all important devices on the network. This will keep track of error messages.

4.7.1. Network

4.7.1.1. Microsoft Operations Manager

Microsoft Operations Manager will be used to monitor the Servers for errors and changes. This will be reported via email or text message to any IT employee for quick response. Some specifications of MOM are:

- Monitoring, troubleshooting, audit collection, and reporting for any server workload or application, including the base operating system, system hardware, and other management agents on the system
- System Center Operations Manager automates routine, redundant tasks, and provides intelligent reporting and monitoring to help increase efficiency and enable greater control of your IT environment
- Operations Manager 2007 and includes the Audit Collection Services feature, which automates the collection and consolidation of Windows security logs
- Audit Collection Services gather the required data to be analyzed against the specific compliance rules

This monitoring software can audit the following changes:

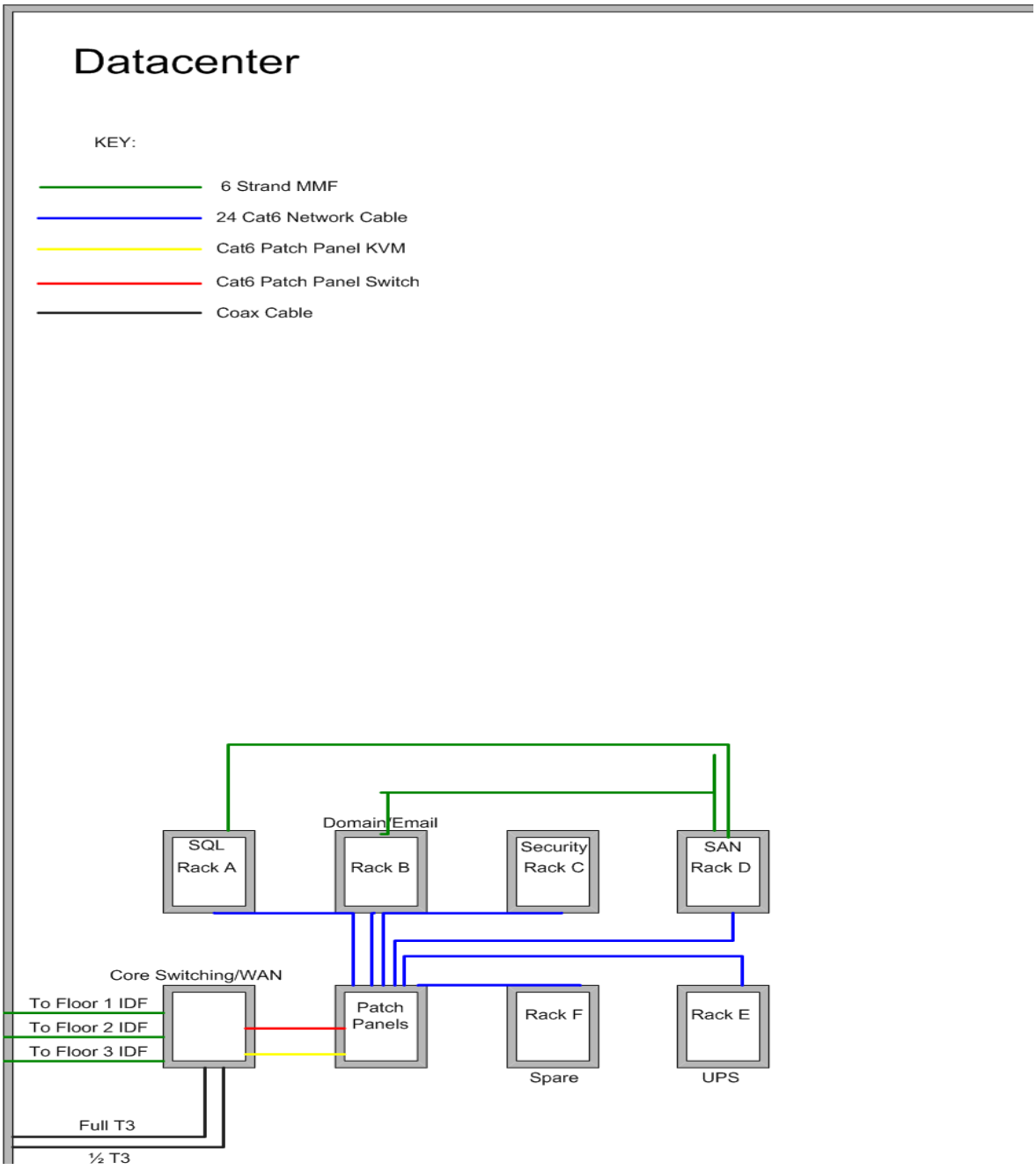
- User account created/deleted, enabled/disabled
- Administrator groups changes
- Group membership changes
- Changing someone else's password
- Computer account created/deleted
- Unauthorized access attempts
- Account locked
- Audit policy changed
- Object permissions changed
- Account policy changed
- Lost events
- Audit failure
- Log cleared
- Privilege added/removed

These audits can be created in a SQL database and sent out in an easy to read report if needed.

4.8. Diagrams

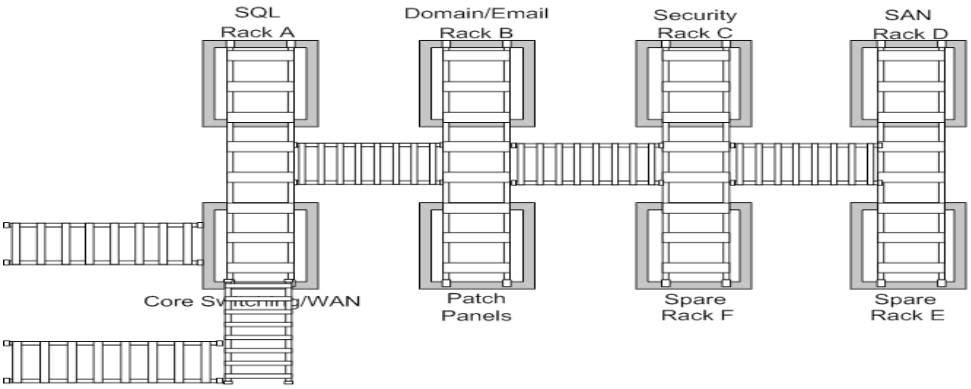
4.8.1. Datacenter

4.8.1.1. Wiring

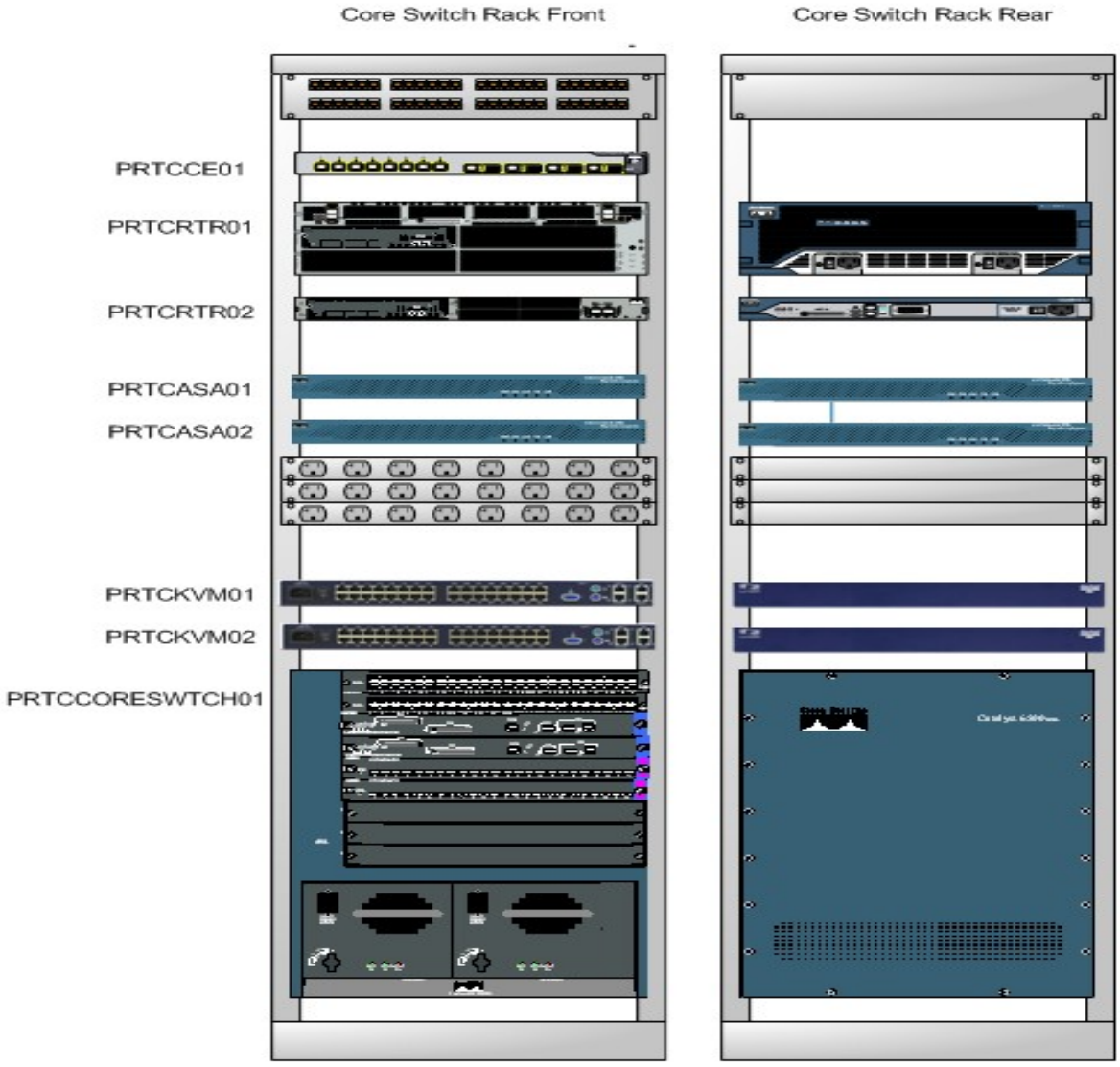


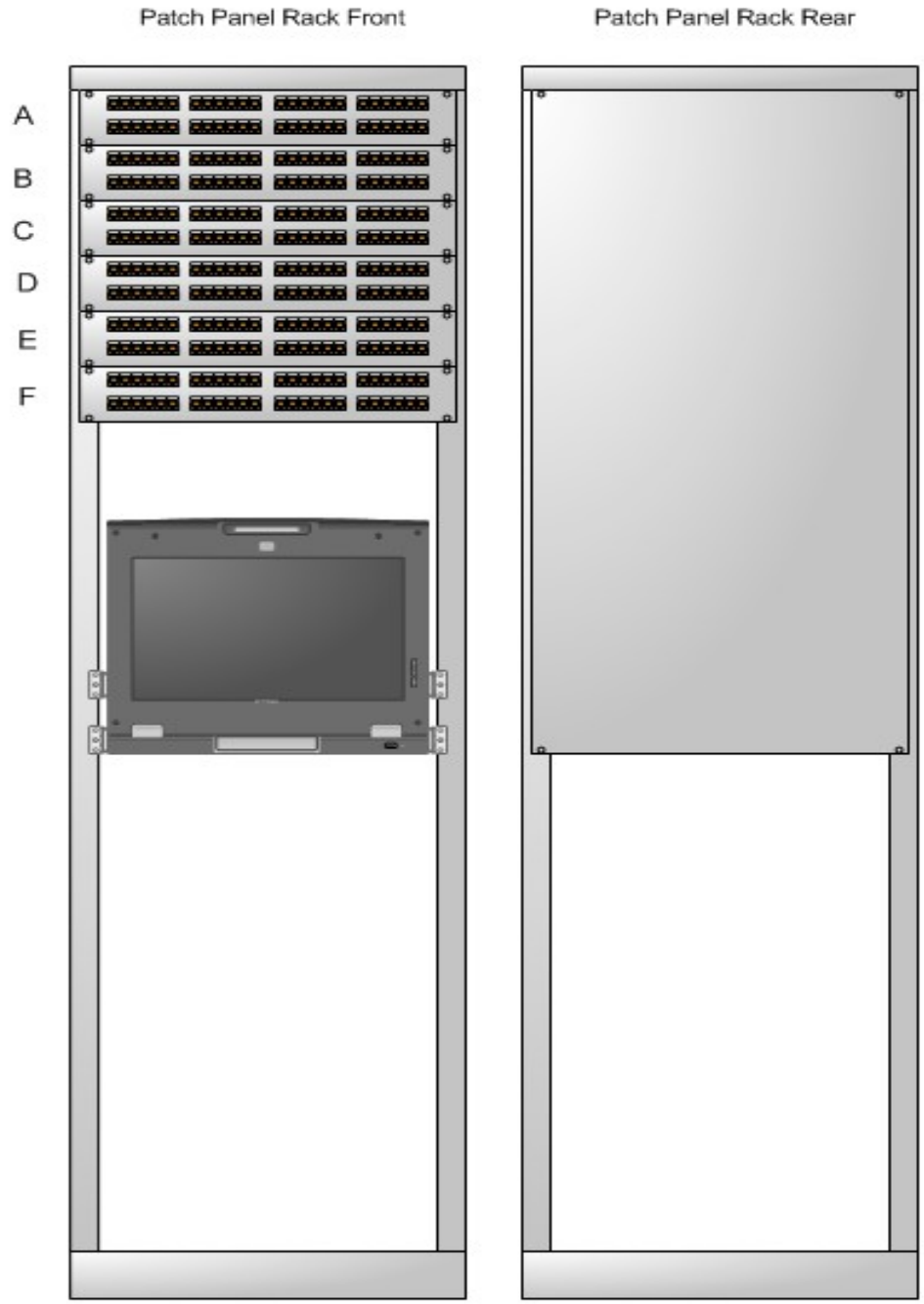
4.8.1.2.Cable Management

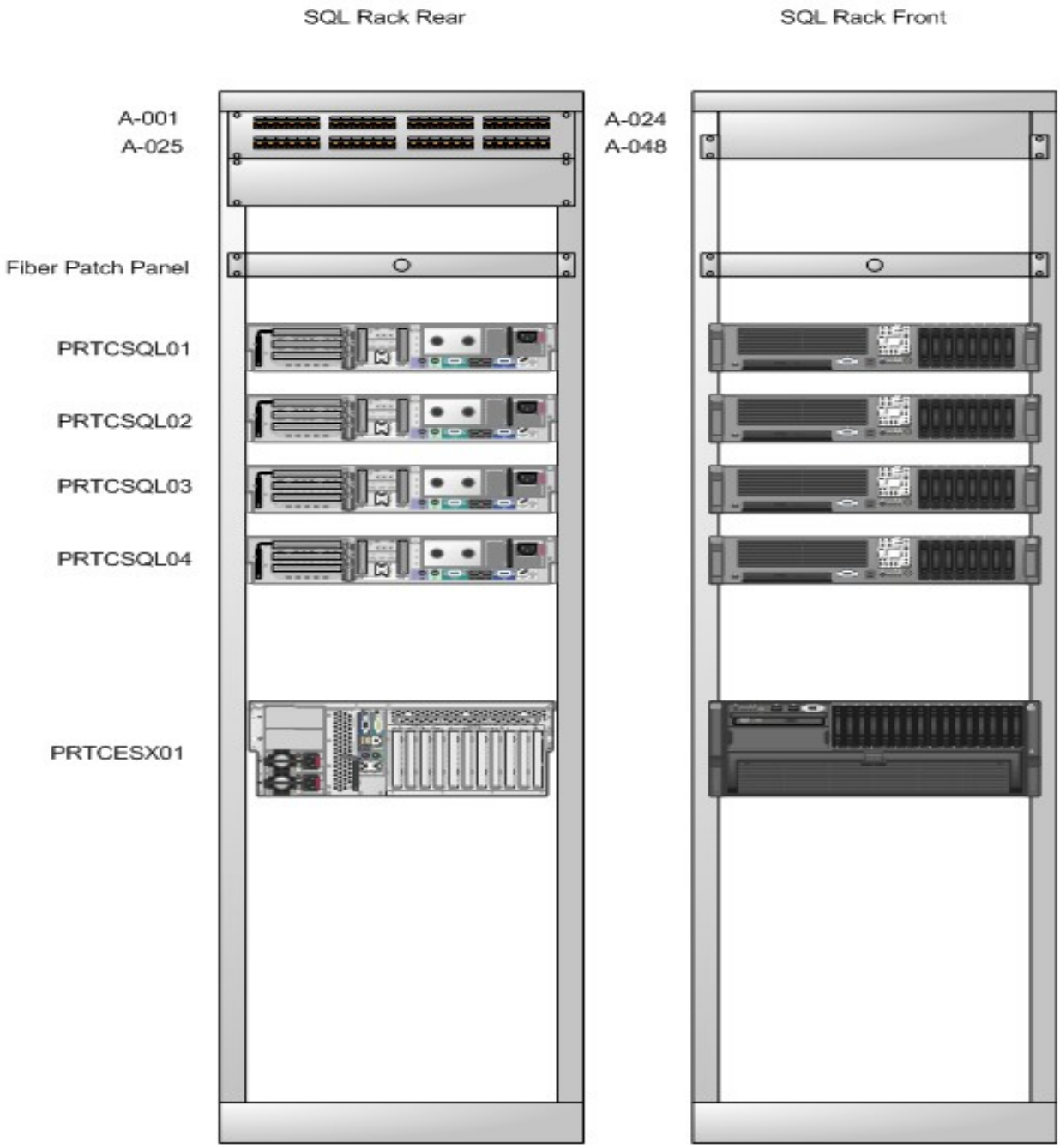
Datacenter

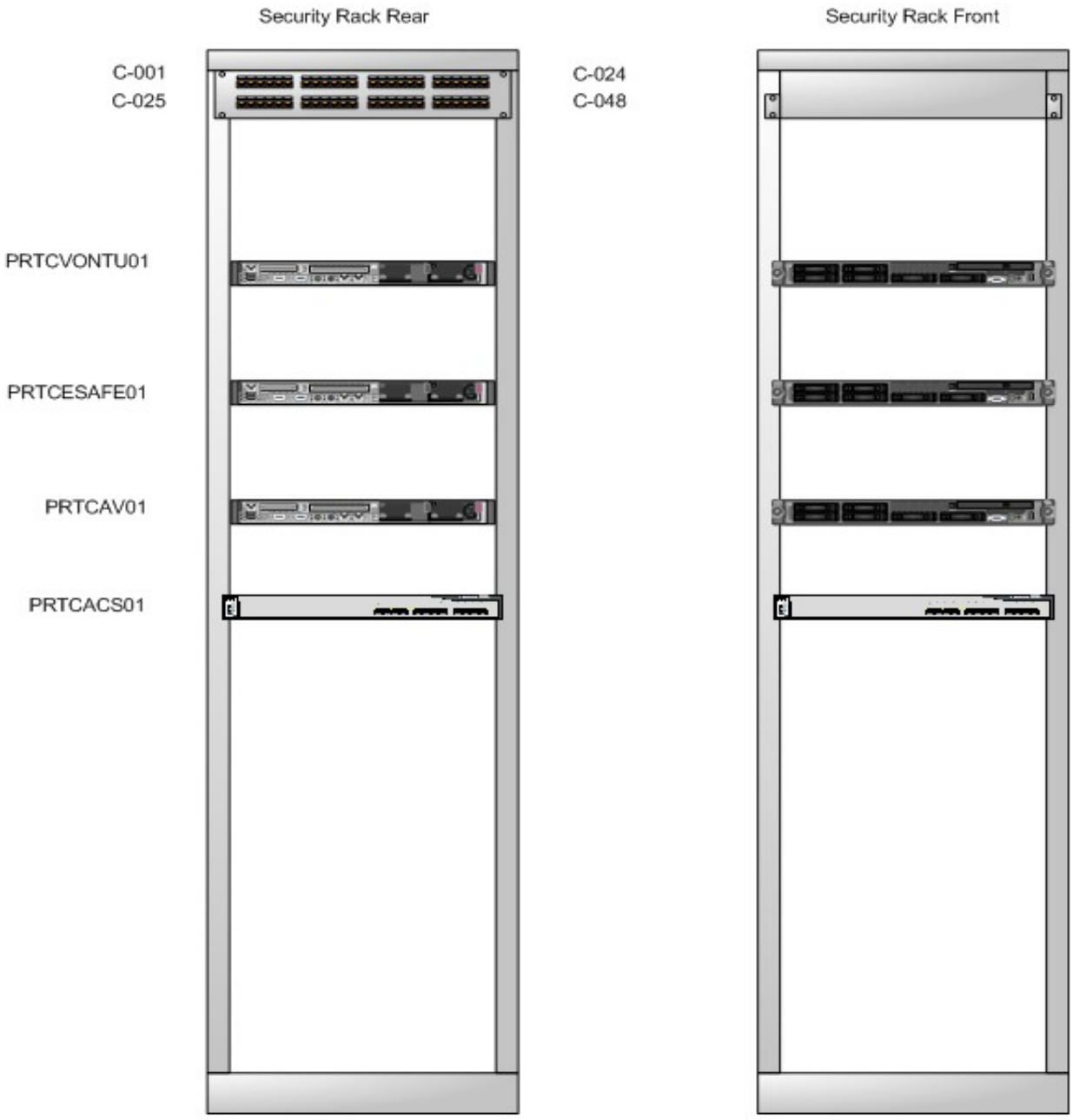


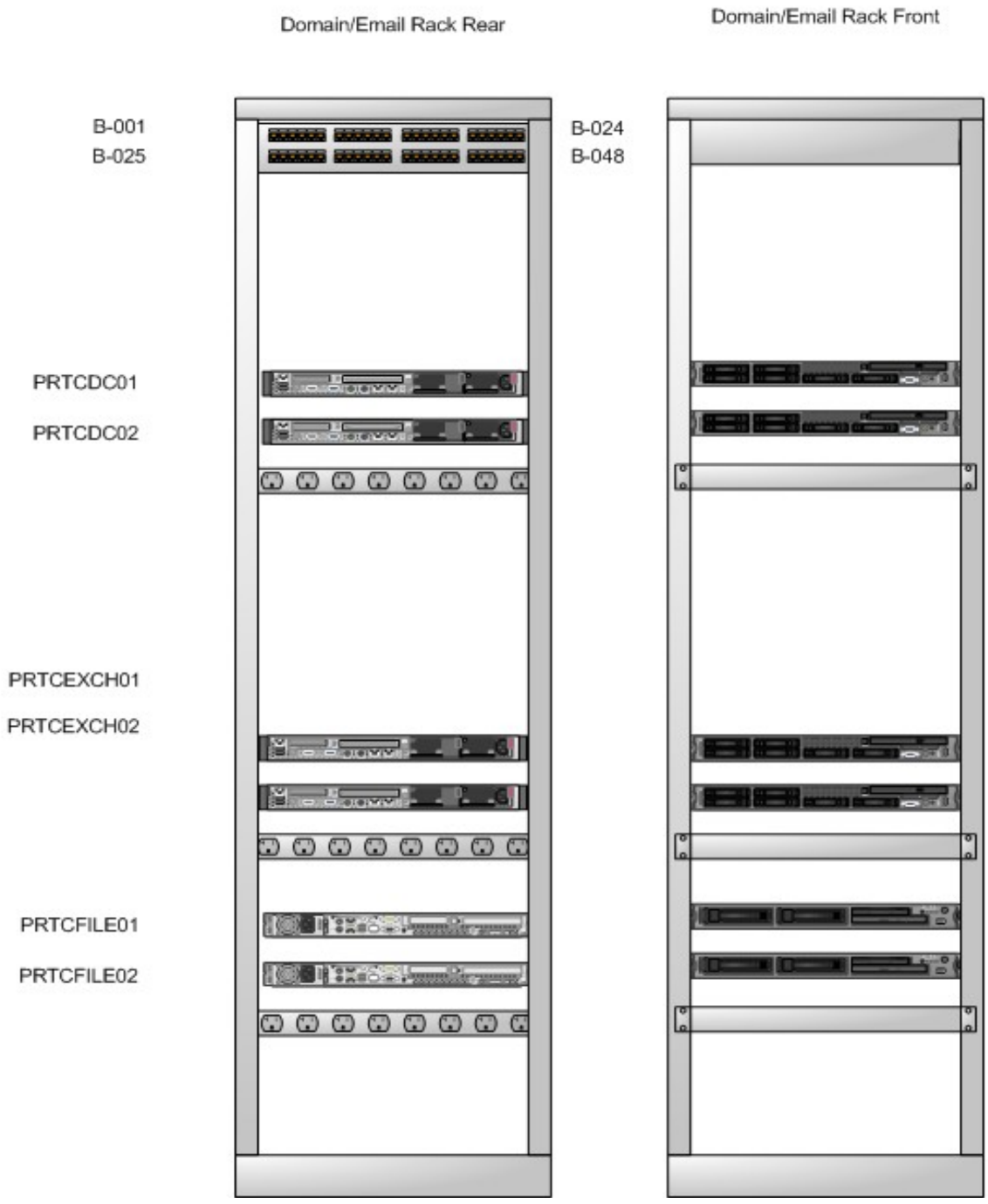
4.8.2.Data Center Racks

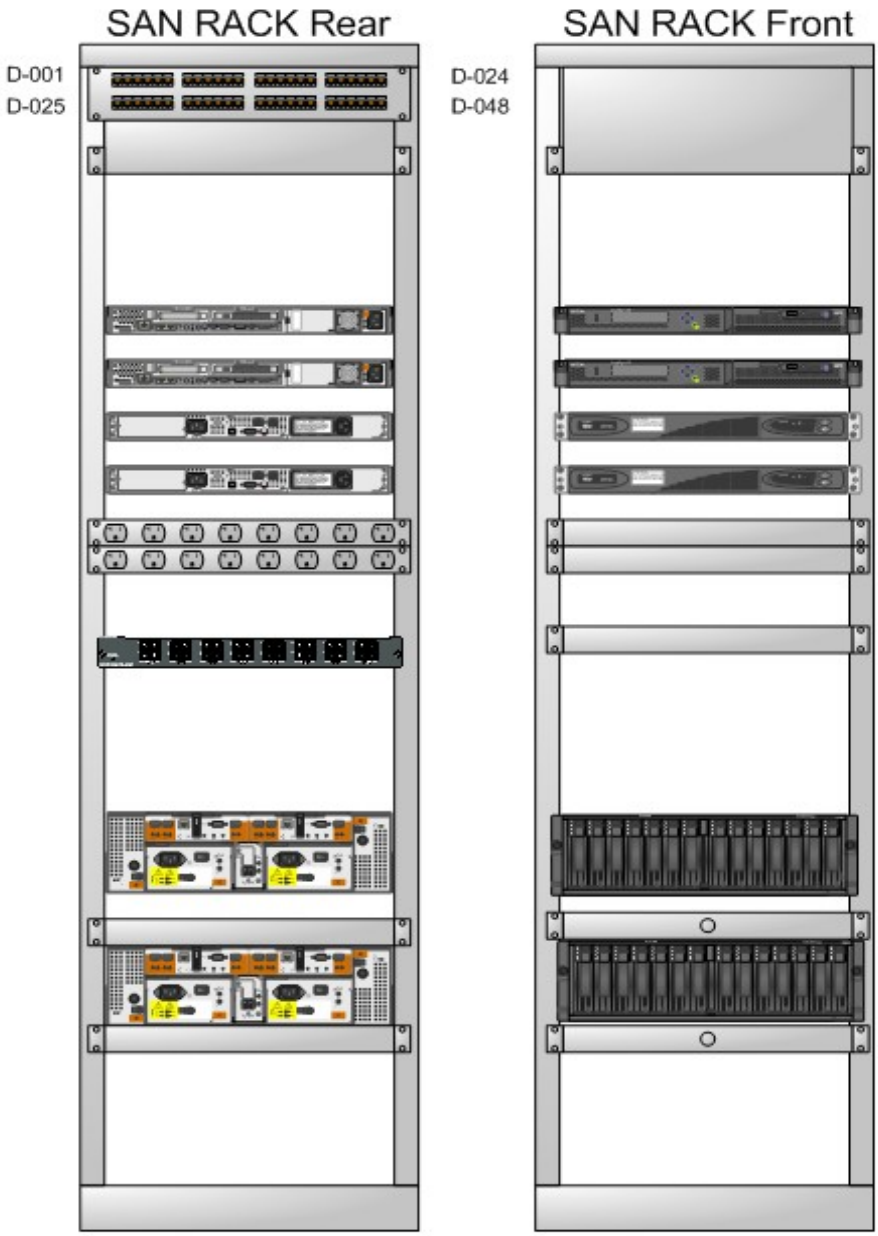



Patch Panel Rack Front
Patch Panel Rack Rear
A
B
C
D
E
F


SQL Rack Rear
SQL Rack Front
A-001
A-025
A-024
A-048
Fiber Patch Panel
PRTCSQL01
PRTCSQL02
PRTCSQL03
PRTCSQL04
PRTCESX01


Security Rack Rear
Security Rack Front
C-001
C-025
C-024
C-048
PRTCVONTU01
PRTCESAFE01
PRTCAV01
PRTCACS01

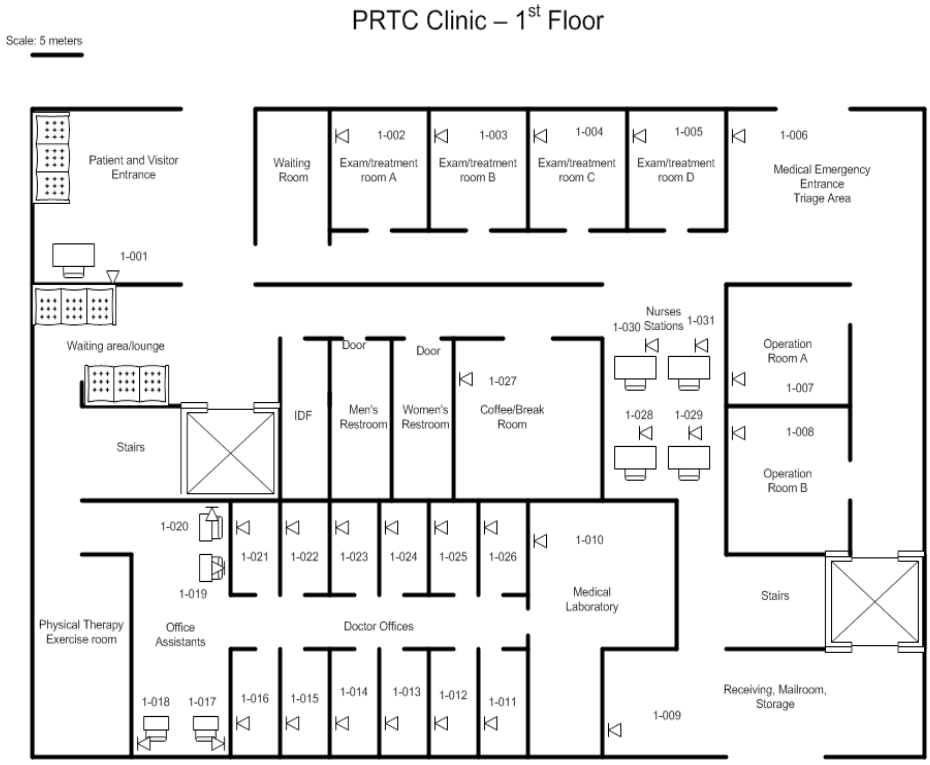

Domain/Email Rack Rear
Domain/Email Rack Front
B-001
B-025
B-024
B-048
PRTCDC01
PRTCDC02
PRTCEXCH01
PRTCEXCH02
PRTCFILE01
PRTCFILE02


SAN RACK Rear
D-001
D-025
SAN RACK Front
D-024
D-048

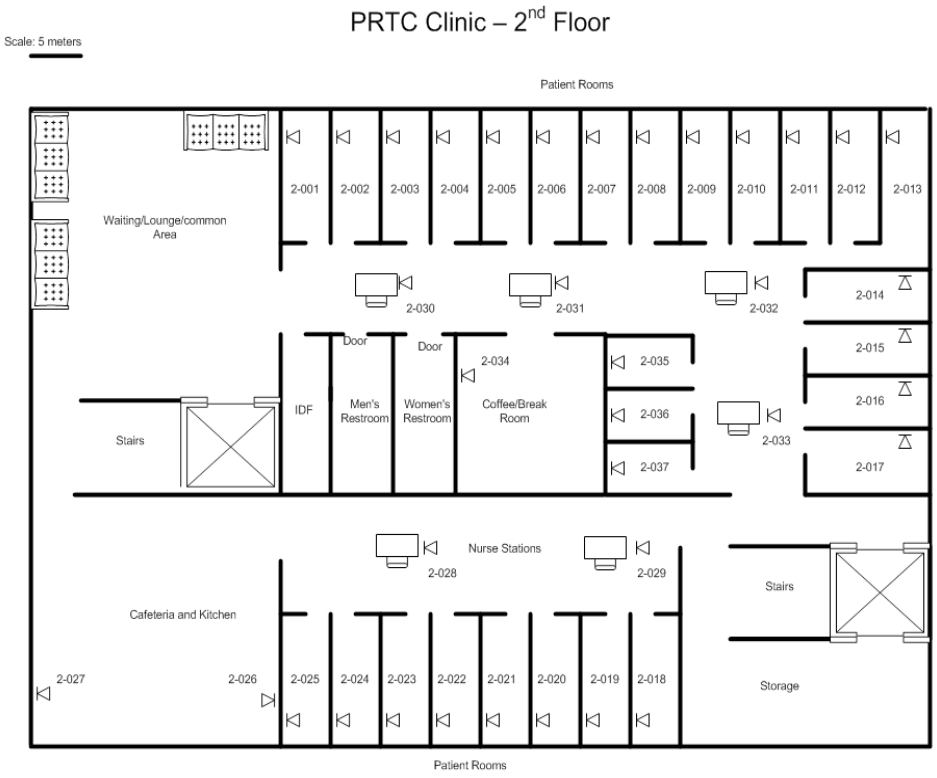
4.8.3. Floor Network Jack Locations

The following diagrams show the network jack locations for the network cable pulls. The Triangle shapes indicate a network jack and the number indicated the corresponding IDF patch panel number

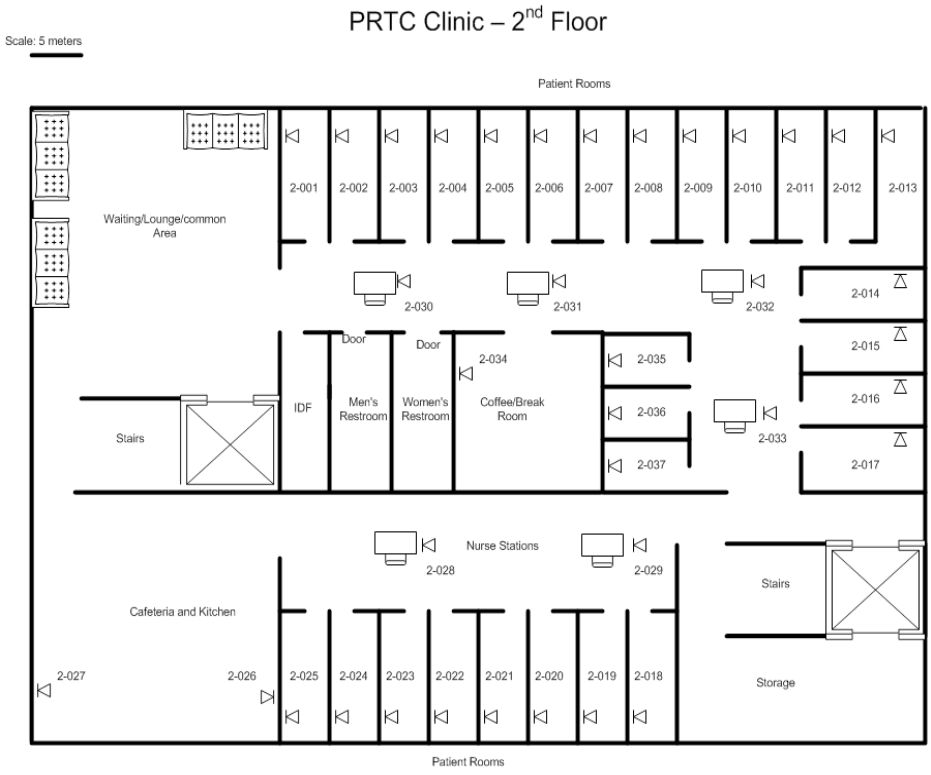
4.8.3.1. First Floor



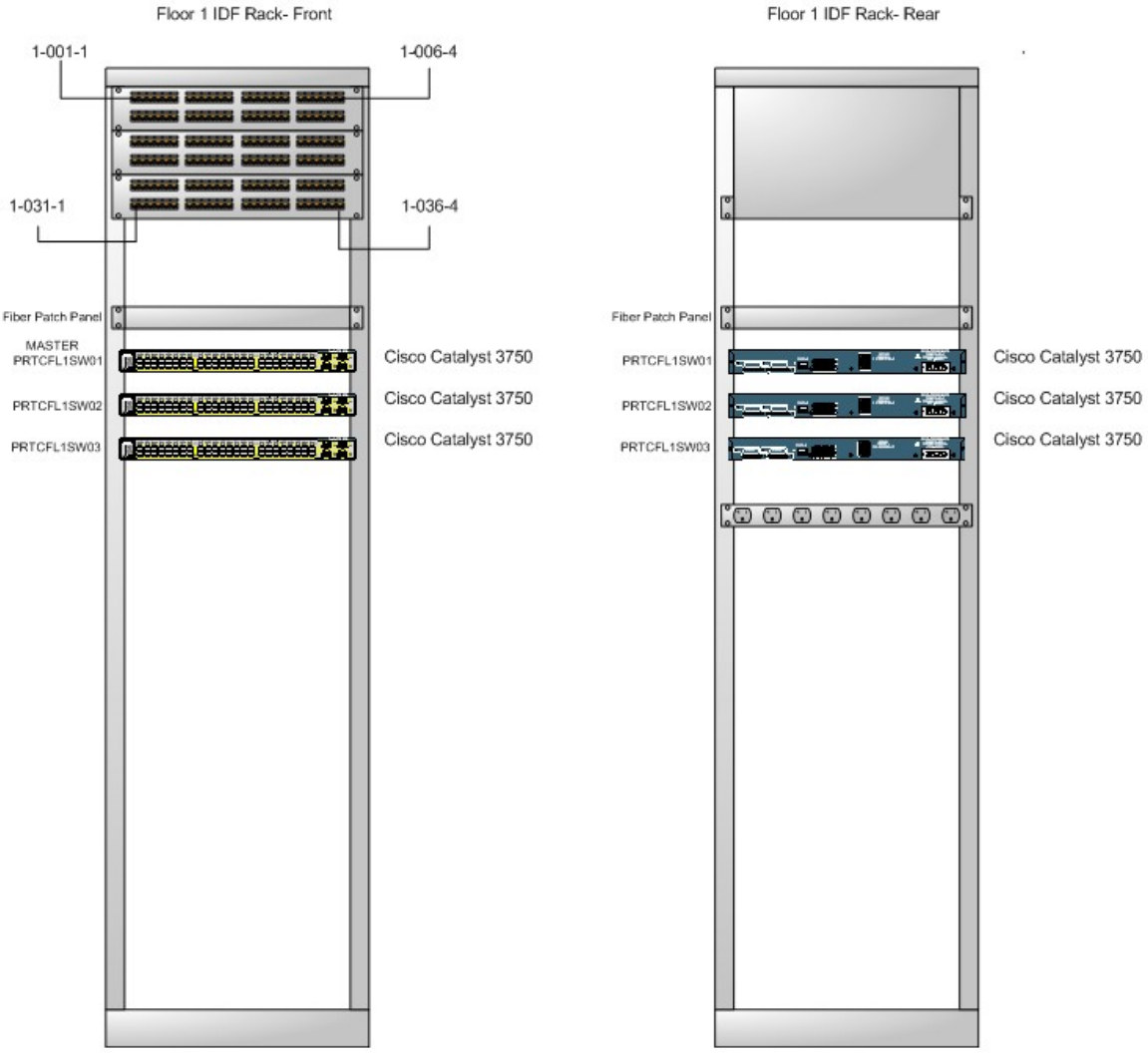
4.8.3.2. Second Floor

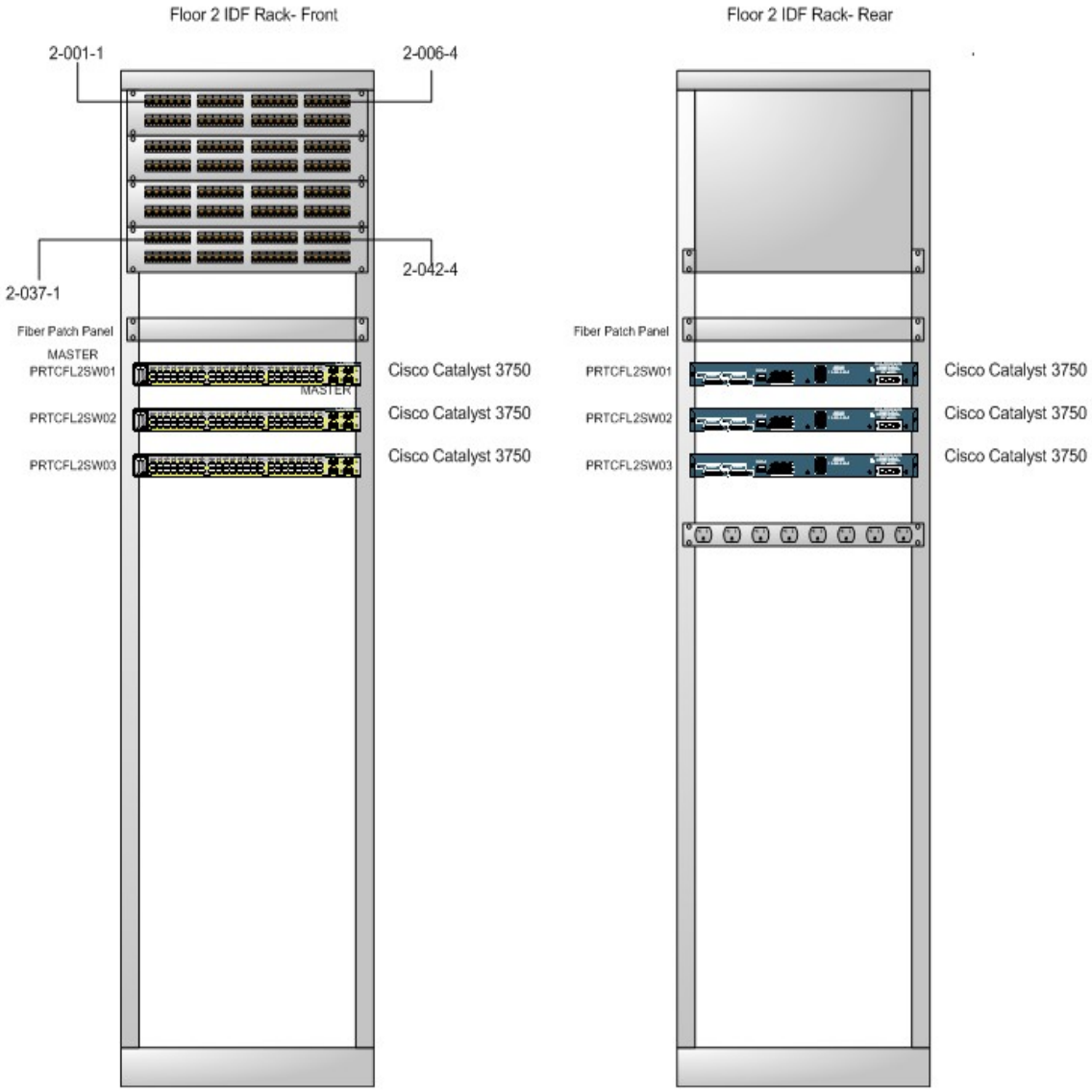


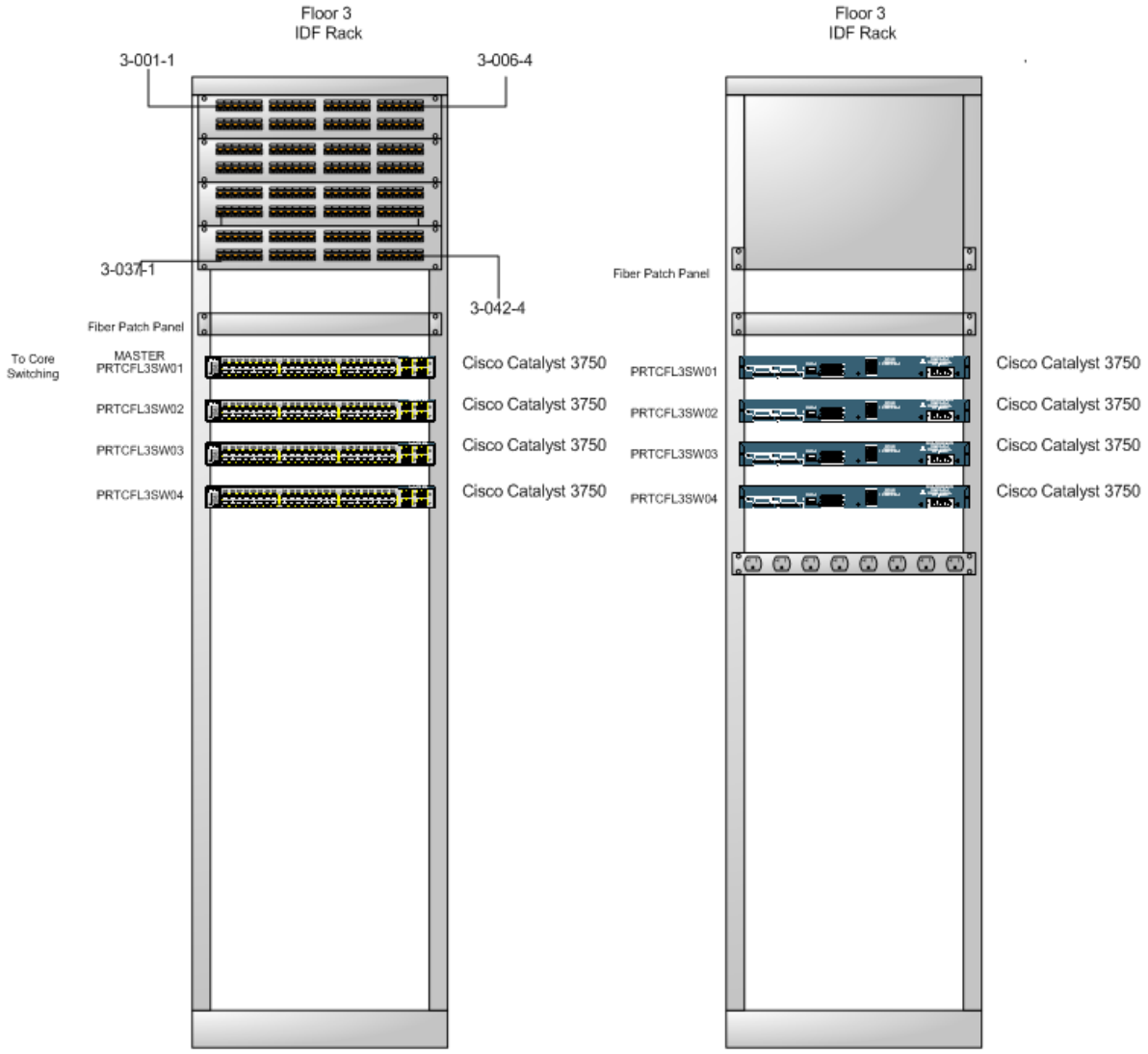
4.8.3.3. Third Floor



4.8.4.IDF Closets




Floor 2 IDF Rack- Front
2-001-1
2-006-4
2-037-1
2-042-4
Fiber Patch Panel
MASTER
PRTCFL2SW01
MASTER
PRTCFL2SW02
PRTCFL2SW03
Cisco Catalyst 3750
Cisco Catalyst 3750
Cisco Catalyst 3750
Floor 2 IDF Rack- Rear
Fiber Patch Panel
PRTCFL2SW01
PRTCFL2SW02
PRTCFL2SW03
Cisco Catalyst 3750
Cisco Catalyst 3750
Cisco Catalyst 3750


Floor 3
IDF Rack
3-001-1
3-006-4
3-037-1
3-042-4
Fiber Patch Panel
To Core Switching
MASTER PRTCFL3SW01
PRTCFL3SW02
PRTCFL3SW03
PRTCFL3SW04
Cisco Catalyst 3750
Cisco Catalyst 3750
Cisco Catalyst 3750
Cisco Catalyst 3750
Floor 3
IDF Rack
Fiber Patch Panel
PRTCFL3SW01
PRTCFL3SW02
PRTCFL3SW03
PRTCFL3SW04
Cisco Catalyst 3750
Cisco Catalyst 3750
Cisco Catalyst 3750
Cisco Catalyst 3750

4.9. Doctor Access

The way the facility is designed, doctors will have to move from floor to floor to visit patients and to their offices. This movement creates a problem when the doctors need access to information about patients and other vital information at all times. The way this is being handled to ensure security is by having each doctor carry a tablet pc that will be able to access the network in each doctor's office and in each patient room. Each patient room and each doctor office will be equipped with a docking station that will be physically plugged into the network. When a doctor needs to move all he/she will have to do is undock their tablet and then dock it in the room they are going into. This brings up a few security risks; one being that patient rooms will have access to the network and the portability of data can cause data leakage if lost or stolen.

4.9.1. Tablet PC's

HP tablets will be purchased for each of the 20 doctors in the clinic. The HP TC4400 has the following features:

- 2.0GHz Intel Core 2 Duo Processor
- 1GB RAM
- 80GB Hard Drive
- 10/100/1000 Ethernet
- WLAN 802.11a/b/g
- Bluetooth 2.0 EDR
- Fingerprint Reader
- 12.1" TFT Display
- Microsoft Windows XP Tablet
-

4.9.2. Security

4.9.2.1. Encryption SafeBoot

The tablets will be able to access network data and therefore needs to be encrypted. SafeBoot will be supplying the much needed security with pre-boot dual authentication using both known passwords and physical RSA keys with changing numbers. The RSA key will also provide an added layer of support due to SafeBoot supporting digital certificates that are stored on the key and used for more authentication security.

4.9.2.2.

4.9.2.3. Sticky MAC

Patient rooms having network access can pose security threats because when the doctor is not in the room there is an open network jack that anyone can plug into and potentially steal data. This will be secured using Stick MAC's provided by Cisco in their IOS. A range of MAC addresses will be assigned to switch ports that will only allow those MAC addresses to send and receive information. If an unknown MAC address is plugged in, the port on the closet IDF switch will shutdown and go into restrictive mode.

4.10.Recommendations

4.10.1.Staffing

This new network infrastructure will be an enterprise solution to help PRTC's business needs for many years to come. Bringing all of this new technology and equipment causes some challenges for the company. IT staffing needs have to be taken into consideration before this new network can be up and running. Staff needs to be familiar with Microsoft and Cisco products; having installation, troubleshooting, and maintenance experience is a definite necessity. At least ten to fifteen people need to be hired on to take on the responsibility of supporting the network and to perform maintenance and updates.

4.10.2.Training

As staff is brought on to handle network challenges the company should consider having trained staff with numerous certifications. At least one person must be certified as a Cisco Certified Professional, and at least two people must be certified as Cisco Certified Network Associates. Cisco training is available through different camps ranging in price with an average of $2000 per week. Microsoft certifications should be held by some employees as well to support and maintain the Microsoft Server environment. Microsoft training can be taken as camps as well with the same price ranges.

5. IP Addressing

5.1. Overview

The following Matrices demonstrate how IP addresses will be distributed amongst devices on PRTC's network. IP Addresses allow devices on the network to uniquely identify one another on a network.

5.2. IP Address Matrices

Hardware	Server Name	Interface ETH0/0	Interface ETH0/1	Subnet Mask	Default Gateway	DNS	Secondary DNS
Raritan KX2-232	PRTCKVM01	172.16.0.4	172.16.0.24	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
Raritan KX2-232	PRTCKVM02	172.16.0.5	172.16.0.25	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCDC01	172.16.0.2	172.16.0.22	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCDC02	172.16.0.3	172.16.0.23	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL580 G5	PRTCSQL01	172.16.0.6	172.16.0.26	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL380 G5	PRTCSQL02	172.16.0.7	172.16.0.27	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL380 G5	PRTCSQL03	172.16.0.8	172.16.0.28	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL380 G5	PRTCSQL04	172.16.0.9	172.16.0.29	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL580 G5	PRTCESX01	172.16.0.10	172.16.0.30	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCEXCH01	172.16.0.11	172.16.0.31	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCEXCH02	172.16.0.12	172.16.0.32	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCFILE01	172.16.0.13	172.16.0.33	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCFILE02	172.16.0.14	172.16.0.34	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCVONTU01	172.16.0.15	172.16.0.35	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCESAFE01	172.16.0.16	172.16.0.36	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
HP Proliant DL360 G5	PRTCAV01	172.16.0.17	172.16.0.37	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
VMWare VM	PRTCBADGE01	172.16.0.18	172.16.0.38	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
VMWare VM	PRTCTIGER01	172.16.0.19	N/A	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
VMWare VM	PRTCLOG01	172.16.0.20	N/A	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
Cisco ACS	PRTCACS01	172.16.0.39	172.16.0.40	255.255.255.0	172.16.0.1	172.16.0.2	172.16.0.3
Cisco 6509 Switch	PRTCCORESWTCH01	172.16.0.1		255.255.255.0	172.16.0.59	JPTelco	
Cisco 3750 Stack FL1	PRTCFL1SW01-03	172.17.0.1		255.255.255.0	172.16.0.1	172.16.0.2	
Cisco 3750 Stack FL2	PRTCFL2SW01-03	172.18.0.1		255.255.255.0	172.16.0.1	172.16.0.2	
Cisco 3750 Stack FL3	PRTCFL3SW01-04	172.19.0.1		255.255.255.0	172.16.0.1	172.16.0.2	
						172.16.0.2	

VLAN NAME	Description	Network	Subnet			
VLAN101	PC Vlan	172.XXX.1.0	255.255.255.0	172.16.0.59	172.16.0.2	
VLAN102	Printer Vlan	172.XXX.2.0	255.255.255.0	172.16.0.59	172.16.0.2	
VLAN103	Optional Phone Vlan	172.XXX.3.0	255.255.255.0	172.16.0.59	172.16.0.2	
VLAN104	IT Vlan	172.16.1.0	255.255.255.0	172.16.0.59	172.16.0.2	
VLAN105	Server Vlan	172.16.0.0	255.255.255.0	172.16.0.59	172.16.0.2	

DHCP Server	Scope	Start Address	End Address			
PRTCDC02	172.17.1.0	172.17.1.10	172.17.1.250	172.16.0.59	172.16.0.2	
PRTCDC02	172.18.1.0	172.18.1.10	172.18.1.250	172.16.0.59	172.16.0.2	
PRTCDC02	172.19.1.0	172.19.1.10	172.19.1.250	172.16.0.59	172.16.0.2	

The following matrix continues the IP Addressing scheme by displaying the IP addressing scheme for the WAN devices:

Hardware	Device Name	Interface FE0	Interface FE1	Interface FE2	Default Gateway	Routing
Cisco ASA 5510	PRTCASA01	172.16.0.52/24	172.16.0.54/24	172.16.0.50/24	172.16.0.59	Static
Cisco ASA 5510	PRTCASA02	172.16.0.53/24	172.16.0.55/24	172.16.0.51/24	172.16.0.59	Static
Cisco Catalyst Express CE 500G	PRTCCE01	Int VLAN0: 172.16.0.56/24			172.16.0.59	Static
Cisco ISR 3845	PRTCRTR01	172.16.0.60/24	172.16.0.57/24	NM T3/E3: 100.1.1.1/24	JPTelco	Static
Cisco ISR 2811	PRTCRTR02	172.16.0.59/24	172.16.0.58/24	NM T3/E3: 100.1.1.2/24	JPTelco	Static

6. Physical Security

6.1.Overview

This documentation will address the issues of physical security, and the implementation wherein physical access from the perimeter of the building (e.g., main entry points) to the accessibility once inside the building to specific floor levels (e.g., elevator and stairways), to specific rooms that are set up via proximity and smart card access, and security levels. This pertains to keeping specific secure areas, deemed by Paul Recovery and Treatment Center, from being accessible from people such as employees, patients, guests/visitors, and unnamed parties (e.g., deliveries). Specific sections of this document will give definitions of what key words mean and pertain to.

- The following criteria is key in accessibility and security levels:
- What is deemed a secure area?
- What equipment is in a given room?
- Who has access to what equipment?
- What purpose is the room for?
- What are the risks involved with entry into the room?
- How is the room monitored?
- What safety measures are in place in the given room?
- What compliances are necessary for the room?
- With these criteria in mind, we can shape the idea of physical security and set specific rules wherein access and safety are addressed?

6.2.Physical Security Concerns

6.2.1.Perimeter Entry

This section pertains to the actual physical access of the building via perimeter entries, given floor level, and specific rooms. The physical entry of given locations to and within the building are addressed by access levels. These access levels are what are designed to give each person within the building, if they are granted access, specific rules in which they are allowed to enter levels and rooms.

The following are a list of definitions that pertain to entry. These definitions may be relevant within other sections of this document, and if they are, it will be noted and referred back to this list:

- Physical Entry: This is defined as a person's ability to physically enter a specific location via manual or assisted power.
- Perimeter Entries: These are doors and/or windows that will allow access into the building itself from outside the facility.
- Floor Level: This facility has 3 stories, which equate to 3 floors that people

are able to access via stair ways or elevator.

- Rooms: A location within, or inside the building that has at least one entry way (e.g., doorway) and at a minimum of 3 walls. The reason the definition pertains to having at least 3 walls, is that some examination rooms may have a curtain access with walls dividing other examination rooms from each other. Examples of rooms are: offices, examinations rooms, operating rooms, pharmacy, physical therapy room, and conference/meeting rooms.
- Access Level: This pertains to the security rules in place for accessing the building from the perimeter (see Perimeter), specified floor level (see Floor Level) and rooms (see Rooms). This is either done via security device (e.g., proximity reader or remote desk unlocking mechanism) or by traditional key and lock. Specific security rules are set for each security device, and access to the traditional key and lock are mandated by the physical security policy (see Physical Security Policy, section x).
- Elevator: A mechanical means of moving between floors (see Floors). Because the building is 3 stories in height, a hydraulic mechanism is powered and elevates a platform from underneath. The system is integrated by a security system that will only allow specific access levels (see access levels). The elevators are not to be used in the case of an emergency as stated by HIPAA, and city, state, and federal laws.
- Stairway: This is a physical means of walking between floors (see Floors). They also are secured by devices that will determine access level (see Access Level) and allow entry from the stairs to specific floors in which entry is granted.

6.3.Designated Access Area

The following is a list and definition of specific rooms that relevant to referencing security access levels. These definitions are broken down into floor levels.

6.3.1. First Floor

- Patient/Visitor Entrance: This refers to the main entry way that a person passing through from the outside perimeter into the building that has a front desk.
- Lounge: This is a room for guests, visitors, and patients that are awaiting treatment, or escort for visiting other patients, or business.
- Coffee/Break Room: This is a place that employees are allowed access to for the purpose of taking sanctioned breaks, and is not allowed access by non-employees.
- Waiting Room: This is designated for those people waiting within the emergency medical wing.
- Restrooms: Male and Female variants.

- Treatment Room: These are rooms that are reserved for medical examinations and treatment.
- Miscellaneous Storage Closet: This is a closet that holds miscellaneous supplies and also houses the IT Equipment Closet.
- IT Equipment Closet: Is located within the Miscellaneous Storage Closet. This houses technology equipment such as local area network switches and routers and cabling.
- Physical Therapy: This is a room that is used for conducting physical therapy on patients.
- Offices: These are rooms specific for doctors to use for their work when not seeing patients.
- Medical Laboratory: This is the onsite laboratory that also houses the pharmacy.
- Mailroom: This is the designated spot for the receipt of any postal service or deliveries.
- Operating Room: This is designated for surgical operations.

6.3.2.Second Floor

- Lounge: This is a room for guests, visitors, and patients that are awaiting treatment, or escort for visiting other patients, or business.
- Coffee/Break Room: This is a place that employees are allowed access to for the purpose of taking sanctioned breaks, and is not allowed access by non-employees.
- Restrooms: Male and Female variants.
- Miscellaneous Storage Closet: This is a closet that holds miscellaneous supplies and also houses the IT Equipment Closet.
- IT Equipment Closet: Is located within the Miscellaneous Storage Closet. This houses technology equipment such as local area network switches and routers and cabling.
- Patient Rooms: These rooms are designated for the treatment of patients that require assistance that last longer than a typical visit.
- Cafeteria and Kitchen: This is the designated eating spot for employees, guests/visitors, and patients that are not ambulatory and wish something other than the food delivered to the rooms.
- Storage: This is a room designated for more supplies (e.g., medical) than what the miscellaneous storage room would allow or require.

6.3.3. Third Floor

- Reception: This is a room for patients or visitors on business that require speaking to the clerical/administration.
- Coffee/Break Room: This is a place that employees are allowed access to for

the purpose of taking sanctioned breaks, and is not allowed access by non-employees.
- Restrooms: Male and Female variants.
- Miscellaneous Storage Closet: This is a closet that holds miscellaneous supplies and also houses the IT Equipment Closet.
- IT Equipment Closet: Is located within the Miscellaneous Storage Closet. This houses technology equipment such as local area network switches and routers and cabling.
- Meeting Rooms: These rooms are designated for the purpose of conferencing and meetings.
- Offices: Used for the administration staff to conduct business.
- Cubicles: Not necessarily a room, but houses clerical and operational staff.
- Computer Operator and IS support: This is a designated place for the technical support staff, and general IT needs.
- Data Center/Computer Room: This houses the main data center including the servers, routers, switches, additional system resources, and spare equipment.
- Storage: This is a room designated for more supplies (e.g., clerical, administrative, and IT) than what the miscellaneous storage room would allow or require.

6.4.Access Points

These are designated entry and exit points that allow access to and from the building, as well as within the building. The following is a list of access points, as well as, the controls (see Equipment) that are in place that will allow access. These are also designated by floor levels:

6.4.1.First Floor

- Main Entrance: This is allows access from the perimeter to the interior. This entrance is equipped a with an integrated proximity/keypad reader that will allow entry for those with either a proximity reader or a pin number. It is also able to be unlocked by a remote panel located at the front desk. This desk would be occupied by a receptionists and a member of the security team. It is emergency rated for egress to allow automatic unlocking if an emergency alarm is set off. It is also set for a man trap if a specific security alarm code is sent to the unit via security software.
- Emergency Room Entrance: This allows direct access to the emergency and triage rooms. This entrance is equipped a with an integrated proximity/keypad reader that will allow entry for those with either a proximity reader or a pin number. It is also able to be unlocked by a remote panel located at the nurses' station desk. This desk would be occupied by a

various nurses and a member of the security team. It is emergency rated for egress to allow automatic unlocking if an emergency alarm is set off. It is also set for a man trap if a specific security alarm code is sent to the unit via security software.

- Mailroom Entrance: This allows direct access to the shipping and receiving room. This entrance is equipped a with an integrated proximity/keypad reader that will allow entry for those with either a proximity reader or a pin number. It is also able to be unlocked by a remote panel located at the shipping clerk desk. This desk would be occupied by a stationed member of the shipping and receiving team. It is emergency rated for egress to allow automatic unlocking if an emergency alarm is set off. It is also set for a man trap if a specific security alarm code is sent to the unit via security software.
- Shipping and Receiving: This room has perimeter entry as stated above and access to the hospital via a doorway and elevator. The doorway is accessible via proximity/keypad reader on either side of the doorway since it does allow entry directly into the emergency room, and visa versa. The elevator has its own access control inside as stated previously.
- Lounge Entry: This entry is also tended by the front desk station. This allows access to the lounge area, stairway, and elevators. The hallway that is accessible is also the restrooms for the main level.
- Miscellaneous Storage Closet: This is accessible by proximity/keypad reader, and holds basic medicinal and cleaning supplies. This also houses the IT closet.
- IT Closet: This is accessible by the miscellaneous storage closet via proximity/keypad reader. This would have a different access level than the main storage closet. It holds any IT networking, switching, cabling and any spare hardware that is necessary for the floor.
- Restrooms: Not secured. They are the facilities for the floor.
- Coffee/Break Room: This is a room specifically for employees to take breaks. It is accessible via proximity reader.
- Operating Rooms: These are allowed access via proximity/keypads. This will allow a member of the medical staff to open the door for the surgical teams that are already prepped and scrubbed for surgery to avoid contamination when entering.
- Treatment Rooms: These rooms would have a standard key lock, as well as a proximity reader that would allow the door to be unlocked during specific hours of the day, or changes be made through the security administration software.
- Stairways: These are allowed to be entered, but the second and third floors have a proximity/keypad readers that will allow access to those with the proper security levels. The doors are rated for egress in case of emergency

and are automatically unlocked if the proper alarm signal is sent.

- Elevators: These allow access between floors of the facility. They have a proximity/keypad reader that will allow specific security levels to access specific floors. There are two such elevators in the building. One is rated for passengers and one is rated for freight, which can include patients, equipment and oversized/weighted loads.
- Main Entry to Physical Therapy/Offices/Lab: This entry allows access to the physical therapy room, doctors' offices, and laboratory. There has been a door added to this entrance that is allowed access via a proximity/keypad. This entry is rated for egress in the case of emergency and will be unlocked if the proper alarm code is sent to the device. It is also able to be used as a man trap in case of malicious attempts at the physical therapy room, doctors' offices, and the laboratory which also holds the pharmacy.
- Doctor Offices: These are offices for use by doctors. They are accessible by proximity readers and specific time ranges.
- Laboratory: This is the hospital lab and it also houses the pharmacy. Because of the nature of having controlled substances and biohazards, this room is controlled by a proximity/keypad reader that requires both to gain entry.

6.4.2.Second Floor

- Lounge Entry: This entry is accessible via stairway or elevator. Both have their own access controls that will allow entry into this area.
- Miscellaneous Storage Closet: This is accessible by proximity/keypad reader, and holds basic medicinal and cleaning supplies. This also houses the IT closet.
- IT Closet: This is accessible by the miscellaneous storage closet via proximity/keypad reader. This would have a different access level than the main storage closet. It holds any IT networking, switching, cabling and any spare hardware that is necessary for the floor.
- Restrooms: Not secured. They are the facilities for the floor.
- Coffee/Break Room: This is a room specifically for employees to take breaks. It is accessible via proximity reader.
- Patient Rooms: These rooms would have a standard key lock, but would be generally unlocked not to hinder medical personnel and treatment. The rooms are accessible via the lounge by proximity/keypad readers.
- Stairways: These are allowed to be entered, but the second and third floors have proximity/keypad readers that will allow access to those with the proper security levels. The doors are rated for egress in case of emergency and are automatically unlocked if the proper alarm signal is sent.
- Elevators: These allow access between floors of the facility. They have a proximity/pin pad reader that will allow specific security levels to access

specific floors. There are two such elevators in the building. One is rated for passengers and one is rated for freight, which can include patients, equipment and oversized/weighted loads.

- Storage: This is a larger storage area that is accessible via stairway and doorway. It would contain miscellaneous medical and various sundry supplies. The stairway has its own access control, and the door leading to the room is controlled by a proximity/keypad reader.
- Cafeteria and Kitchen: This room is available via the lounge area without control access. It also allows access to the patient rooms via proximity/keypad reader on either side of the door. This is due to the nature of accessing patient rooms. It is, as all doors are rated for egress in emergency situations.

6.4.3. Third Floor

- Reception Entry: This entry is accessible via stairway or elevator. Both have their own access controls that will allow entry into this area.
- Reception Area: This is the place that business visitors and/or patients will come for arranged appointments. They must be granted access to this level via access controls in the stairway or elevator. A receptionist is on station to allow visitors entry to the office area. It also holds access to the conference/ meeting rooms, as well as access to the computer operator and IS support doorway.
- Miscellaneous Storage Closet: This is accessible by proximity/keypad reader, and holds basic medicinal and cleaning supplies. This also houses the IT closet.
- IT Closet: This is accessible by the miscellaneous storage closet via proximity/keypad reader. This would have a different access level than the main storage closet. It holds any IT networking, switching, cabling and any spare hardware that is necessary for the floor.
- Restrooms: Not secured. They are the facilities for the floor.
- Coffee/Break Room: This is a room specifically for employees to take breaks. It is accessible via proximity reader.
- Stairways: These are allowed to be entered, but the second and third floors have proximity/keypad readers that will allow access to those with the proper security levels. The doors are rated for egress in case of emergency and are automatically unlocked if the proper alarm signal is sent.
- Elevators: These allow access between floors of the facility. They have a proximity/pin pad reader that will allow specific security levels to access specific floors. There are two such elevators in the building. One is rated for passengers and one is rated for freight, which can include patients, equipment and oversized/weighted loads.

- Storage: This is a larger storage area that is accessible via stairway and doorway, and also by elevator. It would contain miscellaneous administrative and non-sensitive IT supplies. The stairway and elevator has its own access control, and the door leading to the room is controlled by a proximity/keypad reader.
- Conference Rooms: These are only under a standard key lock which would be opened by the receptionist on duty. They do not require specialized access controls.
- Office Entry: This is accessible via proximity/keypad reader or remote unlocking by the receptionist. These controls also are limited by business hours.
- Computer Operator and IS Support Room: This houses the IT support staff, and is accessible through the data center, as well as access from the reception area. Both doors are accessible through proximity/keypad readers, but access to the data center has a separate code as well as is required to have both the proximity card and keypad pin number combination to gain access.
- Data Center: This houses the backbone of the information technology for the entire building. This room has two access points, one through the computer operator and IS support room, as well as a hallway that leads to the stairway and freight elevator. Access is granted through a proximity/keypad device that requires both the keypad pin number and proximity card.
- Offices: These are offices for use by specified administrative and directorial employees. They are accessible by proximity readers and specific time ranges.

6.5.Access Level Rules

This is a simple number based scheme that will allow security personnel to program the security system that is in place to allow specific people into the specified secure areas. The levels are determined by the job functionality of a staff person, and a default level reserved for guests and/or visitors. First is a list of access levels, the definitions of what the access levels pertain to, and finally the designated zones that the levels will grant access to. In the event of a job functionality that bridges two or more levels, the security system (see Equipment, Protector II) makes allowances for multiple levels, or specialized adjustments to be implemented for an individual.

The following is a list of generic access levels:

Level 0: Guest/Visitor
Level 1: Clerical Staff
Level 2: General Medical Staff

Level 3: Specialized Medical Staff
Level 4: Information Technology Staff
Level 5: Security Staff
Level 6: Administrators

6.5.1.Definition of Access Levels

- Level 0 (Guest/Visitor): This is the default level that has no privileges within the building. The party must be accompanied by an employee and the card number that is given to the guest and/or visitor is logged by the designated security personnel. (See Security Procedures)
- Level 1 (Clerical): This pertains to those employees that provide clerical support (e.g., record keeping, notifications, and billing).
- Level 2 (General Medical Staff): The job functionalities that pertain to medical support, but do not include doctors and/or specialists.
- Level 3 (Specialized Medical Staff): The job functionalities that pertain to doctors and/or specialized medical personnel (e.g., anesthesiologists, physical therapists).
- Level 4 (Information Technology Staff): The job functionalities that pertain to the service and support of information technology. Depending on their functionality their access levels may be combined with others.
- Level 5 (Security Staff): This pertains to those who provide on-site physical and law enforcement security.
- Level 6 (Administrators): This job functionality pertains to high level executives and/or building supervisors.

6.5.1.1.Specific Rules on Access Levels

As these are generic template rules, depending on the staff member, other rules may be added to their access level through the implemented support interface for the security system. This could include adding rules for specific rooms (e.g., accessing the office supplies closet:

- Level 0: This is the generic, non-programmed, proximity card. They are able to be programmed for a specific time limit for specific levels for visitors so they may gain approved access. By default these cards have no access privileges.
- Level 1: This gives access to the front entry of the building, third floor elevator and stairway, and break rooms. Individual offices are not accessible on the third floor unless additional access is granted.
- Level 2: This gives access to the front and emergency room entry ways, main medical wing on first floor, elevator and stairway access to the second floor, and break rooms on the first and second floor.

- Level 3: This gives access to the front and emergency room entry ways, main medical wing on first floor, elevator and stairway access to the second floor, and break rooms on the first and second floor. It would also grant access to the doctors' offices, physical therapy room, operating rooms and laboratory. Individual offices are not accessible on the third floor unless authorized.
- Level 4: This gives access to the front and emergency room entry ways, elevator and stairway access to the third floor, and break rooms on the first and third floor. It would also grant access to the computer operator and IS support office, storage, and third floor office area. Individual offices are not accessible on the third floor unless authorized.
- Level 5: This gives access to the front and emergency room entry ways, shipping and receiving entries, elevator and stairway access to all three floors, and break rooms on all three floors. It would also allow generalized access to all areas (e.g., storage rooms, office areas) on all three levels. Individual offices and specialized secure areas (e.g., data center) are not accessible unless authorized.
- Level 6: This would allow access to everything except the data center. This is only for the directors of the facility that would need access to the entire building. This possibly could not be used, but is deemed a right of the owners.

6.6.Equipment

6.6.1. Hartman Controls

6.6.1.1. Door Proximity Access Control Panel

This is a device that will is the communication relay for any specific information that is sent to the specific access control device.

Specifications:

AC Input	12 VAC 40VA through certified CLASS 2 CSA/UL Transformer
Battery Input	1 battery 12 V, 7Ah, supervised, provides up to 17 hours of operation
Enclosure	28.6cm x 38.75cm x 7.7cm (11.25" x 15.25" x 3")
Weight	2.4 kg (5.4 lbs)
Operating Temperature	From 0 ºC to +50º C
Reader Technology Supported	Wiegand, proximity, biometric, bar code,magnetic, integrated keypad and others
Panel to Panel wiring	1200 meters (4,000 feet) - (Category 5)
Panel to Reader Wiring	152 meter (500 feet) – (6 conductor 22 AWG overall shield)
Auxiliary Power	12VDC @ 200mA max
Reader Power	12VDC and 5VDC @ 250mA max each
Inputs	Dry contact closures N/O and N/C
Relay Outputs	8 outputs @ 6 A max load each
Communications	RS232 and RS485, 19,200 baud
Network autonomy	Distributed data and processing

6.6.1.2.HCEC-8 Option

This device allows specific access to floors accessible by an elevator system.

Specifications:

- Floor control
- With Or without button sensing
- Battery back-up Circuitry
- On board firmware clock
- Supports Weigand 26 bit format (others on special request)
- 60,000 user on board storage
- 2000 event on board storage
- Power Requirements: 16.5VAC @ 40VA transformer
- Option Stand By battery 12VDC 7.0Ah
- Relays are Form C contact rated at 10A 125VAC
- On board LED to indicate communications, Active Relays, AC source, as well as the state of the inputs.

6.6.1.3.RF101 Keypad/Proximity Reader

- This device will allow a person to
- Specifications:
- Dimensions: 3.4" x 3.84" x 0.87" or 87mm x 100mm x 23.5mmUp to 4"(10cm) Read Range: Up to 4"(10cm) Read Range
- Built in 12 numeric keypads
- User format available
- 26 bit Wiegand format output
- PSK modulation
- Back lighting on keypad
- 3 LED indicators
- Beep Tones
- High durability and reliability

6.6.1.4.RF10 Proximity Reader

Specifications:

- Dimensions: 1.82" x 4.81" x 0.87" or 46mm x 122mm x 23mm
- Read Range : Up to 4"(10cm)
- Wiegand format output
- PSK modulation
- 100% Weather Proof
- Dual reading tech reader/Active and Passive
- Solid Epoxy potted
- Reverse power polarity protection

6.6.1.5.RS485 to TCP/IP Converter

This device allows the security system to communicate via network protocols.

6.6.1.6.Badge Type Proximity Card

This is the literal “key” to the majority of the access control system. It allows entry as long as the owner is within 4” of the proximity device.

- Dimensions: Regular prox: 2.13" x 3.38" x .07" or 54mm x 86mm x 1.7mm
- Graghics printable prox: 2.13" x 3.38" x .03" 54mm x 86mm x .8mm
- Technology: Passive proximity @ 125 KHz Security:
- Up to 72,058 trillion unique codes Long life
- No direct contact
- No battery
- Capable of an infinite number of reads to formats
- Custom programmable Wiegand format up to 56 user definable bits
- Prox-Linc cards and tags are warranted for life against defects in material and workmanship

6.6.2.AlarmLock

6.6.2.1.RRPM1200P AK Magnetic Lock with Remote Control

Specifications:

- Dimensions: 10.5" Long X 2.875" Wide X 1.5" Deep
- For glass and aluminum doors
- 1200 pound holding force
- Unique passage mode (the ability to be put in an unlocked state) from a remote
- Unique quick lock mode (the ability to be instantly locked when in the passage mode) from a remote
- Door ajar feature
- Hard wire a request to exit switch or add a card reader!
- Will work at distances up to 35 feet on the outside of protected area and 15 feet inside.
- Comes with a power supply ready to plug in

6.7.Training

Training is set up into the following three categories with definitions:

- General: This is the generic user that is shown how to use the system to enter the building and access their approved areas.
- Trainer: This is a user that would be approved to train the general user category in the operation of the security system, but may not physically program the system.
- Programming: This is the action of actually programming the security system to assign the specific access levels to the proximity cards, assign keypad pin numbers and designate any specialized security and emergency codes that would require the system to respond in a specific manner (e.g., fire and man trap procedures).

The following are the required procedures to train the two categories in using the security system:

6.7.1.General

This would require properly authorized and trained security personnel (e.g., trainer) to give the basics of the system use. The requirements that the general user category would need is listed in the following:

- Procedures on obtaining an authorized proximity card (e.g., getting their card, getting the picture taken for their id that is placed on the proximity card)
- Procedures on obtaining an authorized keypad code.
- Explanation of their authorized access, limitations, and documentation, with

signature of recipient, of accepting and receiving their proximity card and keypad personal identification number.

- The documentation that the general category user receives will contain the following:
  - Procedures on how to enter the building using the proximity card.
  - Procedures on how to enter the building using the keypad functionality.
  - Procedures on how to access their authorized locations within the building.
  - Procedures on how to report a missing or stolen proximity card.
  - Procedures on changing of access levels.
  - Procedures on proper emergency protocols.
  - Procedures on visitors or guests.

6.7.2.Trainer

This would require authorized security personnel to go through and understand the general category training, and have higher authorization than a generic user. Generally this would be an on-site high ranking or specially designated security guard. They would have knowledge of the system and some basic programming knowledge of the system. That information would be gained from the programmers. The following requirements would be needed to be able to be considered a trainer:

- Understanding of security and safety procedures.
- Part of the security personnel team.
- Undergo an approved training program that would explain and teach the person in the matters of training people.
- Excellent understanding of the general category training procedures.
- Excellent understanding of the building layout, design and purpose.
- Excellent written and vocal skills.
- Undergone general category training.
- Guide the general category personnel through gaining their id badges/proximity cards and keypad pin numbers.
- Excellent record keeping that will adhere to facility requirements.

6.7.3.Programmer

This is a special position that requires the person to have undergone proper training in the system itself. The following are required for a programmer of the security system:

- Full understanding of the design and layout of the security system.
- Knowledge of Networking.
- Training by approved dealers of the manufacturer.
- Quick procedural response times.
- Excellent technical writing skills
- Able to train the trainer categories.
- Able to adjust to system and authorization requirements.
- Ability to set procedures for time and access limited visitor keypad pin or proximity cards.

6.8.Pricing

6.8.1.Overview

The following is a pricing matrix for the physical security of PRTC.

6.8.2.Pricing Matrix

Retailer	Product Type	Manufacturer	Model	Price	Quantity	Total
Access Control Hardware						
The Keyless Lock Store	Hartmann Controls 4 Door Proximity Access Control Panel	Hartman	N/A	$2,790.00	1	$2,790.00
The Keyless Lock Store	Hartmann Controls 8 Door Proximity Access Control Panel	Hartman	N/A	$4,490.00	9	$40,410.00
The Keyless Lock Store	Hartmann Controls RF 101 Keypad/Proximity Reader	Hartman	N/A	$439.00	8	$3,512.00
The Keyless Lock Store	Hartmann Controls RF 10 Proximity Reader	Hartman	N/A	$229.00	30	$6,870.00
The Keyless Lock Store	AlarmLock Magnetic Lock w/ Remote Control	Hartman	N/A	$559.00	36	$20,124.00
Total						$73,706.00

7. Virtual Security

7.1.Overview

The following section contains the software and hardware needed to fend off virtual threats to PRTC's network. Here you will find various solutions to secure the network and keep data integrity intact.

7.2.Anti- Virus, Spam, Spyware

In order to reduce the risk of viruses, Trojans, unsolicited commercial email (spam), and spyware, we have selected McAfee's Total Protection for Enterprise. This software has several modules that provide the protection against these types of threats. The following modules are provided by this software:
Centralized management console: enables the IT staff to deploy, manage and report across physical or virtual desktops, laptops, and severs.
Desktop and file server anti-virus: provides comprehensive protection to guard against bots, viruses, worms, Trojans, and targeted hacker attacks.
Desktop anti-spyware: provides comprehensive protection to guard against spyware, adware, and keystroke loggers.

Desktop host intrusion prevention: provides signature and behavioral-based host intrusion protection which secures desktops against zero-day and known threats.
Desktop firewall: provides and additional layer of protection against viruses, worms, hackers, spyware, and adware by blocking or allowing network traffic over specified communication ports.

Email server anti-virus and anti-spam: provides email protection which stops unsolicited commercial email (spam) and viruses before they invade the network, and eliminates inappropriate content that may cause legal liabilities.

Implementation of the McAfee Total Protection for Enterprise will be as follows. The centralized management console will be installed on server PRTCAV01. This console will be used to deploy new installations of the McAfee software as well as the updated virus definition files and any product upgrades. The console will provide the ability to remotely manage the various settings associated with the software, and to gather reports for use in risk assessments and evaluations. The Email server anti-virus/spam module will be installed directly on the email server. The remaining modules will be installed on all systems – desktops, laptops, and servers.

McAfee Total Protection for Enterprise is sold as a per seat license. The cost per seat license is $118.08. This includes 3 years of 24x7 support, maintenance, software subscription, updates, and upgrades. At the time of this writing, we estimated 60 licenses which brings the total for this implementation to $7,084.80.

7.3.Network Authentication, Auditing, and Scanning

7.3.1.Authentication

The PRTC network will be protected from unauthorized access with the Cisco Network Admission Control 3310 server. The Cisco NAC 3310 allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless and remote users and their machines prior to allowing users onto the network. Since users and their devices are recognized at the point of authentication, malicious code that may be present is prevented from causing damage to the PRTC network. The Cisco NAC 3310 evaluates machines to see if they are compliant with security policies which can vary by user type, device type or operating system.

These security policies are enforced by blocking, isolating and repairing non-compliant machines. This is accomplished by redirecting the non-compliant machines to a quarantine area where remediation occurs at the discretion of the network administrator. The connection methods supported by the Cisco NAC 3310 are LAN, WLAN, WAN, or VPN. The security policies for this device are updated automatically, providing the latest and most up to date protection for the PRTC network. The Cisco NAC 3310 provides a Web-based management console that allows administrators to define the types of scans required for each role as well as the related remediation packages necessary for recovery.

The implementation of the Cisco NAC 3310 is as follows. The passing traffic mode will be setup as a real IP gateway. The physical deployment model will be centrally located in the network. The client access mode is going to be Layer 3. The traffic flow model will be out-of band which mean that the Cisco NAC 3310 is only inline during authentication, posture assessment and remediation. This is a self-contained device and does not need additional hardware. It will be rack mounted in the data center.

The cost for the Cisco NAC 3310 is $5,679.34. The SMARTnet extended service agreement for 3 years is $2,776.02. The total cost to implement the Cisco Network Admission Control 3310 server for a period of 3 years is $8,455.36

7.3.2.Auditing and Scanning

We have chosen the GFiLANguard Network Security Scanner software to provide auditing and scanning of the PRTC network. This software provides real-time as well as scheduled auditing and scanning of the three pillars of vulnerability management. The three pillars consist of: security scanning, patch management, and network auditing. This is done through a single integrated console which provides an efficient way to perform these tasks and reduces the total cost of ownership. GFI LANguard N.S.S. contains a database which contains over 15,000 known vulnerabilities and includes standards such as OVAL (2,000+ checks) and SANS Top 20. This database is regularly updated with information from BugTraq, SANS Corporation, OVAL, CVE, and others. Additionally, GFI LANguard keeps track of third party security applications such as anti-virus and anti-spyware to ensure that they are always up to date with the latest virus definition files and latest scanning engines. The reporting feature of this software allows the security or IT administrator to filter the results of the report for quick identification of any security vulnerabilities. Whenever possible, a web link or more information on a particular threat is provided, such as a BugTraq ID or Microsoft Knowledge Base article ID. GFI LANguard scans for open communication ports, unused local users and groups, blacklisted applications, and dangerous USB devices, wireless nodes and links. The security or IT administrator can, from the integrated console, remedy these situations which provide real-time correction of security issues. An additional feature of this software is the ability to deploy network-wide patch and service pack management. This includes custom/third party software applications.

GFI LANguard also contains an automated alerting facility that can email the security or IT administrator informing him or her of possible security threats. Finally, this software supports various operating systems and languages.
GFI LANguard will be implemented as follows. The software will be installed on server PRTCESAFE01. GFI LANguard also requires a database backend for storing network audit results. This will be installed on one of the database servers. In order for the network scans and audits to work properly, all desktops, laptops and servers will need to have their firewall settings adjusted to allow access to the necessary ports and services. This will be accomplished through Active Directory's Group Policy Objects. The communication ports that need to be open are: port 135 and one or more in the range of 1070 through 1170. The following GFI LANguard knowledge base article contains the detailed step by step instructions for performing this task: http://kbase.gfi.com/showarticle.asp?id=kbid002177

The cost for GFI LANguard is based on the number of scan-able IP addresses. Since we know that we will have at least 40 desktops and numerous severs deployed at

PRTC, we have selected the LANSS64 which will allow scanning of 64 IP addresses. The cost for the LANSS64 is $650.00. The maintenance agreement which provides support, updates and upgrades is purchased in 1 year increments at 20% of the purchase price and since we are providing a 3 year total cost of ownership, this cost is $390.00. The total investment for the GFI LANguard implementation is $ 1,040.00 for 3 years.

7.4.Data Loss Prevention

Since PRTC is in the healthcare industry, we have selected the Symantec Vontu Data Loss Prevention suite of software to protect the sensitive data that will be stored at this location. This software suite is a multi-layered, policy based application that is used for securing sensitive healthcare data. The Healthcare Solution Pack selected for this installation provides policies for Healthcare Insurance Portability and Accountability Act (HIPPA), Payment Card Industry (PCI), Sarbanes-Oxley Act (SOX), Employee data protection, Resumes, Confidential documents, Encrypted data, and Mergers and acquisitions. Vontu DLP provides end-to-end protection of data at three levels: Storage, Endpoint and Network. The Storage Data Loss Prevention discovers and protects confidential data exposed on file servers, databases, Microsoft Exchange, web servers and other data repositories. The Endpoint Data Loss Prevention discovers confidential data stored on laptops and desktops and prevents it from being copied to USB devices, burned to CD/DVDs and downloaded to local drives. The Network Data Loss Prevention monitors and prevents confidential data loss with comprehensive coverage including email, IM, Web, Secure Web (HTTPS), FTP, P2P, and generic TCP. The Vontu Enforce Platform automatically enforces data loss prevention policies with a centralized platform for detection, workflow and automation, reporting, system management and security.

Vontu DLP will be implemented as follows. Each desktop, laptop and server will have the necessary agent deployed on it to allow for scanning and reporting. The Vontu Enforce Platform will be installed on server PRTCVONTU01.

7.5.Web Security

In order to minimize any security threats that might arise from Web based searches and communications, we have selected the iPrism 10H Internet Filtering appliance. This device is a completely self-contained solution which provides a low total cost of ownership. The iPrism 10H protects employees and the network from Spyware, Malware, and Phishing attacks by blocking the sites that propagate and deliver infected applications to the organization. Additionally, the iPrism 10H blocks Instant Messaging (IM) which typically bypasses firewalls and Peer to Peer (P2P) which poses risks such as illegal file sharing of copyrighted material and even more serious, loss of sensitive or proprietary corporate data. These protocols can be

monitored and/or blocked across the entire network. Since this is a self-contained device, it contains comprehensive on-box reporting, automatic upgrades and daily URL database updates.

The iPrism 10H will be implemented as follows. Since this is a self-contained device, it will not require any additional hardware. It will be rack mounted in the data center. It will be placed at the network perimeter and positioned so that all network traffic will pass through it for filtering.

The cost for the iPrism 10H is $4,788.75. This cost includes 3 years of support, maintenance and the web filtering subscription.

7.6.Backup

We have selected the Acronis True Image Echo Enterprise Server for data backup. This software is not only traditional backup software, but also a disk imaging software as well. Some of the many features offered by this software are:

- Support for physical and virtual servers
- Full disk restoration including support for dynamic disks
- Event driven backups
- 256 bit archive encryption
- Support for a wide range of storage devices, including tape libraries
- The ability to restore images to different hardware with the optional Universal Restore agent
- 64 bit Windows support
- Backup databases while actively online
- Create bootable CD images, PXE packages, and bootable recovery media ISOs
- Live disk imaging

The ability of this backup solution to create disk images as well as the traditional full, incremental and differential backups is paramount to the safety of the PRTC data. It is also a high end disaster recovery solution because of its ability to create complete disk images. It also allows PRTC to upgrade the server hardware and restore the previous disk image to the new hardware. This is accomplished with the optional Universal Restore agent which has also been selected for the PRTC backup solution.

The Acronis True Image Echo Enterprise Server will be implemented as follows. Each server will have the software installed. The administrative console can be accessed from any one of the servers. Each backup schedule can be adjusted from the single administrative console.

The cost for the True Image Echo Enterprise Server is $41,536.00. This cost includes the Universal Restore agent and the maintenance agreements for both product for up to 3 years.

7.7.Recommended Utilities

We recommend that PRTC use Diskeeper 2008 Enterprise Server on each of its servers to eliminate hard disk defragmentation. Hard disk fragmentation can dramatically affect server disk access performance over time. Disk defragmentation is also a problem that gets exponentially worse as fragmentation increases. Diskeeper 2008 Enterprise Server can eliminate this problem with its ability to defragment on the fly - Invisitasking™. Diskeeper is compatible with Volume Shadow Copy Service (VSS) and supports native 64 bit operating systems. Diskeeper also contains Frag Shield™ 2.0 which boosts reliability and availability by automatically preventing crash-inducing fragmentation of critical system files and I-FAAST™ 2.0 (Intelligent File Access Acceleration Sequencing Technology) which automatically boosts access speeds for the most commonly used files. It also contains the Terabyte Volume Engine 2.0 which provides powerful defragmentation for high capacity and high traffic servers with disk volumes containing hundreds of thousands to millions of files. This is a complete defragmentation solution including both file and free space defragmentation. Diskeeper 2008 Enterprise Server can be centrally administered through the Diskeeper 2008 Administrator.

The implementation of Diskeeper 2008 Enterprise Server will be as follows. Each server will have this software installed. The Administrator console will be installed on the PRTCESAFE01 server. The automatic defragmentation settings will be applied through the Administrator console to complete the installation.

The cost for Diskeeper 2008 Enterprise Server is $36,629.45. This cost includes a copy for each server, 3 years of maintenance, support, upgrades, and updates, Diskeeper 2008 Administrator, and 3 years of maintenance, support, upgrades and updates.

We are also recommending Diskeeper 2008 Professional for each desktop and/or laptop as well. The advantages of this software are the same as it was explained for the servers. The installation of Diskeeper 2008 Professional on the desktops can also be centrally managed through the Diskeeper 2008 Administrator.

Diskeeper 2008 Professional will be implemented as follows. Each desktop and/or laptop will have a copy installed on the hard drive. The Administrator console will be used to adjust the defragmentation options to complete the installation.

The cost for Diskeeper 2008 Professional is $3,555.60. This cost includes the 3 years of maintenance, support, upgrades and updates.

We are also recommending the installation of Undelete Server on each server. This program guards against accidental or intentional file deletions over the network. When a file is accessed over the network, and then deleted, it is not sent to a recycle or trash bin. The file is deleted with no way to retrieve it other than being restored from backup tape. Undelete Server acts as a network recycle/trash bin. Additionally, Undelete can keep track of Microsoft Office file versions as it is being edited. This allows you to restore previous versions of your document in progress. In an effort to keep help desk calls down, an Undelete client agent can be installed which will allow users to restore their files without the help of the IT or helpdesk staff.

Undelete Server will be implemented as follows. Each server will have the software installed. Each desktop and/or laptop will have the client agent installed.

The cost for Undelete Server is $10,803.00. This cost includes a copy of Undelete for each server and 40 Undelete client agents as well as 3 years of maintenance, support, upgrades, and updates.

7.8.Cisco Secure ACS

7.8.1.Overview

Cisco Secure Access Control Server (ACS) Express is an appliance that deals with network access and device administration. To do this, the ACS appliance implements Authentication, Authorization, and Accounting (AAA) controls to administer devices, regulate users, and retain the posture of the networking environment.

7.8.2.Equipment

- Cisco Secure ACS Express Appliance 5.0 Model# CSACS-5.0-EXP-K9 – x1
- Cisco Software Application Support Model # CON-SAS-C50EXPK9 – x1

7.8.3.Configuration

Authentication: The Cisco Secure ACS Express Appliance will be configured to use our Active Directory servers PRTCDC01 and PRTCDC02 as a credential source. A credential source is a device or devices that the ACS will query for validity a user or device account on the network. All networking devices will have their AAA backend connected to the ACS using TACACS+ to allow central management of user and device accounts.

Authorization: There are a number of points where an account will require authorization. A primary example is one where a user brings in a personal laptop to connect to the clinic's network. Machine access restrictions keep a user from connecting and successfully integrating that machine with the network unless it had been previously authenticated by an administrator. It also enacts a number of other policies which are used to determine if a user account has authorization to log onto a machine at a certain time because of type of designation and what type of privileges one receives.

The ACS will be configured to restrict network access to all unauthenticated devices. It is a major security threat to allow users to bring in their questionable devices. So it will be set as a policy to not allow this type of network access. Group access is another important part to authorization. Group access will be used to restrict what machines users can and cannot access based on the group designation. An extension of that that will be in place is the time during which one can log onto a machine.

Accounting: As for administration, it provides two very powerful tools which are logging and reporting. Logging will allow the ACS to keep a log of all events deemed “interesting” by an administrator. These logs will be hosted on a Syslog server (PRTCLOG01), a machine which holds logs for all machines, which will only be available to high level Network and Security administrators. Contained in these logs will be information about authentication successes and failures, other accounting logs, and debug logs.

This version of the ACS supports a maximum of 50 AAA clients. In addition to the clients, a maximum of 350 user logons to AAA through TACACS+ (and RADIUS), are allowed for a 24 hour period starting at twelve o'clock AM.

7.9.Cisco Secure MARS

7.9.1.Overview

Given the extreme sensitive nature the work being performed in the clinic, we must be proactive in determining and neutralizing threats. It is not enough to perform logging of certain events and relying on security appliances to deal with attacks and audits expire after a period of time. New threats arise rapidly and are constantly evolving to find a way around our security policies. This calls for an addition to the PRTC security arsenal which completes the comprehensive solutions package provided by Kerberos Consulting. With that, we introduce the Cisco MARS appliance which takes an extremely proactive role in exactly what it is named for: Monitoring, Analysis, and Response.

Specifically, MARS is an appliance which identifies, isolates, and recommends removal processes (Cisco.com). It helps maintaining policy compliance within a company as well as raise the level at which PRTC is approaching regulatory compliance. The MARS appliance achieves the following:

> • Integrating network intelligence to modernize correlation of network anomalies and security events
> • Visualizing validated incidents and automating investigation
> • Mitigating attacks by taking full advantage of your existing network and security infrastructure
> • Monitoring systems, network, and security operations to aid in compliance
> • Delivering a scalable appliance that is easy to deploy and use with the lowest total cost of ownership (TCO)
>
> *Cisco.com*

MARS essentially queries the network gathering intelligence to keep an edge on security threats that may arise. Without this type of appliance PRTC's data, which will constantly be under siege by malicious users and rogue machines, will suffer loss of integrity and the network will be at extreme risk.

7.9.2.Equipment

- Cisco Secure MARS Model# CS-MARS-20R-K9 – x1

7.9.3.Configuration

With the Cisco MARS Appliance we plan to take an active role in identifying, planning, and acting on new and developing threats on PRTC's computer network. Actively polling the network and reporting on found data using actual computer security administrators can be costly in terms of time, money, and other resources. There is also the fact that even if that team were very diligent in their analysis, the amount of polling and analysis gathered by the team would be marginal in comparison to the amount gathered by data.

This appliance has must aid in the detection of new threats as well as aid in upholding company policies. We will need to configure it to use data taken from it's own polling and that from statistics gathered from other network devices and applications to create a more comprehensive analysis of the PRTC network.

Given the large impact that implementing this product will have, a number of Security Administrators will need to be trained to analyze the reports generated by the appliance, maintain the equipment, and relay any findings to other necessary individuals. This will require training for each individual designated to manage the device and information gathered from MARS.

In terms of administrative configuration there will be an AAA backend connection with ACS. There will also be local users for emergency use should the ACS (PRTCACS01) become unavailable to offer RADIUS authentication to MARS. System logs will be sent to a Syslog server (PRTCACS01). Monitoring of MARS will be provided by an SNMP server (PRTCMOM01). It will be configured to alert all security administrators of any network threats via email and SMS.

7.10.Equipment Maintenance and Replacement

7.10.1. Software

All software purchased for the Virtual Security of PRTC comes combined with support.

7.10.2. Hardware

Device	Support Model Number	Quantity	Features
Cisco ACS	CON-SAS-C50EXPK9	3	Technical Support Phone Consultation 1 Year 24x7 Support
Cisco 2811 ISR	CON-OS-2811	3	Extended Service Agreement Replacement 1 Year 8x5 Support 4 Hour Response

7.11.Pricing (Part One)

Retailer	Product Type	Manufacturer	Model	Price	Quantity	Total
ACS Appliance						
CDW.com	Access Control Server	Cisco	CSACS-5.0-EXP-K9	$3,421.99	1	$3,421.99
CDW.com	Cisco Software App Support	Cisco	CON-SAS-C50EXPK9	$1,121.99	3	$3,365.97
Total						$6,787.96
MARS Appliance						
CDW.com	Monitoring, Analysis, and Response System	Cisco	CS-MARS-2OR-K9	$5,219.99	1	$5,219.99
CDW.com	Smartnet Support	Cisco	CON-SNTE-MARS2OR	$1,859.99	3	$5,579.97
Total						$10,799.96
Anti-Virus						
	Anti-Virus	McAfee	McAffee Total Prot. For Bus	$118.08	60	$7,084.80
Total						$7,084.80
Auditing						
	Auditing	GFILANguard	GFILANguard Server	$575.00	1	$575.00
	Maintenance and Support	GFILANguard		$390.00	1	$390.00
	Network Access Control	Cisco	Cisco NAC	$5,679.34	1	$5,679.34
	Maintenance and Support	Cisco	Smartnet for Cisco ACS	$2,776.02	1	$2,776.02
Total						$8,455.36

7.12.Pricing (Part Two)

Backup						
	Backup and Recovery Software	Acronis	Acronis True Image Echo Enterprise Server	$999.00	20	$19,980.00
	Maintenance and Support	Acronis	Acronis True Image Echo Enterprise Server maintenance (3 years)	$599.40	20	$11,988.00
	Backup and Recovery Server	Acronis	Acronis True Image Echo Enterprise Server Universal Restore agent	$5,980.00	1	$5,980.00
	Backup and Recovery Restore Agent	Acronis	Acronis True Image Echo Enterprise Server Universal Restore agent maintenance (3 years)	$3,588.00	1	$3,588.00
Total						$9,568.00
Data Loss Prevention						
	Endpoint Data Integrity Support	Vontu	Vontu Data Loss Prevention suite	$25,000.00	1	$25,000.00
Total						$25,000.00
Web Security						
	Appliance	iPrism	iPrism 10h Appliance	$12,000.00	1	$12,000.00
	Web Filtering Subscription	iPrism	iPrism Appliance Filter Subscription	$3,588.75	1	$3,588.75
Total						$15,588.75
Utilities						
	Hard Drive Management	Diskeeper	Diskeeper Enterprise Server	$19,980.00	1	$19,980.00
	Maintenance and Support	Diskeeper	Diskeeper Enterprise Server Support	$16,197.00	1	$16,197.00
	Administration	Diskeeper	Diskeeper Administrator Console	$249.95	1	$249.95
	Maintenance and Support	Diskeeper	Diskeeper Administrator Console Support	$202.50	1	$202.50
	Licenses	Diskeeper	Diskeeper (Workstation) Client Licenses	$49.95	40	$1,998.00
	Maintenance and Support	Diskeeper	Diskeeper (Workstation) Client Support	$12.95	40	$518.00
	File Retention Management	Undelete	Undelete Server	$5,980.00	1	$5,980.00
	Maintenance and Support	Undelete	Undelete Server Support	$4,497.00	1	$4,497.00
	Licenses	Undelete	Undelete Client Licenses	$5.00	40	$200.00
	Maintenance and Support	Undelete	Undelete Client Support	$3.15	40	$126.00
Total						$326.00

8. Security Assessment

8.1.Overview

The purpose of this assessment is to quantify the potential risks and threats involved so that they may be identified and resolved.
Scope: This is a medical facility located in Beverly Hills, California that will specialize in providing assistance to high profile clientele, which can include clinical, psychological, rehabilitation, and surgical procedures.
The site will have restricted access to the physical building, as well as, access restrictions on internal floors, and/or rooms. The use of proximity cards, smart cards, and biometrics will be used for physical controls.

There will be data being transferred from the building, as well as being received through a VPN connection. There will be a data store house on site, as well as a data backup that will be sent offsite for disaster recovery. Protection to data will include

- physical controls (e.g., restricted physical access to the building, floors, and rooms)
- component (e.g., logon controls and usb keys)
- system (e.g., firewall, vpn, and server controls)
- data (e.g., backups, and encryption controls)

Technology will be provided for medical personnel to use on site (e.g., TabletPCs) that will be regulated through record keeping controls, and not allowed off site. Protection for this equipment also include a replacement process that will assess the current inventory, and then follow proper warranty procedures for replacements, while having a small readily available replacements on hand in a secure location (e.g., data center or equipment closet).

Other materials include, but are not limited to the following:

- Pharmaceutical (e.g., drugs)
- Dressings (e.g., bandages, sponges, tape)
- Medical Equipment (e.g., EKG, EEG, anesthetic, and theraputic)
- Clerical (e.g., printing, and writing materials)
- Janitorial (e.g. cleaning supplies)
- Shipping and Receiving (e.g., packaging and mail delivery)
- Technical (e.g., cabling, hand tools)

8.2.Current Approach of the Risk Assessment

8.2.1.Technique in Gathering Information

This is the process of analyzing the ground up infrastructure of the organization. Since this system is in the design phase, system information will be derived from the current design and/or requirements. This will help ascertain possible

weaknesses in the design.
This information is a general overview of a basic risk assessment and reviewing the documentation of current requirements.
This information is a general overview of a basic risk assessment and reviewing the documentation of current requirements.

The logistics are the following:

- How will people get into the facility?
- How will people access levels inside the facility?
- How will people access secure information?
- How will people access secure technology?
- What reasons would people need access to any of the previous?
- What technology is at risk?
- What data is at risk?

8.3.System Characterization

8.3.1.System-Related Information

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- System mission (e.g., processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity (level of protection required to maintain system and data integrity, confidentiality, and availability)

8.3.2.Operational Environment

- Functional requirements of the IT system
- Users of the system (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)
- System security policies governing the IT system (e.g., organizational policies, federal requirements, laws, industry practices)
- System security architecture
- Current network topology
- Flow of information pertaining to the IT systems (e.g., system interfaces, system input and output flowchart)
- Management controls used for the IT system (e.g., rules of behavior, security planning)

- Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment of the IT system (e.g., facility security, data center policies)
- Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

8.4.Threat Identification

The following tables will refer to the possible threats that the institution may face: They are broken up in to two categories:

- **Human:** This refers to the actions that people would take that could pose possible threats to the institution, generally through deception and electronic means.
- **Physical:** This refers to those threats that may or may not include human intervention, however cause physical harm to the institution.

Human Threats: Table 1-1

Threat-Source	Motiviation	Threat Actions
Hacker, Cracker	Challenge Ego Rebellion	● Hacking ● Social Engineering ● System Intrusion, Break-ins ● Unauthorized system access
Computer Criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	● Computer crime ● Fraudulent act ● Information bribery ● Spoofing ● System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	● Bomb/Terrorism ● Information warfare ● System attack ● System penetration ● System tampering
Industrial espionage	Competitive advantage Economic espionage	● Economic exploitation ● Information theft ● Intrusion of personal privacy ● Social engineering ● System penetration ● Unauthorized system access
Insiders	Curiosity Ego Intelligence Monetary gain Revenge Unintentional error and Omissions	● Assault on an employee ● Assault on a patient ● Blackmail ● Browsing of proprietary information ● Computer abuse ● Fraud and theft ● Information bribery ● Input of falsified, corrupt data ● Interception ● Malicious code

Insiders (Continued)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional error and Omissions	• Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access
Outsiders not including the previous	Curiosity Ego Intelligence Monetary gain Revenge	• Unauthorized system access • Unauthorized facility access • Assault on an employee • Assault on a patient • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupt data • Interception • Malicious code

Definitions of key points above:
Unauthorized Access: Physical or virtual, this is access that is unwanted and unwarranted by malicious means, be it harmful, or not harmful.
Blackmail: Is the unlawful use of intelligence to gain specific means by threat of release of said intelligence or physical harm.
Intelligence: This is the act of gaining information.
Competitive Advantage: This is the use of intelligence for gaining trade secrets to bolster one company or institution over another.
Malicious code: Is programming code that causes deliberate circumvention of security measures.
Assault: This is the act of violence done upon another person by mechanical or physical means.
Interception: The acquisition of intelligence by redirection.
Monetary gain: The act of conspiracy for financial rewards.
Ego: Initiating an act in the order to seem self-important or fame.
Fame: Recognition for actions taken. It also can be construed as infamy, recognition in a negative way.
Revenge: Causing a deliberate act out of retribution for a specific reason.
Illegal information disclosure: This is relevant to Intelligence, and supplying the material to the media or other parties that are not privy to said intelligence.

Sale of personal information: This is the monetary gain from illegal information disclosure, but about a specific person, rather than a company, agency and/or business.
Exploitation: This refers to the use of information or intelligence to gain influence or obtain gains within the institution.
Unauthorized data alteration: Unauthorized change of data within a system.
Input of falsified or corrupt data: This is the deliberate illegal modification or changing of data.
Fraud: Act of deliberate misinformation for personal or monetary gain.
Unintentional error or omissions: Data entered is not, by deliberate action, accurate.
Industrial espionage: The action of attempting to gain intelligence for reasons of causing competition failure and/or gaining the competitive advantage. This can also implicate the passage of such intelligence into other hands, e.g. data mining, for profit.
Hacker, Cracker: These are people whom wish to access the network via remotely or possibly social engineer their way into the facility.
Terrorists: A person that terrorizes or frightens others by illegal acts.
Insiders: These are people that are employed by the said institution or business.
Outsiders not including the previous: These are people that are not employed by said institution or business. They are not included in the specified threats, but can include anomalies that may not malicious.

8.4.1.Physical Threats

The following table depicts the possible physical threats that are probable, related or unrelated to human causation. This is described in what the threat is (Threat Source), what or why it would happen (Motivation), and the possible results of said action (Threat Actions).

Table 1-2

Threat-Source	Motivation	Threat Actions
Natural Disasters	Environmental	Damage to Equipment Damage to Data Loss of Data Loss of Equipment Loss of Productivity Physical Harm to Staff Physical Harm to Patients
Electrical	Accidental Fires Brown-Out Black-Out Shorts	Damage to Equipment Damage to Data Loss of Data Loss of Equipment Loss of Productivity Physical Harm to Staff Physical Harm to Patients
Water	Result from Natural Disaster Result from Fire Suppression Accidental Spilling of Liquids	Damage to Equipment Damage to Data Loss of Data Loss of Equipment Loss of Productivity Physical Harm to Staff Physical Harm to Patients
Chemicals	Accidental Spillage Purposeful Spillage	Damage to Equipment Destruction of Equipment Loss of Productivity Loss of Data Contamination Hazards to People Contamination Hazards to Hardware Physical Harm to Staff Physical Harm to Patients

Definitions of above: The following are definitions of those items that are not self evident in table 1-2.

Natural Disaster: Also known as "Acts of God." Uninhibited destruction from natural sources which include, and not limited to: wild fires, floods, tornados, earthquakes, landslides, and hail storms.

Electrical: The properties that would include an electrical discharge in some manner from a source which include, but not limited to: electrical outlets, power lines, transformers, surge protectors, telephone cables, and network cables.

Water: This is the property of a water source that is not included in the definition of *Natural Disaster*. Examples include, but are not limited to: ceiling fire suppression units, saline solution bags, water bottles, fire hoses, perimeter water intakes, cooling units, plumbing, outside faucets, outside sprinkler systems and ice makers.

Chemicals: This includes all other matters of solid and/or liquid that is not covered in the previous definitions. They would include, but not limited to: Medications, bacteria, mutagens, blood, viruses, acids, and any other source that would be listed in the material safety data sheets (MSDS) that are required by law to be on premise with a list of chemicals on the premise.

Contamination hazards to people: This is defined as exposure to a substance that is hazardous to a person's health. This would commonly be an item from the *chemicals* definition.

Contamination hazards to hardware: This is defined as exposure and end result of a substance that could be hazards that would be within the bounds of the *chemicals* definition to various types of hardware such as: computers (end-user and network), cables, and security devices.

8.5.Vulnerability Identification

An vulnerability is defined as a flaw or weakness in a system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.[1]

Any vulnerability has a threat that would coincide with it. Identifying the different vulnerabilities and their matching threats will enable a better understanding of the security policies, and ascertain what could be the best method to preempt those threats from exploiting vulnerabilities.
The following table gives examples of potential vulnerability/ threat pairing. It is broken down into 3 groupings, What the vulnerability is (Vulnerability), what would cause a threat to that vulnerability (Threat-Source), and the resulting action taken on that vulnerability (Threat-Action).

[1] Found by NIST Special Publication 800-30

Table 1-3

Vulnerability	Threat-Source	Threat Action
Fire Suppression Systems may cause damage to the IT equipment.	Fire, Negligence, Faulty Suppression System	Suppression System activating
Patients are allowed visitors	Unauthorized access	Patient guests may circumvent, unknowingly or willingly, security measures.
High profile patients	Outsiders (e.g., Media, Revenge Seekers, Fame seekers, Fans)	Social engineering would be considered to attempt to gain access to patients and their private/personal data.
Social Engineering by Patients for special, non-compliant actions	Unauthorized access	Patients will attempt to gain special privileges because of their status. Those privileges may include walking the facility unattended, accessing the network, requesting visitors to have special privileges
Hospital facility has a pharmacy onsite.	Unauthorized access	In/Outsiders may attempt to gain unauthorized access to the pharmaceutical cabinet to get non-prescribed drugs for personal use or illegal distribution
The system has a VPN set up so that X-ray images may be transferred to offsite doctors to analyze.	Unauthorized users (e.g., hackers, terminated employees, computer criminals, disgruntled employees, terrorists, social engineering)	Though security on the sending connection will be hardened and protected, there is the possibility of interception and/or unauthorized access on the receiving end network.

The system has a VPN set up so that an off-site transcription service may be transferred onsite for doctor's records. The transcription's hold all the doctors notes on the patients they are treating.	Unauthorized users (e.g., hackers, terminated employees, computer criminals, disgruntled employees, terrorists, social engineering)	Security will be maintained onsite, however it is uncontrolled on the senders (e.g., transcription company) side. There is a possibility of interception and/or unauthorized access on the sending company's network.
The facility contains an emergency room, by law under the Public Health and Welfare code (Title 42, Chap 7, SubChapter XVIII, Part E, 1395dd) must accept medical emergencies if they are approached by a patient. Though they may be allowed to transfer the patient if the facility is not able to treat the injury, or the patient is screened, examined and found able to be discharged.	Unauthorized access (e.g., media, terrorists, social engineering)	As bad as it may seem, people will do almost anything to gain access to a secure facility. One way is to pose (social engineer) as an emergency patient, in which the hospital must at least take the patient and do an initial assessment of their condition. This could leave an opening for the posing patient to bypass security measures.
TabletPCs are distributed to doctors for use in the facility in order to gain access to patient data via internal wireless network.	Unauthroized access (e.g., hackers, terrorists, data mining, information theft), Interception.	An unauthorized person may set up and attempt to intercept signals to analyze data transmissions to gain unauthorized access in to the network.

8.6.Security Requirements

These are basic security requirements shown in Table 1-4. These requirements create a checklist in three security areas that can help evaluate and identify the vulnerabilities of assets. These are broken down into two groups. Security Area refers to what type of system area would need to be assessed, and Security Criteria.

- Management
- Operational
- Technical

Table 1-4

Security Area	Security Criteria
Management Security	Assignment of responsibilities Continuity of support Incident response capability Periodic review of security controls Personnel clearance and background investigations Risk Assessment Security and technical training Separation of duties System authorization and reauthorization System or application security plan
Operational Security	Control of air-borne contaminants (smoke, dust, chemicals) Controls to ensure the quality of the electrical power supply Data media access and disposal External data distribution and labeling Facility protection (e.g., security access, data center, facility) Humidity control Temperature control Workstations, TabletPCs, and stand-alone personal computers
Technical Security	Communications (e.g., network infrastructure, security infrastructure) Cryptography Discretionary access control Identification and authentication Intrusion detection Object reuse System audit

8.6.1.Control Analysis

Because this network infrastructure has not been implemented as of yet, the controls have not been initiated and will be analyzed with a follow up risk assessment to help tighten the security of the system.

8.6.2.Control Methods

Though not implemented the following table is a list of control categories and the methods within. The categories are as follows: *Preventive* controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication; *Detective* controls warn of violations or attempted violations of security policy.

Preventive	Physical Entry Card Readers/Biometrics Firewalls Encryption Secure VPN Logins Active Directory Anti-Virus
Detective	Audit trails Intrusion detection Checksums

8.6.3.Likelihood Determinations

This is the ability to gain a more focused rating that will give the probability that potential vulnerabilities may be exercised within the construct of the security structure. It must be assessed by: Threat-source motivation and capability, Nature of the vulnerability, and Existence and effectiveness of current controls. The likelihood definitions are as follows:

- **High:** The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
- **Medium:** The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
- **Low:** The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

8.6.4.Impact Analysis

This determines the impact if a vulnerability would be exploited. In essence, this is

how much vulnerability would cost the institution in the event of it being threatened, even if it was not fully exploited. This would be found in the institutions Business Impact Analysis (BIA) document. This is measured by the following:

- System mission (e.g., the processes performed by the IT department)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity

The different ways that the vulnerability can impact the institution is determined in terms of loss or degradation of any, or a combination of any, of the following:

- **Loss of Integrity:** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
- **Loss of Availability:** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness may result in loss of medical treatment and/or productivity.
- **Loss of Confidentiality:** This is especially important for this institution, because of patient-doctor confidentiality, personal and medical records are stored, and the natures of the patients themselves are a constant target. Losing confidentiality can be detrimental to the facility and the patients.

8.6.5.Magnitude of Impact Definitions

The following is how to define the magnitude of the impacts, much like the likelihood definitions:

- **High:** Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede the organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
- **Medium:** Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources, (2) may violate, harm, or impede an organization's mission, reputation, or interest, or (3) may result in human injury
- **Low:** Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources, (2) may noticeably, harm, or impede an organization's mission, reputation, or interest.

8.7.Risk Assessment

It is a good way to see, in numbers, the risk level, but also be able to compute the actual level of threat by multiplying the threat likelihood by the threat impact. The following table shows how to determine the Risk Level. The final number is rated on a scale of

- **High**: >50 – 100
  If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures.
- **Medium**: >10 – 50
  If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time
- **Low**: 1 to 10
  If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required to decide to accept the risk.

Table 1-6

Risk Matrix	Impact		
Threat Likelihood	**Low (10)**	**Medium (50)**	**High (100)**
High (1.0)	**Low** 10 x 1.0 = 10	**Medium** 50 x 1.0 = 50	**High** 100 x 1.0 = 100
Medium (0.5)	**Low** 10 x 0.5 = 5	**Medium** 50 x 0.5 = 25	**Medium** 100 x 0.5 = 50
Low (0.1)	**Low** 10 x 0.1 = 1	**Low** 50 x 0.1 = 5	**Low** 100 x 0.1 = 10

Taking from the previous examples in Table 1-3, shows those vulnerabilities with the risk assessment. Please remember that this is initial assessment and that without being able to test a fully operational system, it is impossible to account for every single vulnerability until after implementation.

Vulnerability	Threat-Source	Risk Matrix Calculations (Likelihood x Impact)	Reasoning
Fire Suppression Systems may cause damage to the IT equipment.	Fire, Negligence, Faulty Suppression System	Likelihood = Low Impact = High 0.1 x 100 = 10: Low	Though the likelihood of the fire suppression system activating is low, and though some are rated for electronics, could damage the systems this could: ● result in the highly costly loss of major tangible assets or resources. ● violate, harm, or impede the organization's mission, reputation, or interest;
Patients are allowed visitors	Unauthorized access	Likelihood = High Impact = Medium 0.5 x 100 = 50:	The likelihood of patients having visitors is high, since people not doing well and are in the hospital generally enjoy

		Medium	having the company of friends and family, they may attempt to circumvent the security measures because of their status with the patient they are associating with. The impact of these people gaining access would be: ● costly loss of tangible assets or resources if they were allowed access to secure systems by one means or another. ● may violate, harm, or impede an organization's mission, reputation, or interest by circumventing the security policies and possibly impede treatment. ● may result in human injury by the fact of human relationships between other patients (rivals) and if the treatment process is impeded by a visitor, could cause more medical problems.
High profile patients are sought by fans, media, enemies, and other people for personal	Outsiders (e.g., Media, Revenge Seekers, Fame seekers, Fans)	Likelihood = High Impact = High 1.0 x 100 = 100: High	Because of the nature of the patients, they are sought after by fans, media, and potential threatening entities. Though the building is secure, social engineering would be a large portion of attempting to gain

gain.			access to the patients and their data by any means necessary. Since they are indeed sought after, this would be a constant threat and if patient information or access to the physical person was gotten then it: ● may result in the highly costly loss of major tangible assets or resources, by theft of data. ● may significantly violate, harm, or impede the organization's mission, reputation, or interest by giving the idea of easy access to the stars. Word of mouth can destroy specialized businesses. ● may result in human death or serious injury by the access of the patient and the intent on which the threat deems warranted.

Social Engineering by Patients for special, non-compliant actions	Unauthorized access	Likelihood = Medium Impact = Low 0.5 x 10 = 5: Low	With any high profile clientele, often they want special considerations for themselves. This can be anything from wanting internet access or free roam of the building. Likelihood that they will ask for special considerations are moderate, but seeing they are there for a special purpose, and not feeling well, they may not be able to do much. Also the nursing staff would be on hand to watch for non-compliance. It: ● may result in the loss of some tangible assets or resources, by gaining access to the hospital and if not under observation may gain access through social engineering to sensitive materials.
Hospital facility has a pharmacy onsite.	Unauthorized access	Likelihood = Low Impact = High 0.1 x 100 = 10: Low	In/Outsiders may attempt to gain unauthorized access to the pharmaceutical cabinet to get non-prescribed drugs for personal use or illegal distribution. ● may result in the loss of some tangible assets or resources because of the loss of controlled substances. ● may noticeably, harm, or impede an organization's mission, reputation, or interest since the loss of controlled substances is high on the law

			enforcement radar.
The system has a VPN set up so that X-ray images may be transferred to offsite doctors to analyze.	Unauthorized users (e.g., hackers, terminated employees, computer criminals, disgruntled employees, terrorists, social engineering)	Likelihood = High Impact = High 1.0 x 100 = 100: High	Though security on the sending connection will be hardened and protected, there is the possibility of interception and/ or unauthorized access on the receiving end network. Because of the nature of the information being sent, the likelihood would be high for a constant attempt to access the data and/or the network through that VPN. If the offsite facility is not secure as well, then protocols and passwords may become compromised, this: ● may result in the highly costly loss of major tangible assets or resources by the loss or theft of data. ● may significantly violate, harm, or impede the organization's mission, reputation, or interest by the loss of patient information, potential security breach and compromising of the network infrastructure.

The system has a VPN set up so that an off-site transcription service may be transferred onsite for doctor's records. The transcription's hold all the doctors notes on the patients they are treating.	Unauthorized users (e.g., hackers, terminated employees, computer criminals, disgruntled employees, terrorists, social engineering)	Likelihood = High Impact = High 1.0 x 100 = 100: High	Security will be maintained on-site, however it is uncontrolled on the senders (e.g., transcription company) side. Because of the nature of the information being received, the likelihood would be high for a constant attempt to access the data and/or the network through that VPN. There might be attempts of redirection from off site, to spoof the incoming VPN to gain access. If the offsite facility is not secure as well, then protocols and passwords may become compromised, this: ● may result in the highly costly loss of major tangible assets or resources by the loss or theft of data. ● may significantly violate, harm, or impede the organization's mission, reputation, or interest by the loss of patient information, potential security breach and compromising of the network infrastructure.
The facility contains an emergency room, by law under the Public Health and Welfare code (Title 42, Chap 7, SubChapter XVIII, Part E,	Unauthorized access (e.g., media, terrorists, social engineering)	Likelihood = Low Impact = High 0.1 x 100 = 10: Low	As bad as it may seem, people will do almost anything to gain access to a secure facility. One way is to pose (social engineer) as an emergency patient, in which the hospital must at least take the patient and do an initial assessment of their condition. This could leave an opening for the posing patient

1395dd) must accept medical emergencies if they are approached by a patient. Though they may be allowed to transfer the patient if the facility is not able to treat the injury, or the patient is screened, examined and found able to be discharged.			to bypass security measures. This: ● may result in the loss of some tangible assets or resources, by gaining access to the hospital and if not under observation may gain access through social engineering to sensitive materials. ● may noticeably, harm, or impede an organization's mission, reputation, or interest by the act of accessing of patients through malicious and fraudulent means.

TabletPCs are distributed to doctors for use in the facility in order to gain access to patient data via internal wireless network.	Unauthroized access (e.g., hackers, terrorists, data mining, information theft), Interception, physical theft.	Likelihood = Medium Impact = High 0.5 x 100 = 50: Medium	An unauthorized person may set up and attempt to intercept signals to analyze data transmissions to gain unauthorized access in to the network. Another possibility is the physical theft of the TabletPC. This: ● may result in the costly loss of tangible assets or resources by the loss of sensitive data, and/or the loss of the physical system. ● may violate, harm, or impede an organization's mission, reputation, or interest by the loss of data and/or physical machine that would require assessment of the situation, the impact of what data was on the TabletPC, and the security measures to adjust for the loss of the TabletPC and it's authorization level to the network infrastructure. ● may result in human injury by the sheer fact that often times the best way to steal something is to use brute force.

8.8.Assets

The following is a list of assets, though not limited to, without a full inventory list provided by the Paul Recovery and Treatment Center.

Table 1-8

Type	Equipment
Networking Servers	• SQL • Domain • Exchange • File and Print Server • Data Protection (Vontu) • Email Proxy (E-Safe) • Anti-Virus (McAfee) • ESX Server (VMWare)
Networking Routers, ASA, and Switches	• Cisco 3845 ISR • Cisco 2811 ISR • Cisco Catalyst 6509 • Cisco Catalyst 3705 • Cisco Catalyst Express CE500G-12TC • Cisco ASA 5510
Software	• Operating Systems • EMR Software (Electronic Medical Records) • Security (BioScrypt) • Microsoft Office • License Agreements
Media	• CD • DVD • USB

Cabling	• CAT 5e
	  ○ Straight (Patch)
	  ○ Crossover
	• Fiber
	• USB

Peripherals and End-User Systems	• TabletPC • USB keys • Monitors

	• Keyboards • End-User PCs • Printers
Networking Hardware	• Server Racks • Hand Tools • Power Tools
Not Directly IT Related	• Building (Facility) • Cleaning supplies • Medical supplies • EEG • EKG (ECG) • Therapeutic Equipment • Office Furniture • Operating Room Equipment • Pharmaceuticals • Fax Machines • Security Devices (Secure Entry Hardware) • Security keys/cards • Cafeteria and Break room equipment

9. Security Policy

9.1.Physical Access

9.1.1.Overview

The following security policy is presented by Kerberos Security for use by PRTC. These policies are subject to change, as industry and governmental standards may vary. These policies reflect best practices and seek to comply with the ISO 27001 standard, as well as HIPAA.

These policies seek to mitigate risks associated with PRTC's business process. They address the following areas:

- Physical Access
- Data Access
- Data Retention
- Data Destruction
- Network Appliance
- Workstations
- Servers
- Anti-Virus
- Acceptable Use
- Auditing

Specifically, these areas are discussed in relation to their scope, the resulting policy, enforcement, definition of terms, as well as a revision history. The security does not eliminate risks, but seeks to accommodate PRTC's specific risk appetite and mitigate those risks in the best way possible. Those risks can be referenced in the risk assessment conducted by Kerberos Security.

9.1.2. Scope

This policy applies to all PRTC employees, contractors, workforce members, vendors and agents with access to PRTC's facilities.

9.1.3.Policy

Appropriate measures must be taken when accessing PRTC facilities to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitivity information is restricted to authorized users.

9.1.3.1.Employee Requirements

Workforce members accessing PRTC facilities must consider why they are accessing the area they are entering, as well as how long they need to remain in the facility. This should be purposeful and kept to a minimum.

9.1.3.2.PRTC Required Action

PRTC will implement physical and technical safeguards for all access into facilities.

9.1.3.3.Appropriate Measures for Physical Access

Appropriate measures include:

- Restricting physical access to areas that contain sensitive information, such as the datacenter to essential personnel only.
- Restrict access to vital assets throughout the facilities such as wiring closets.
- Normal access should be logged, as well as abnormal access. Abnormal access should also be logged and flagged, as to elicit the appropriate response.
- ID cards with specific access will be distributed to all workforce members that dictate access to all areas required to complete their work.
- ID card access will logged as stated previously and attempts to access areas that are unauthorized will send an alert.
- A central repository of access, both legitimate and unauthorized will be maintained and kept according to the data retention policy (3.0).

9.1.4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.1.5.Definitions

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of PRTC.

9.2. Data Access

9.2.1. Overview

The purpose of this policy is to provide guidance for data access for PRTC in order to ensure the security of the information employees may have access to. Additionally, the policy provides guidance to ensure the requirements of HIPAA and federal guidelines are met.

9.2.2. Scope

This policy applies to all PRTC employees, contractors, workforce members, vendors and agents with access to PRTC's facilities.

9.2.3. Policy

Appropriate measures must be taken when accessing any data created by, for, or relevant to, PRTC to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

9.2.3.1. Employee Requirements

Workforce members accessing data must consider why they are accessing that data and if it is relevant to them completing their job. This should be purposeful and kept to a minimum.

9.2.3.2. PRTC Required Action

PRTC will implement physical and technical safeguards for access to its data.

9.2.3.3. Appropriate Measures for Data Access

- Employees may only access data for which they have been already authorized to do so.
- Employees may only access data by using their personal login information.
- Employees may not share their login information with any other people.
- Employees may only access data that is relevant to their job and task at hand.
- Employees will be mindful that they are the only person viewing any data that they access.
- Employees will not copy data for any reasons other than the requirements of their job.
- Employees will not modify any data unless specified by their current task.
- Employees will not delete any data unless specified by their current task and are in compliance with the current data retention and destruction policies (3.0, 4.0).
- PRTC will specify what data a given employee should be able to access to complete their job.

- PRTC will ensure that the correct permissions are set for various users, as well as to storage devices containing data.
- PRTC will ensure that these measures are kept up to date and reviewed frequently.

9.2.3.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.2.3.5.Definitions

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of PRTC.

Data includes: Any information produced for, by, or relevant to PRTC.

9.3.Data Retention

9.3.1.Overview

The purpose of this policy is to provide guidance for data retention for PRTC in order to ensure the security of client data, as well as other sensitive data of importance. Additionally, the policy provides guidance to ensure the requirements of the HIPAA standards are met.

9.3.2.Scope

This policy applies to all PRTC employees, contractors, workforce members, vendors and agents with medical data related to PRTC, as well as any other data the PRTC deems sensitive or relevant.

9.3.3.Policy

Appropriate measures must be taken concerning patient data, medical records, billing information of and other information related to PRTC deems sensitive. The confidentiality, integrity and availability of sensitivity information, including protected health information (PHI) and that access to sensitivity information is restricted to authorized users. The data must be retained in a secure environment that meets with current industry standards and legal compliance.

9.3.3.1.Employee Requirements

Workforce members shall consider the necessity to keep sensitive or non-sensitive information, including protected health information (PHI) that may need to be retained by law.

9.3.3.2.PRTC Required Action

PRTC will implement physical and technical safeguards for all data including, but not limited to protected health information, billing records, and patient data to ensure that they are retained for the appropriate length of time.

9.3.3.3.Appropriate Measures for Sensitive Data

Appropriate measures for sensitive data include:

- Encryption of retained data to meet current industry standards.
- Data will be retained of the appropriate amount of time, in compliance with federal guidelines.
- Data deemed sensitive will be kept for 6 years, as well as 2 years after death.
- Data will only be accessible by authorized personnel.
- Data will be kept on-site, as well as at off-site locations that meet or surpass these standards.

- Employees will not release data to people other than the patient or authorized personnel.
- Employees may not copy any information to any other media for any reasons that do not comply with this or any other PRTC policy.
- Data that becomes relevant in legal proceedings will be kept indefinitely or until their relevance is deemed unnecessary.

9.3.3.4.Appropriate Measures for Non-Sensitive Data

Appropriate measures for non-sensitive data include:

5. Emails relating to administrative correspondence will be kept for 4 years.
6. Emails relating to fiscal correspondence will be kept for 4 years.
7. Emails relating to ephemeral correspondence well be retained until read, and then destroyed.
8. Other documents that correspond to the above email policies will be treated in the same way and retained appropriately.
9. Data that becomes relevant in legal proceedings will be kept indefinitely or until their relevance is deemed unnecessary.

9.3.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Criminal charges brought forth by governing bodies or individuals as result of a violation or this policy will absolve PRTC and all parties related to PRTC of any responsibility. PRTC reserves the right to pursue legal action against any employee or organization for financial repercussions due to federal action that are a direct result of their actions.

9.3.5.Definitions

Sensitive information includes: Patient data, medical records, billing information, or any other information electronic or otherwise that PRTC chooses to apply this policy to.

Non-Sensitive data includes: Any data that is not considered sensitive and is produced by, or related to, PRTC.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of PRTC.

9.4. Data Destruction

9.4.1.Overview

The purpose of this policy is to provide guidance for data destruction for PRTC in order to ensure the security of client data, as well as other sensitive data of importance. Additionally, the policy provides guidance to ensure the requirements of the HIPAA standards are met.

9.4.2.Scope

The purpose of this policy is to provide guidance for data destruction for PRTC in order to ensure the security of client data, as well as other sensitive data of importance. Additionally, the policy provides guidance to ensure the requirements of the HIPAA standards are met.

9.4.3.Policy

Appropriate measures must be taken concerning the destruction of patient data, medical records, billing information of and other information related to PRTC deems sensitive. The destruction of sensitive information, including protected health information (PHI) should meet with current industry standards and legal compliance.

9.4.3.1.Employee Requirements

Workforce members shall comply with all company and legal guidelines when destroying information, including protected health information (PHI), whether it is paper or electronic.

9.4.3.2.PRTC Required Action

PRTC will implement physical and technical safeguards for all data destruction including, but not limited to, protected health information, billing records, and patient data.

9.4.3.3.Appropriate Measures for Sensitive Paper Documents

Appropriate measures for the destruction of paper documents include:

- Employees will only destroy data when the data retention policy (3.0) no longer applies to data, and is no longer required for any purposes, legal or otherwise.
- Employees may not duplicate any documents in any way when it should be appropriately destroyed. See data retention policy (3.0) for appropriate duplication.
- Paper documents will be shredded according to the strictest legal and

industry standards.
- The appropriate shredders to complete these actions will be readily and easily accessible to all staff where appropriate.
- When an employee is not certain as to the correct action to be taken concerning data destruction they are required to notify a supervisor for clarification.

9.4.3.4.Appropriate Measures for Electronic Media

Appropriate measures for the destruction of electronic media include:

- Employees will only destroy data when the data retention policy (3.0) no longer applies to data, and is no longer required for any purposes, legal or otherwise.
- Employees may not duplicate any electronic media or transfer said media in any way when it should be appropriately destroyed. See data retention policy (3.0) for appropriate duplication.
- Electronic media must be destroyed according to the governmental and industry standards for that specific type of media.
- The appropriate methods for destruction of various electronic media must be readily and easily accessible to all staff where appropriate.
- When an employee is not certain as to the correct action to be taken concerning data destruction they are required to notify a supervisor for clarification.

9.4.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Criminal charges brought forth by governing bodies or individuals as result of a violation or this policy will absolve PRTC and all parties related to PRTC of any responsibility. PRTC reserves the right to pursue legal action against any employee or organization for financial repercussions due to federal action that are a direct result of their actions.

9.4.5.Definitions

Paper document includes: Any data that is stored on a media other than electronic. This includes files, folder, notes, and any other documents PRTC deems appropriate. Electronic Media includes: Any data that is stored on a media that is not paper. This includes, but is not limited to, compact disks (CD), universal serial bus (USB) drives, portable music devices, email attachments, electronic file formats, hard drives, or any other media that PRTC deems appropriate.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of PRTC.

9.5. **Network Appliance**

9.5.1.Overview

The purpose of this policy is to provide guidance for network appliance security for PRTC operated network appliances. This is meant to ensure the security of data relevant to PRTC. Additionally the policy provides guidance to ensure that the requirements of HIPAA are met.

9.5.2.Scope

This policy applies to all network appliances owned, operated, leased, or under the control of PRTC and on a PRTC network

9.5.3.Policy

Appropriate measures must be taken to secure all PRTC network appliances connected to a PRTC network. These measures seek to further secure the integrity, confidentiality, availability of protected health information (PHI) and any other information relevant to PRTC.

9.5.3.1.Employee Requirements

Workforce members with authorized access to network appliances must comply with the measures dictated by this policy in order to help minimize the possibility of information becoming compromised as a result of a network appliance not being compliant with this policy, government, and industry best practices.

9.5.3.2.PRTC Required Action

PRTC will ensure that there are physical and technical safeguards to protect all network appliances.

9.5.3.3.Appropriate Measures for Network Appliances

Appropriate measures include:

- Periodically auditing network appliances to ensure that they are not running any erroneous services, see auditing policy (10.0).
- Physically securing network appliances so that only PRTC authorized personnel may access them.
- Ensuring that network appliances are patched and running the latest version of relevant software.
- Connections made to network appliances for administrative purposes must use a secure protocol that meets governmental and industry standards.
- All network appliances must have a redundant power source.
- All network appliances must be mounted on an appropriate rack in a area that meets with the specifications stated in the physical access

policy (1.0).
- All network appliances must authenticate to a centralized server when a user attempts to access them to verify that user.
- The centralized server that manages users and their access to network appliances must be kept up to date and audited periodically, see auditing policy (10.0).

9.5.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.5.5.Definitions

Network Appliance includes: routers, switches, hubs, cables, or any device that facilities computer networking or that PRTC deems appropriate or relevant.

9.6. **Workstations**

9.6.1.Overview

The purpose of this policy is to provide guidance for workstation security for PRTC workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

9.6.2.Scope

This policy applies to all PRTC employees, contractors, workforce members, vendors and agents with a PRTC-owned or personal-workstation connected to the PRTC network.

9.6.3.Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information, including protected health information (PHI) and that access to sensitivity information is restricted to authorized users.

9.6.3.1.Employee Requirements

Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

9.6.3.2.PRTC Required Action

RTC will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

9.6.3.3.Appropriate Measures for Workstations

Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected
- Complying with all applicable password policies and procedures.
- Ensuring workstations are used for authorized business purposes

only.
- Never installing unauthorized software on workstations.
- Storing all sensitivity information, including protected health information (PHI) on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitivity information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the Portable Workstation Encryption policy
- Complying with the Anti-Virus policy
- Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).

9.6.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.6.5.Definitions

Workstations include: laptops, desktops, PDAs, computer based medical equipment containing or accessing patient information and authorized home workstations accessing the PRTC network.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of PRTC

9.7. **Servers**

9.7.1.Overview

The purpose of this policy is to provide guidance for server security for PRTC servers. Additionally this policy provides guidance to ensure the requirements of HIPAA are met.

9.7.2.Scope

This policy applies to all PRTC employees, contractors, workforce members, vendors and agents with a PRTC-owned server connected to the PRTC network.

9.7.3.Policy

Appropriate measures must be taken to secure PRTC servers to ensure that they meet industry and governmental standards. These guidelines seek to enhance the security of all information relevant to PRTC, as well as its patients.

9.7.3.1.Employee Requirements

Workforce members authorized to use servers shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

9.7.3.2.PRTC Required Action

PRTC will implement technical safeguards for all servers that reside on a PRTC network.

9.7.3.3.Appropriate Measures for Servers

Appropriate measures include:

- Servers must only run the services that are necessary for them to function correctly.
- Servers must only have the software installed that for them to function correctly.
- Servers must be patched and up to date with regard to the operating system they are running.
- Servers should not be accessible from the outside world unless specifically needed for a PRTC approved reason.
- Servers accessible from the outside world should be located in a DMZ unless specifically needed for a PRTC approved reason.
- Servers must be patched and up to date with regard to the software they are running.
- Servers may only be accessed by PRTC personnel with the appropriate permissions.

- Only authenticated users with the appropriate authorization may access servers.
- Restricting physical access to servers to only authorized personnel.
- Securing servers (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that servers that were left unsecured will be protected
- Complying with all applicable password policies and procedures.
- Ensuring servers are used for authorized business purposes only.
- Never installing unauthorized software on servers.
- Servers must be periodically audited for vulnerabilities and those issues must be addressed in a timely fashion. See auditing policy (10.0).

9.7.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.7.5.Definitions

Servers include: Computer based equipment containing or accessing patient information accessing the PRTC network that is being utilized as a server.
Workforce members include: employees, volunteers, trainees, and other persons under the direct control of PRTC

9.8. **Anti-Virus**

9.8.1.Overview

The purpose of this policy is to provide guidance for workstation security for PRTC workstations in relation to anti-virus. Additionally, the policy provides guidance to ensure the requirements of HIPAA are met.

9.8.2.Scope

This policy applies to all PRTC employees, contractors, workforce members, vendors and agents with a PRTC-owned or personal-workstation connected to the PRTC network.

9.8.3.Policy

Appropriate anti-virus software must be installed on any computer accessing information created by, produced for, and stored by PRTC. This guideline seeks to enhance the security of all information relevant to PRTC, as well as its patients.

9.8.3.1.Employee Requirements

Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

9.8.3.2.PRTC Required Action

PRTC will implement technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

9.8.3.3.Appropriate Measures for Anti-Virus

Appropriate measures include:

- Restricting network access to computers that have current, installed anti-virus software
- PRTC must ensure that all computers with network access have the appropriate anti-virus software that is sanctioned by PRTC.
- PRTC must ensure that they have currently purchased appropriate anti-virus software, with the correct licensing.
- PRTC must provide an automated and efficient way to update anti-virus software.
- PRTC must provide an automated and efficient way to update virus signatures utilized by the anti-virus software.

- PRTC must ensure that any and all anti-virus software is working correctly, and is running not only installed, but running on all computers.
- PRTC must ensure that any changes meant to effect anti-virus enterprise-wide are carried out quickly and completely.

9.8.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.8.5.Definitions

Workstations include: laptops, desktops, PDAs, computer based medical equipment containing or accessing patient information and authorized home workstations accessing the PRTC network.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of PRTC

9.9. **Acceptable Use**

9.9.1.Overview

The purpose of this policy is to provide guidance for the acceptable use for PRTC computers in order to ensure the security of information handled by PRTC.

9.9.2.Scope

This policy applies to all PRTC employees, contractors, workforce members, vendors and agents with a PRTC-owned or personal computers connected to the PRTC network.

9.9.3.Policy

Computers that are PRTC-owned or workforce members' personal computers that are connected to the PRTC network should only be used for tasks related to PRTC.

9.9.3.1.Employee Requirements

Computers that are PRTC-owned or workforce members' personal computers that are connected to the PRTC network should only be used for tasks related to PRTC.

9.9.3.2.PRTC Required Action

PRTC will implement physical and technical safeguards to ensure that PRTC-owned or personal computers attached to the PRTC network are used appropriately.

9.9.3.3.Appropriate Measures for Acceptable Use

Appropriate measures include:

- PRTC related tasks should only be done on computers.
- Workforce members will not download or install any software on PRTC-owned computers or on computers connected to a PRTC network.
- Workforce members will not browse the Internet for non-PRTC related reasons.
- Workforce members will not click on suspicious links.
- Workforce members will not open suspicious emails.
- Workforce members will be aware of their surroundings and ensure that they are not allowing others to view information displayed on their screen.
- Workforce members will not leave their computer without first locking it or logging off.
- Workforce members will not copy any data unless authorized by

PRTC.

- Workforce members will not share any sensitive information related to PRTC with any other parties.
- Workforce members will not attempt to access any information that is not necessary for them to complete their job.
- Workforce members are required to report any violations of this policy to their immediate supervisor.
- PRTC will restrict and filter as much erroneous content as possible.

9.9.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.9.5.Definitions

Computers include: Any computer based device that is PRTC-owned or connected to a PRTC network.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of PRTC

9.10. Auditing

9.10.1.Overview

The purpose of this policy is to provide guidance for PRTC in relation to auditing in order to ensure the security of information handled by PRTC.

9.10.2.Scope

This policy applies to all PRTC employees, contractors, workforce members, vendors and agents with a PRTC-owned or personal computers connected to the PRTC network.

9.10.3.Policy

Computers that are PRTC-owned or workforce members' personal computers that are connected to the PRTC network should be audited according to governmental and industry standards.

9.10.3.1.Employee Requirements

Workforce members responsible for the technical success of PRTC must ensure that all computer-based systems are audited.

9.10.3.2.PRTC Required Action

PRTC will implement physical and technical measures to ensure that PRTC-owned or personal computers attached to the PRTC network are audited appropriately.

9.10.3.3.Appropriate Measures for Auditing

Appropriate measures include:

- Weekly auditing servers to ensure that their operating systems are patched or sooner as vulnerabilities are discovered.
- Automated patching of workstations, both portable and stationary to ensure that their operating systems are up to date.
- Weekly patching of network appliances to ensure that they are patched and running the latest version of their software or sooner as vulnerabilities are discovered.
- Logging of appropriate access or access attempts on all systems.
- Timely analysis of logs.
- Quarterly risk assessments to ensure that a clear understanding of how the information system has changed.
- Semi-annual penetration testing to ensure that the PRTC network is configured in an acceptably secure manner.

9.10.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.10.5.Definitions

Computers include: Any computer based device that is PRTC-owned or connected to a PRTC network.

Workforce members include: employees responsible for the technical success of the PRTC in relation to information technology.

9.11.Awareness Training

9.11.1.Overview

The purpose of this policy is to provide guidance for PRTC in relation to awareness training in order to ensure the security of information handled by PRTC.

9.11.2.Scope

This policy applies to all PRTC employees, contractors, workforce members, vendors and agents.

9.11.3.Policy

Workforce members must participate in awareness training related to all technology that may pose a risk to the security of information handled by PRTC, as well as to comply with governmental and industry standards.

9.11.3.1.Employee Requirements

Workforce members are responsible for attending and successfully completing awareness training provided by PRTC.

9.11.3.2.PRTC Required Action

PRTC will ensure that appropriate measures, there is a relevant and up to date awareness training curriculum in place, and that all necessary topics relevant to maintaining a secure environment are covered in the training.

9.11.3.3.Appropriate Measures for Awareness Training

Appropriate measures include:

- PTRC must cover the physical access security policy.
- PTRC must cover the data access security policy.
- PRTC must cover the data retention security policy.
- PTRC must cover the data destruction security policy.
- PRTC must cover the workstations security policy.
- PRTC must cover the anti-virus security policy.
- PRTC must cover the acceptable use security policy.
- PRTC must cover any revisions to any and all policies.
- PRTC must cover any other policies relevant to the PRTC workforce.
- Workforce members must attend all topics presented in the awareness training.
- Workforce members must successfully complete all sections of the awareness training

9.11.4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.11.5.Definitions

9.11.5.1.Workforce members include: employees responsible for the technical success of the PRTC in relation to information technology.

10. Total Cost

10.1. Overview

The following is a matrix showing the grand total for the entire project.

10.2. Pricing Matrices

WAN		
Main Router		$18,940.97
Standby Router		$9,195.97
Main and Standby Security Appliances		$19,169.94
Main Switch		$3,204.17
Backup Power		$951.58
Services		$280,800.00
	Total:	$332,262.63
Virtual Security		
ACS Appliance		$6,787.96
ACS Appliance		$10,799.96
Anti-Virus		$7,084.80
Auditing		$8,455.36
Backup		$9,568.00
Data Loss Prevention		$25,000.00
Web Security		$15,588.75
Utilities		$326.00
	Total:	$83,610.83
LAN		
Cabling		$60,230.55
Core Switching		$137,952.74
Distribution Switching		$97,490.54
Tablet PCs		$54,358.82
Encryption		$2,307.76
	Total:	$352,340.41
Data Center		
Racks		$24,639.70
KVM Switches		$14,839.76
Server (SQL)		$25,703.72
Server (Other)		$24,539.80
Server (ESX)		$22,567.00
Licensing (Microsoft/VMWARE)		$42,547.58
Licensing (RSA)		$4,180.20
SAN		$211,385.80
UPS		$67,788.96
	Total:	$438,192.52
Physical Security		
Access Control Panels		$43,200.00
Keypads/Proximity Readers		$3,512.00
Proximity Readers		$6,870.00
Magnetic Locks w/ Remote		$20,124.00
	Total:	$73,706.00
	Grand Total:	$1,280,112.39

11. Implementation Plan

11.1. Overview

The following matrices are timelines for when a project can be completed. Many of these projects can be performed at the same time to be time efficient.

11.2. Implementation Matrices

WAN Implementation Matrix

Objective	**Time**
Purchase and Receiving Shipments	2 Weeks
WAN Hardware Configuration	2 Weeks
T3 Service Installation	1 Week
Bring WAN Connection Online	1 Week
Test WAN connectivity, setup connections to JP Medical Transcription Service and JP X-Ray Asian Diagnostic,	1 Week
Audit and Hardening of WAN Equipment	1 Week
Final Testing	1 Week
Training	1 Week

LAN Implementation Matrix

Objective	**Time**
Purchase and Receiving Shipments	2 -3 Weeks
LAN Hardware Configuration	2 Weeks
Cable Runs	1 Week
Connect WAN	1 Week
Test connectivity and configurations	1 Week
Audit and Hardening of LAN Equipment	1 Week
Final Testing	1 Week
Training	1 Week

Data Center Implementation Matrix

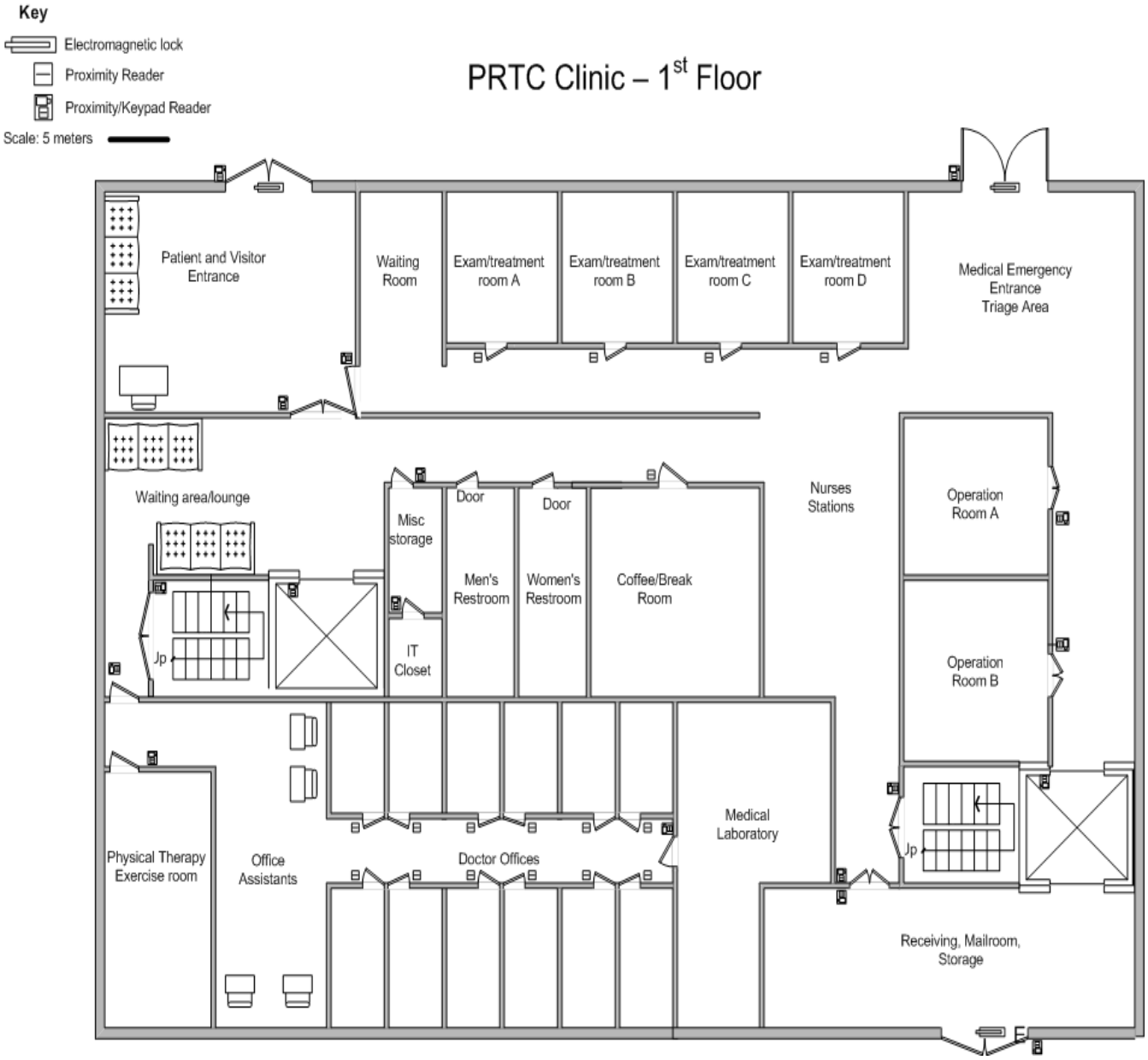
Objective	**Time**
Purchase and Receiving Shipments	2 -3 Weeks
Server Connections	2 -3 Days
Server Configuration	2 Weeks
SAN Configuration	1 Week
Test connectivity and configurations	1 Week
Audit and Hardening of Server Equipment	1 Week
Final Testing	1 Week
Training	1 Week

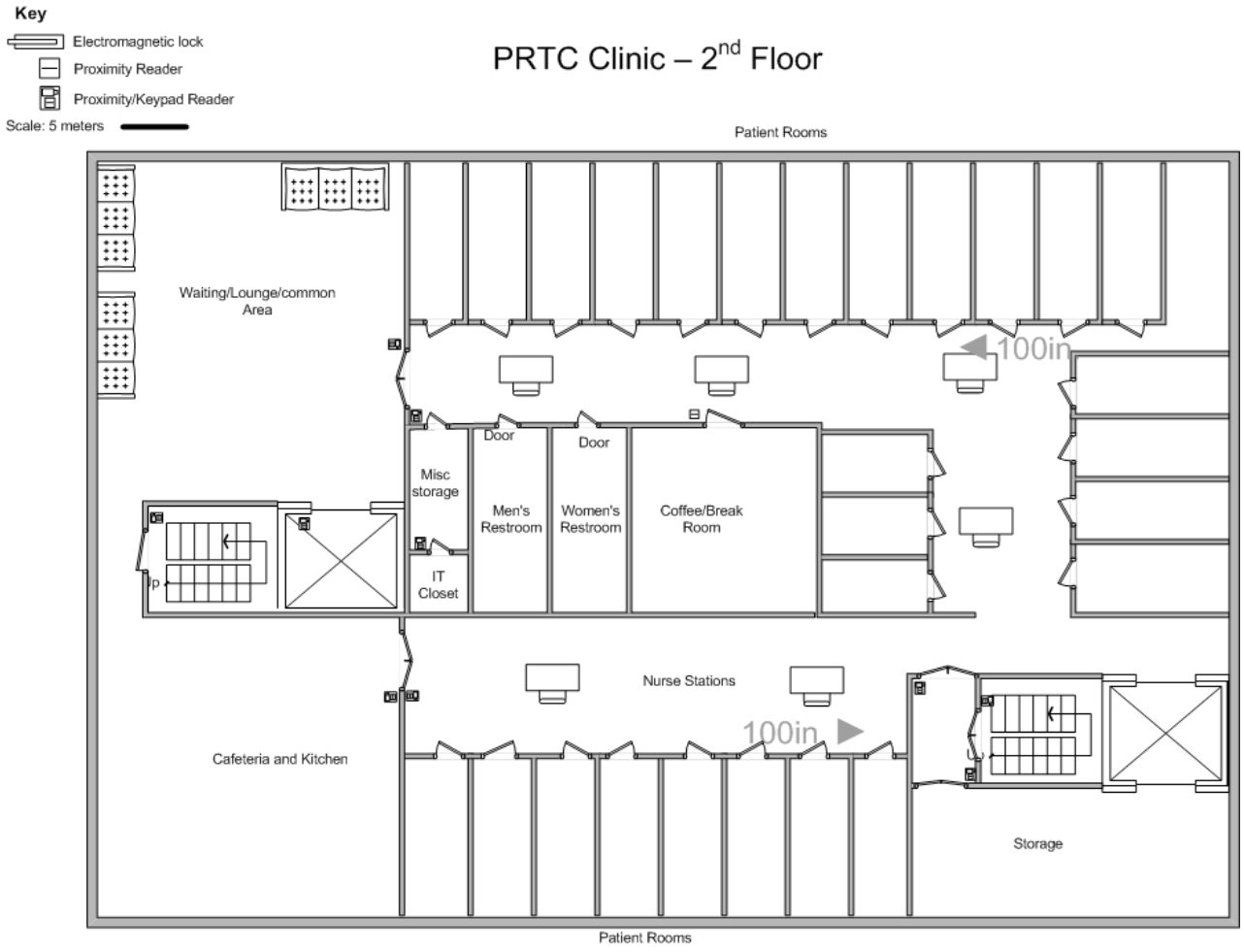
Special Notes on Installing Physical Access System

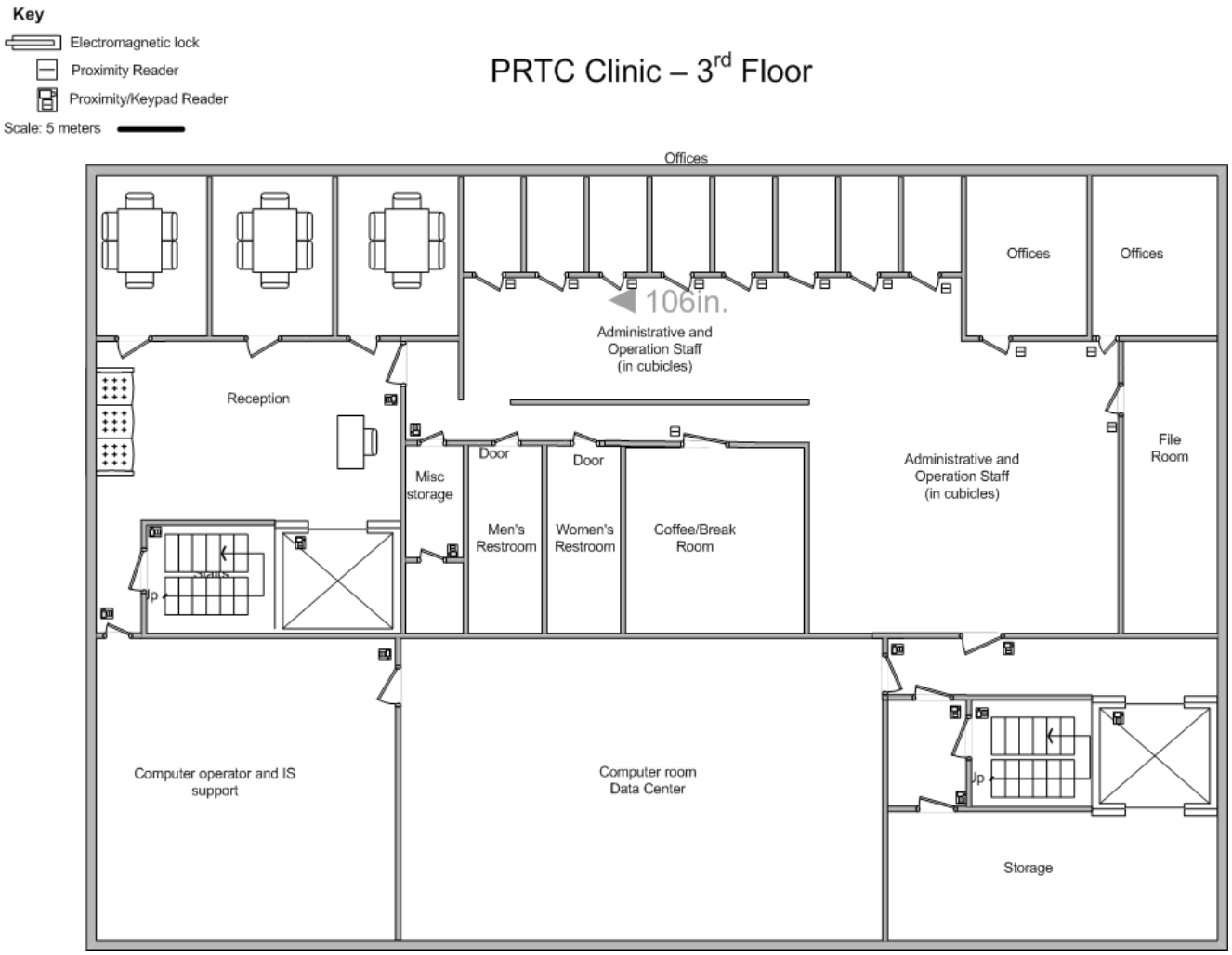
The following guidelines are needed before following the implementation process designed by the manufacturer:

- Knowledge of the network topology
- Knowledge of assigned IP addressing for the internal network.
- Vender approved installers (see Physical Security Appendix: Hardware Manufacturers)
- External physical security audit by a company with HIPAA certifications to allow for compliance audit trail and records for city, state, and federal regulations.
- Have had at least one security personnel rated as trainer and one IT personnel have gone through vendor approved training and rated as a programmer as stated in the Physical Security Manual.

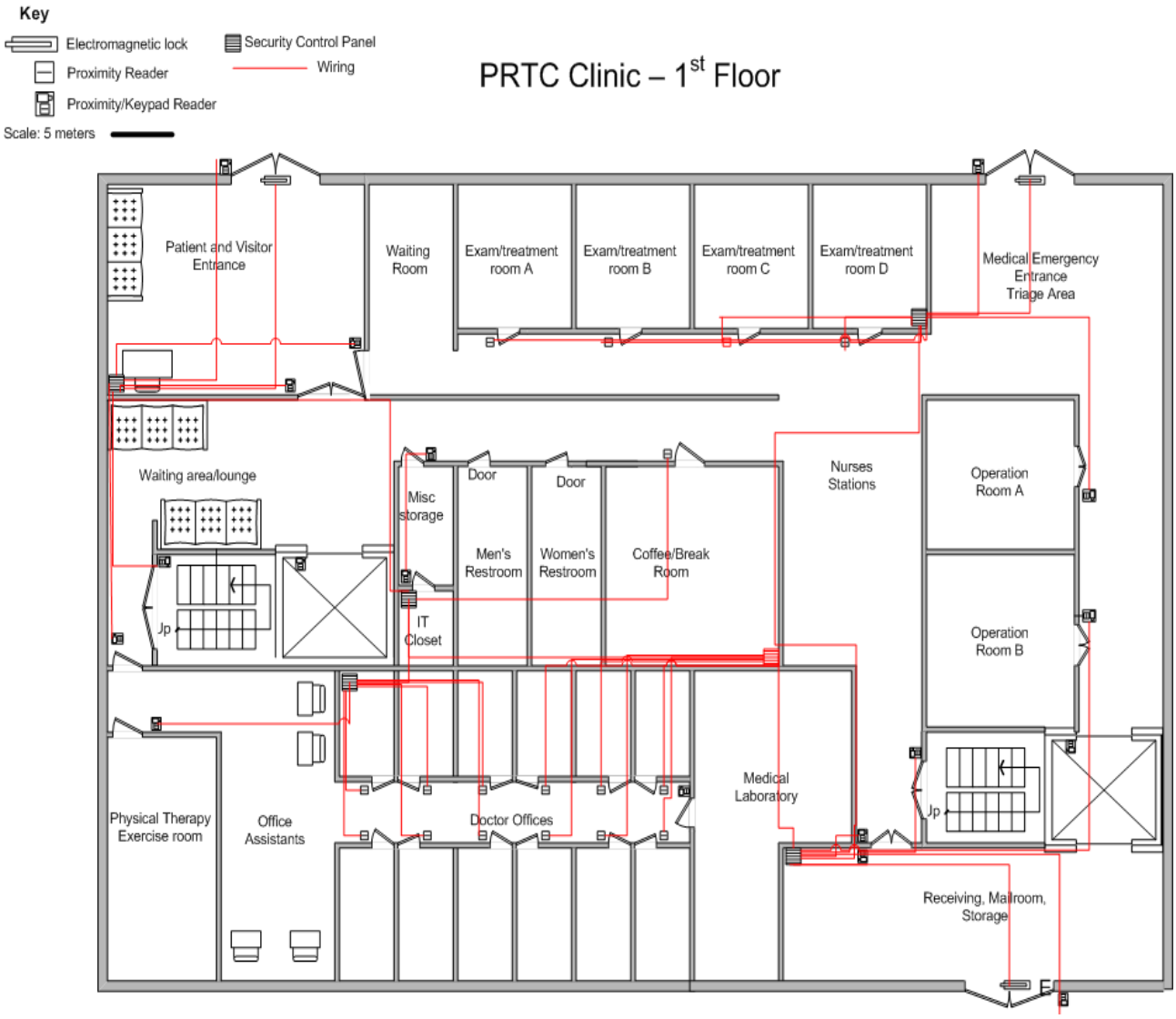
Physical Security Access Control Layout:

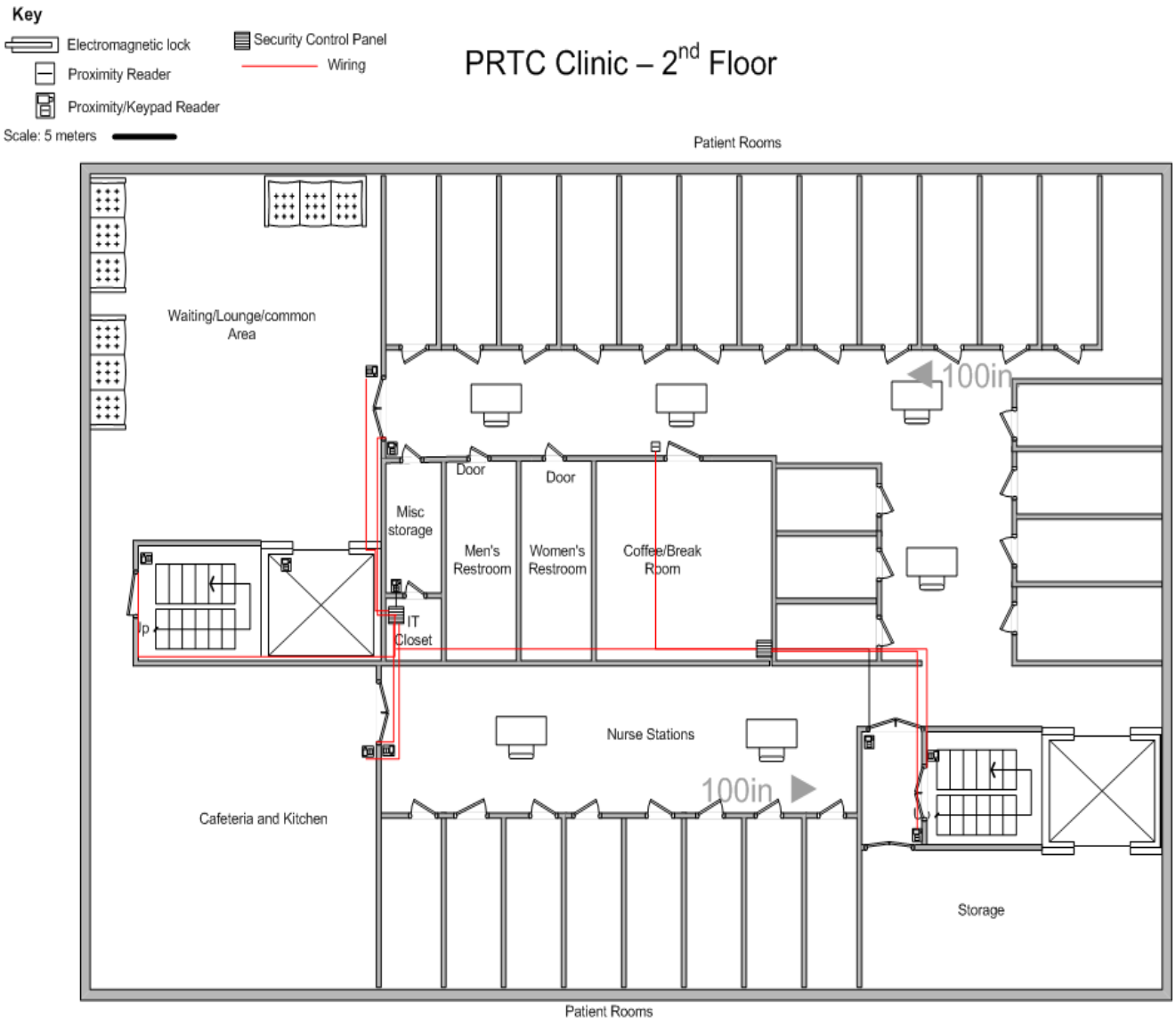


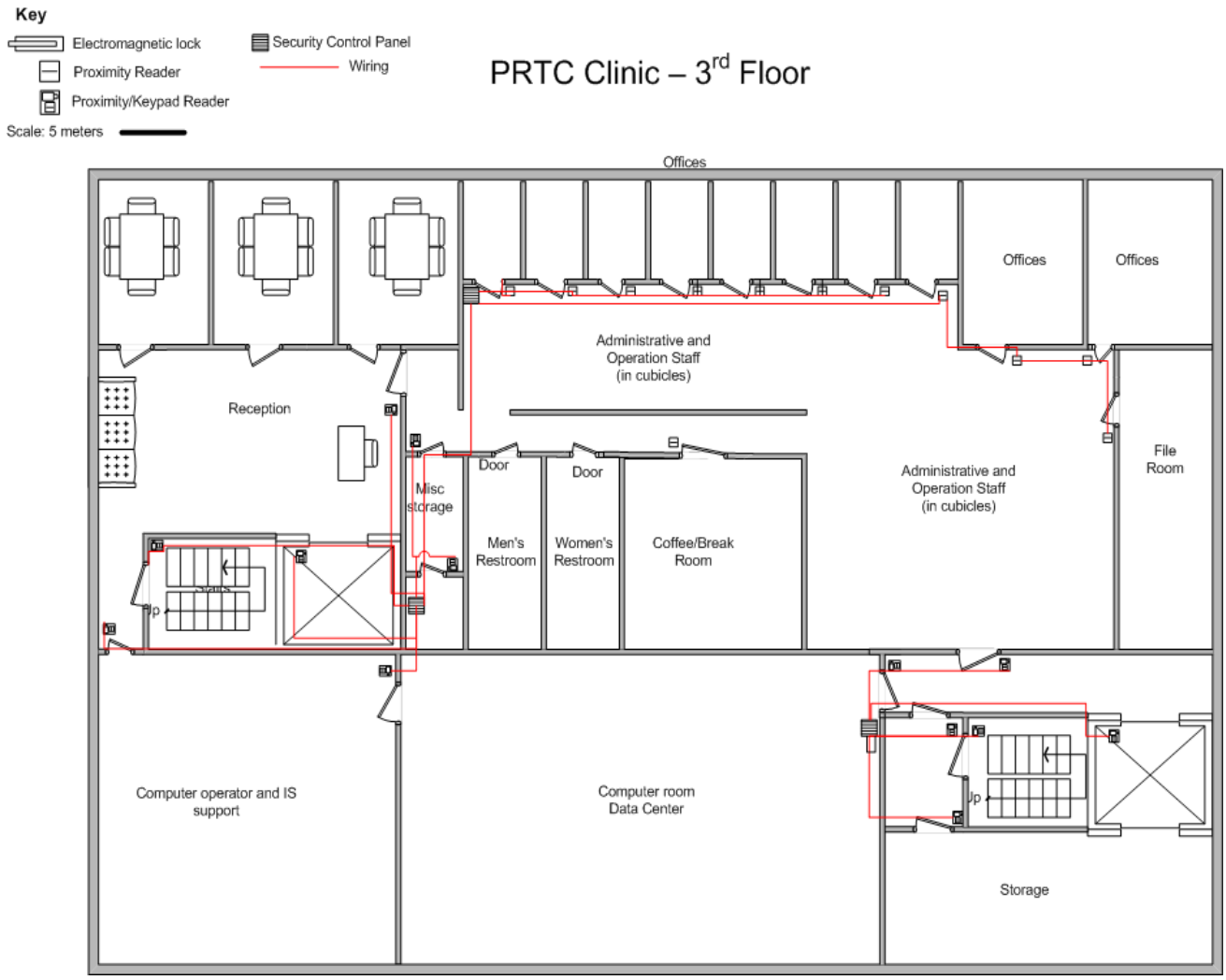

Key
Electromagnetic lock
Proximity Reader
Proximity/Keypad Reader
Scale: 5 meters
PRTC Clinic – 2nd Floor
Patient Rooms
Waiting/Lounge/common Area
100in
Door
Door
Misc storage
Men's Restroom
Women's Restroom
Coffee/Break Room
IT Closet
Nurse Stations
100in
Cafeteria and Kitchen
Storage
Patient Rooms


Key
Electromagnetic lock
Proximity Reader
Proximity/Keypad Reader
Scale: 5 meters
PRTC Clinic – 3rd Floor
Offices
Offices
Offices
106in.
Administrative and Operation Staff (in cubicles)
Reception
Misc storage
Door
Door
Men's Restroom
Women's Restroom
Coffee/Break Room
Administrative and Operation Staff (in cubicles)
File Room
Up
Computer operator and IS support
Computer room Data Center
Up
Storage

Physical Security Access Wiring Diagrams:




Key
Electromagnetic lock
Proximity Reader
Proximity/Keypad Reader
Security Control Panel
Wiring
Scale: 5 meters
PRTC Clinic – 2nd Floor
Patient Rooms
Waiting/Lounge/common Area
100in
Door
Door
Misc storage
Men's Restroom
Women's Restroom
Coffee/Break Room
IT Closet
Nurse Stations
100in
Cafeteria and Kitchen
Storage
Patient Rooms



Implementation for Alarm Electromagnetic Lock with remote wiring diagram for integration into the Hartmann Controls System:
See the Alarm Lock Electromag Lock document in the Appendix

Implementation of Security Access hardware:
See the Protector Tech Guide document in the Appendix

Implementation of Security Access Software:
See the Protector Software Guide document in the Appendix

12. Assumptions

- PRTC will install a generator that is capable of sustaining the hospital's power needs for a reasonable amount of time after a five to ten minute warm-up period.
- The Data Center will be adequately cooled to keep room at operating temperature
- Facility will be able to receive large shipments
- PRTC will have adequate staffing on hand for training purposes
- Extra storage rooms can be turned into Intermediate Distribution Facilities
- PRTC will create IT area, IT storage, and IT Testing Areas in Data Center