

***PROJECT PROPOSAL FOR***

***NATIONAL INSURANCE COMPANY***

**WIRELESS NETWORK**

Version 1.0

*12/10/2014*

**VERSION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Authors** | **Date** | **Reason** |
| 1.0 | Glen Sayarot, Mike Fetick | 11/12/2014 | Assemble the proposal. |
|  | Glen Sayarot | 11/12/2014 | 1 Introduction  1.1 Proposal  1.2 Current Configuration  2 Design of the Wireless Network  2.1 Planned Configuration  4 Wireless Network Installation and Setup  4.1 Routing and IP Addresses  5 Policies Implementation  5.1 IT Department – Network Operations Policy  5.2 IT Department – Wireless Communication Policy  5.3 IT Department – Software Usage Policy  5.4 IT Department – Network Security Policy  6 Contingencies & Unforeseen Events  6.1 IT Department – Disaster Recovery (DR) Plan |
|  | Mike Fetick | 12/6/2014 | 2.2 Assumptions and Constraints  2.3 System Organization  2.4 Hardware-Network Diagrams (Visio)  2.5 Site Survey Access Point Form – Completed  2.6 Site Survey Questionnaire Form – Completed  3 Component Specifications of the Wireless Network  3.1 Hardware Network Controllers  3.2 Hardware Routers and Switches  3.3 Hardware Security Equipment (Firewall)  3.4 Hardware Wireless Access Points  3.5 Hardware-Cabling and Connectors  3.6 Hardware Lightening Protection Equipment  3.7 Hardware-Outdoor Antennas  3.8 Hardware Outdoor Cameras  3.9 Cost-Budget (Hardware Cost Break-Down)  4.2 Software Configuration and Bootstrap Files  4.3 Software Licenses and Account Management  4.4 Signal Coverage Validation – Power Measurements and Adjustments  7 Conclusion  APPENDIX A: Project Proposal Approval  APPENDIX B: WORKS CITED |

**Table of Contents**

[1 Introduction 5](#_Toc406435746)

[1.1 Proposal 5](#_Toc406435747)

[1.2 Current Configuration 5](#_Toc406435748)

[2 Design of the Wireless Network 5](#_Toc406435749)

[2.1 Planned Configuration 5](#_Toc406435750)

[2.2 Assumptions and Constraints 6](#_Toc406435751)

[2.3 System Organization 7](#_Toc406435752)

[2.4 Hardware-Network Diagrams (Visio) 7](#_Toc406435753)

[2.5 Site Survey Access Point Form – Completed 12](#_Toc406435754)

[2.6 Site Survey Questionnaire Form – Completed 21](#_Toc406435755)

[3 Component Specifications of the Wireless Network 30](#_Toc406435756)

[3.1 Hardware Network Controllers 30](#_Toc406435757)

[3.2 Hardware Routers and Switches 30](#_Toc406435758)

[3.3 Hardware Security Equipment (Firewall) 30](#_Toc406435759)

[3.4 Hardware Wireless Access Points 31](#_Toc406435760)

[3.5 Hardware Cabling and Connectors 31](#_Toc406435761)

[3.6 Hardware Lightening Protection Equipment 31](#_Toc406435762)

[3.7 Hardware Outdoor Antennas 32](#_Toc406435763)

[3.8 Hardware Outdoor Cameras 32](#_Toc406435764)

[3.9 Cost-Budget (Hardware Cost Break-Down) 32](#_Toc406435765)

[4 Wireless Network Installation and Setup 33](#_Toc406435766)

[4.1 Routing and IP Addresses 33](#_Toc406435767)

[4.2 Software Configuration and Bootstrap Files 34](#_Toc406435768)

[4.3 Software Licenses and Account Management 34](#_Toc406435769)

[4.4 Signal Coverage Validation – Power Measurements and Adjustments 34](#_Toc406435770)

[**5 Policies Implementation 35**](#_Toc406435772)

[5.1 Information Technology (IT) Department – Network Operations Policy 35](#_Toc406435772)

[5.2 IT Department – Wireless Communication Policy 36](#_Toc406435773)

[5.3 IT Department – Software Usage Policy 38](#_Toc406435774)

[5.4 IT Department – Network Security Policy 42](#_Toc406435775)

[5.5 IT Department – Security Incident Reporting and Response Policy 44](#_Toc406435776)

[6 Contingencies & Unforeseen Events 47](#_Toc406435777)

[6.1 IT Department – Disaster Recovery (DR) Plan 47](#_Toc406435778)

[**7 Conclusion 50**](#_Toc406435779)

[**APPENDIX A: Project Proposal Approval 51**](#_Toc406435784)

[APPENDIX B: Works Cited 52](#_Toc406435785)

# ****1 Introduction****

## 1.1 Proposal

As we look to the future, we have to think with the current trend of technology. Our business is looking to expand its operations and we have to look at feasible ways to do this. One of the ways to accomplish this mission would be to upgrade our current information technology into the next generation of wireless technology.

### ****1.2 Current Configuration****

Currently, all our offices are equipped with a combination of desktops and laptops. What we are proposing is that we integrate a form of wireless technology into the company. Currently, company data is stored on a server connected to an existing wired network and shares are managed by a Microsoft Domain Controller. The software controls access with role-based authenticated control (RBAC) with user login-host authentication and handled by a RADIUS Server. The network control is physically safeguarded in the data room with restricted access. Logical security is provided by two Security Devices providing hardware firewalls for controlling packet transmission for hosting the company website in a DMZ zone, between the LAN and the Internet. A diagram of the equipment is presented in succeeding chapters.

# ****2 Design of the Wireless Network****

### ****2.1 Planned Configuration****

We will be implementing a Wi-Fi refresh for both the existing building and the new building. The new implementation will consist of newer 802.11AC Wi-Fi standard access point which will be the newest standard in Wi-Fi technology, and will theoretically achieve speeds of up to 1300 Mbps. Additionally, as there will be an additional building with no means of running a physical link between the two, a highly directional antenna will be placed on the roof of each building. These antennae will be capable of near or 1 gigabyte per second speeds.

There will also be the addition of newer software based wireless controllers that will be brought online with existing hardware for each building. With the addition of these controllers, the Wi-Fi implementation will be much easier to implement as well as being able to incorporate newer technologies such as roaming capabilities.

The only upgrade to the existing infrastructure will be the addition of two new wireless routers that will add an additional layer 3 boundary between the two buildings. All existing hardware can be utilized to populate the new building.

Assemble a plan to implement a Wireless Local Area Network (WLAN) at the expanding headquarters of the Insurance Company. The system will provide additional service for Internet connectivity when the company expands from the current population of 100 employees to 300 employees.

The planned configuration will implement the WLAN, as an addition, to connect to the wired systems of the current configuration. The design of the planned configuration takes into account safety, security, performance, scalability, and value.

### **2.2 Assumptions and Constraints**

The planned configuration carries some assumptions and constraints for the following factors:

* Safety – Protection against the dangers of lightning strikes and electrical shorts
* Performance – High data transfer rates achieved by optimizing 802.11ac technology, good signal reception in a complete coverage area, and building-to-building bridging will ensure uninterrupted service throughout the facility
* Scalability – WLAN Controller has the capacity for expanded demand via increasing the quantity of Access Points (APs) and/or simultaneous client connections.
* Value – Costs versus features will meet the decisions of desired system capabilities
* Schedule – Phases of implementation will be on-time and certified operational

### ****2.3 System Organization****

The system structure consists of the following major system components:

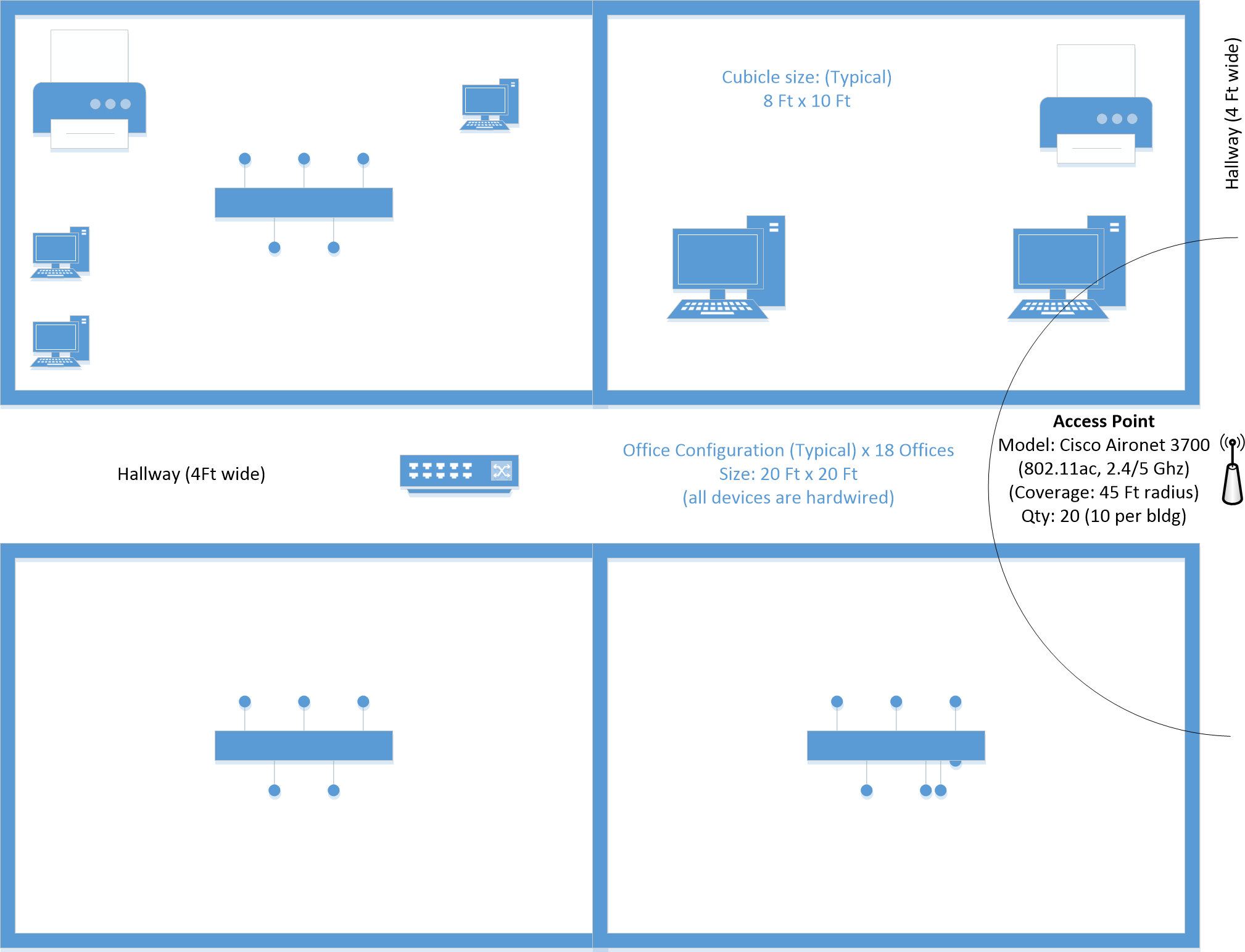
* Hardware – WLAN Controller (primary), WLAN Controller (secondary), Access Points (Omni-directional), Access Points (Semi-Directional), inter-building external antennas (Highly-directional), lightning rods and spark arrestors, cabling and connectors, test and monitoring equipment.
* Software – WLAN Controller management software, test and monitoring equipment software, software licenses
* Scalability – The WLAN Controllers will have the capacity for expanded demand via increasing the quantity of Access Points (APs) and/or simultaneous client connections.
* Value – Light-weight access points. Primary and secondary controllers with fail-safe over.
* Schedule – Phases of implementation will be on-time and certified operational

### ****2.4 Hardware-Network Diagrams (Visio)****

Existing wired network is managed by a Microsoft Domain Controller, host authentication is handled by a RADIUS Server, and two Security Devices provide hardware firewall for a DMZ zone between the LAN and the Internet. All the equipment is centrally located in the data room and is connected to the proposed Wireless LAN Controller device and routers. The routers are connected to the access points with existing node cabling but additional networks will be anticipated.



Existing Wired Network Servers and Routers in the Data Room



The access points (APs) have reliable transmit/receive capability of a 45 foot radius so the design incorporates a 10% margin for the placement of APs with a 40 foot radius coverage.



APs placement and signal overlap will ensure 100% coverage. The highest amount of data throughput is the goal. Throughput will drop if poor signal quality causes the stations (nodes) to retransmit because they couldn’t hear the APs’ ACK signal.

Some connection needs require higher throughput other than the normal BSS, like VoIP (Voice) or multimedia streaming. These higher needs can be serviced with a higher priority by configuring the equipment and program applications to take full advantage of the 802.11e or WMM for priority access.

For security, the WLAN will have a Wi-Fi Protected Access (WPA) certification and will broadcast the 802.1X/EAP framework. Some connections will require higher levels of security and there will be a RADIUS server for further authentication.



An outside bridge is a point-to-point link for the wireless LAN distribution mode between the two buildings. The line of sight (LOS) between the two semi-directional grid antennas will have to be adjusted to determine the RF LOS and the effects caused by multipath interference.

The RF beams’ Fresnel zone has 20 feet clearance from the ground midway of the span. This avoids reflection and multipath interference from metal surfaces. Obstacles are avoided, such as the metal fence, tall trees, and tall delivery trucks are rerouted to a side entrance.

## ****2.5 Site Survey Access Point Form – Completed****



Site Survey Access Point Form is accompanied with a coverage layout (shown above). Link budget calculations will be performed when evaluating RF coverage holes, found during the site survey. There are potential problems from the near/far phenomena where far nodes are weak or drowned out by near nodes. Power adjustments, AP relocations, and node relocations are some of the actions to fine-tune the Quality of Service (QOS) of the wireless

**Site Survey Access Point Form**

Engineers Name/Email: Glen Sayarot, hardwaredude@gmail.com

Mike Fetick, mikefetick@gmail.com

Customer Name: National Insurance Company

Job Number: 20141218

AP Name: (20): Bldg1-east01 thru Bldg1-east10; Bldg1-west01 thru Bldg1-west10

(20): Bldg2-east01 thru Bldg2-east10; Bldg2-west01 thru Bldg2-west10

(10): Reserved for coverage enhancement

*(50): Total = Capacity of WLAN Controller*

This AP Name:

AP Make/Model: (Typical) Cisco Aironet 3700 Series AP

AP Type: (Typical) 802.11ac Dual-Band

**AP Role in Network:** Root Repeater Bridge

**Wiring Closest:** (Name/Location/Number)

**Data Cabling:** (from AP to Wiring Closest)

Cable Type/Length (Typical) Cat-6,

Existing Network Connectivity Type: (Typical) 100baseTx Switch

Ethernet Switch: Manufacturer/Model: (Typical) Cisco Nexus 5548 Layer 3 Switching Module

IP Address (managed): Port Number:

**Survey Data Rates:** Existing Wired LAN - 802.11g (25 Mbps),

Proposed Wireless LAN - 802.11ac Wave 1 (750 Mbps)

Total Throughput Required Through AP: (Typical) 375 Gbps +/- 25 Mbps

**Prevailing Traffic Types (For QoS Purposes) (Circle for this AP)**

x FTP

x HTTP

x VoiP

x Video

x Telnet/SSH

x File Sharing

x POP/SMTP

x Data Backup

x Database Access

x Warehouse Data

x Instant Messaging

x Non-IP Protocols

x Routing Protocol

**Types of Clients that will connect:**

x Mobile Scanners

x Laptop PC

x Desktop PC

x Tablet PC

x VoiP Phones

x Mobile Printers

x Other

**Channels (Circle):**

01, 02, 03, 04, 05, 06, 07, 08, 09, 10,

11, 12, 13, 14, 36, 40, 44, 48, 52, 56,

60, 64, 149, 153, 157, 161, 165

Output Power (mW or dBm):

Antenna Type & Gain:

Pigtail Cable (on external antennas):

Power Cabling:

Surge Protection: Yes No

PoE Injector (single, multiple)

Lightening Protection (type, ohms)

RF Cabling & Connectors (type, length, ohms) \_

Mounting Location:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Building/Floor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Floor Plan I Map Grid Reference:

Mounting height

Mounting Gear Required:

Identifying Landmarks *I* Items around AP:

**Plenum Rating Required?** \_\_\_\_\_Yes \_\_\_\_\_No

**AP Housing Type:**

\_\_\_\_\_\_NEMA Enclosure \_\_\_\_\_\_Lockable Enclosure \_\_\_\_\_\_None

Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**AP Mounting Information**

YES\_\_\_\_Wall \_\_\_\_Mast \_\_\_\_Ceiling \_\_\_\_Tower \_\_\_\_Enclosure \_\_\_\_\_Roof

Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_Ladder required

\_\_\_\_ Lift Required

\_\_\_\_Tower Climber Required

Polarization: Vertical Horizontal Circular Phased-Array

Other \_\_\_\_\_\_\_\_\_\_\_

Orientation/Alignment \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mounting Gear Required\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Notes\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Measurement Points:**

Point 1: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Values: Signal\_\_\_\_\_\_\_ Noise\_\_\_\_\_\_\_ SNR\_\_\_\_\_\_\_ Other \_\_\_\_\_\_\_\_

Interference: \_\_\_\_\_\_Narrowband \_\_\_\_\_WLAN \_\_\_\_\_ ISM Equipment

Other\_\_\_\_\_\_\_\_

Notes\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Point 2: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Values: Signal\_\_\_\_\_\_\_ Noise\_\_\_\_\_\_\_ SNR\_\_\_\_\_\_\_ Other \_\_\_\_\_\_\_\_

Interference: \_\_\_\_\_\_Narrowband \_\_\_\_\_WLAN \_\_\_\_\_ ISM Equipment

Other\_\_\_\_\_\_\_\_

Notes\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Point 3: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Values: Signal\_\_\_\_\_\_\_ Noise\_\_\_\_\_\_\_ SNR\_\_\_\_\_\_\_ Other \_\_\_\_\_\_\_\_

Interference: \_\_\_\_\_\_Narrowband \_\_\_\_\_WLAN \_\_\_\_\_ ISM Equipment

Other\_\_\_\_\_\_\_\_

Notes\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Known Dead Spots:**

Point 1: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Caused by:­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Suggestion:­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Point 2: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Caused by:­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Suggestion: ­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Point 3: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Caused by:­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Suggestion: ­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Obstacles in the immediate environment:**

\_\_\_\_\_Metal Blinds \_\_\_\_\_Fire doors \_\_\_\_\_Metal mesh windows

\_\_\_\_\_HVAC \_\_\_\_\_Duct work \_\_\_\_\_Fire wall

\_\_\_\_\_Elevator \_\_\_\_\_Machinery \_\_\_\_\_Warehouse shelves/good

\_\_\_\_\_Pipes

Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Environment where AP will be placed:**

\_\_\_\_\_Open office space \_\_\_\_\_\_Office with cubicles \_\_\_\_\_ Warehouse I Distribution

\_\_\_\_\_\_Retail Sales \_\_\_\_\_\_\_Freezer/Cold Storage \_\_\_\_\_Hallway /Corridor

\_\_\_\_\_\_Manufacturing \_\_\_\_\_\_outdoors

Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Elements to which the AP will be exposed:**

\_\_\_Heat \_\_\_Cold \_\_\_Fluctuating Temperature \_\_\_\_Rain/Snow

\_\_\_Dirt/Dust \_\_\_Grease \_\_\_Chemicals \_\_\_Sunlight \_\_\_Vibration \_\_\_Wind

Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Notes: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Configuration Information:

AP Management Information:

HTTP \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telnet\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SSH/SSH2\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SNMP \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Console/Serial Port\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Custom Application­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Wireless VLANs:**

ESSID\_\_\_\_\_\_\_\_\_ VLAN\_\_\_\_\_\_\_\_ ESSID\_\_\_\_\_\_\_\_\_ VLAN\_\_\_\_\_\_\_\_

ESSID\_\_\_\_\_\_\_\_\_ VLAN\_\_\_\_\_\_\_\_ ESSID\_\_\_\_\_\_\_\_\_ VLAN\_\_\_\_\_\_\_\_

ESSID\_\_\_\_\_\_\_\_\_ VLAN\_\_\_\_\_\_\_\_ ESSID\_\_\_\_\_\_\_\_\_ VLAN\_\_\_\_\_\_\_\_

ESSID\_\_\_\_\_\_\_\_\_ VLAN\_\_\_\_\_\_\_\_ ESSID\_\_\_\_\_\_\_\_\_ VLAN\_\_\_\_\_\_\_\_

IP Address:

MAC Address (Ethernet):

MAC Address (802.11a):

MAC Address (802.11g):

ESSID:

**Authentication/Encryption:**

\_\_\_\_\_802.1X/LEAP \_\_\_\_\_802.1X/EAP-TLS \_\_\_\_\_802.1X/PEAP

\_\_\_\_\_802.1X/EAP-TTLS \_\_\_\_\_802.1X/EAP-MD5 \_\_\_\_\_WPA2/802.11i

\_\_\_\_\_EAP-Kerberos \_\_\_\_\_L2TPVPN \_\_\_\_\_KeyGuard

\_\_\_\_\_WPA-PSK \_\_\_\_\_CCMP/AES \_\_\_\_\_ WPA-RADIUS

\_\_\_\_\_TKIP/RC4 \_\_\_\_\_ PPTPVPN \_\_\_\_\_IPSec VPN

\_\_\_\_\_802.1X/EAP-TTLS

**Authentication Server Type:**

\_\_\_\_\_RADIUS \_\_\_\_\_LDAP \_\_\_\_\_Active Directory/Kerberos

Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Pictures of Access Point Mounting:**

In the following fields, record the name and description of each digital photograph taken.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Pictures of Custom Mounting Equipment (if required)**

In the following fields, record the name and description of each digital photograph taken.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## ****2.6 Site Survey Questionnaire Form – Completed****

**Site Survey Questionnaire B**

Customer Name: Point of Contact:

Address:

Main Facility

Phone Number:

Contact Direct

Phone Number:

Contact Cell

Phone Number:

Contact Email

Address:

Contact Fax

Number:

**Interview type:** In Person Phone Email

**Site Survey Definition**

A site survey is a task-by-task process by which the surveyor discovers and records the RF behavior throughout a facility. This information includes coverage, interference, and proper hardware placement within the facility. Site surveying involves analyzing a site from an RF perspective to determine what kind of RF coverage and hardware is required for a facility to meet the business goals of the customer.

**Existing RF Network Information**

Has a site survey ever been performed at this facility prior to today?

YES NO

Will any previous site surveys be made available to our staff?

YES NO

Existing Equipment at customer premises (Choose all that apply)

802.11B 802.11A 802.11G

Other:

How many existing users on the Wireless LAN?

What are the maximum users that are expected to be on the WLAN in the near future?

6 months:

12 months:

24 months:

Are there any peak and/or off-peak times at which certain users access the wireless LAN more than other times?

YES NO

What are the peak times? to AM/PM

What are the off peak times? to AM/PM

How many users does a typical access point support during peak use?

HOW many access points are currently in place?

What brands of access points and wireless bridges are currently in place?

Are there any existing contracts for certain brands of wireless LAN hardware in place?

YES NO

Are the existing access points performing load balancing?

YES NO

What kind of Wireless LAN security solution(s) are currently in place? (Select all that apply)

None Kerberos EWG

WEP RADIUS EEG

LEAP LDAP Firewall

EAP-TLS Active Directory Router/L3 Switch

EAP-TTLS NDS Other:

PEAP VPN

VLANs WVPN

What type of wireless LAN environment is currently in place? (Choose all that apply)

Campus

In-building

Building-to-Building

MAN

Other:

Current problems with the existing wireless LAN? (Choose all that apply)

Slow throughput

Frequent disconnects

Difficulty roaming

Logon problems

Other (explain thoroughly, and include documentation if available):

If the existing WLAN is having problems, has any troubleshooting of the existing problems been performed yet?

YES NO

Are there any known sources of RF in or around the facility?

YES NO

Source 1:

Source 2:

Source 3:

Are there any known RF dead zones?

YES NO

If yes, attach documentation showing location(s) of dead zone(s).

**RF Network Design**

What applications are/will be used over the wireless LAN?

Voice

Video

Connection-oriented Data

Connectionless Data

Other:

Do users need to roam across routed (layer 3) boundaries?

YES NO

What types of wireless client devices will be used?

Laptops

Desktops

Handheld/PDA

Scanners

Thin Clients/Terminals

Other:

Are clients mounted on vehicles of any type?

YES NO

Explain:

Is wireless printing a requirement?

YES NO

Explain:

What network protocols and traffic types are in use over the wireless LAN?

IP

IPX

Routing protocols

Internet traffic

Other:

Are switches or hubs used for network access?

Switches

Rubs

Are there enough available network access ports to accommodate the access points?

YES NO

Are access points to be powered directly by AC power sources or is

Power over Ethernet going to be used?

AC PoE

What subnet(s) will be assigned to the wireless network?

Private IP subnet

Public IP subnet

Subnet Information:

Will a naming scheme for wireless infrastructure devices be provided by the customer?

YES NO

Describe the naming conventions, and/or provide examples or naming convention documentation.

How will the wireless network be managed?

SNMP

HTTP/HTTPS

Telnet

Console/Serial port

Custom application

**Site Survey Request**

What type of site survey is necessary?

Indoor Outdoor

Will production application analysis be required? (Without this analysis, proper application functionality cannot be guaranteed.)

YES NO

Application(s):

If indoors, what kind of facility?

Warehouse

School

Multi-tenant Office Building

Manufacturing Plant

Hospital

Other:

If outdoors, is this a point-to-point or point-to-multipoint connection? What distance(s)?

Point-to-Point

Point-to-Multipoint

Are there other organizations in or around your building using wireless?

LANs?

YES NO

Need verification:

Are Blueprints, Floor Plans, Campus Map, or other Topology Map available?

YES NO

Which technology is the customer considering for the new installation? (Choose all that apply)

802.11A

802.11B

802.11G

Other:

Expected or Required Data rate (in Mbps)

**802.11A**

6 9 12 18 24 36 48 54 Proprietary:

**802.11B**

1 2 5.5 11

**802.11G**

1 2 5.5 11 6 9 12 18 24 36 48 54

Other:

Additional information:

**Special Stipulations**

HIPAA:

US Government

State Government:

Workers Union:

OSHA:

Other:

# ****3 Component Specifications of the Wireless Network****

## ****3.1 Hardware Network Controllers****



(2) Cisco 5508 Wireless Controller (AIR-CT5508-50-K9)

(List: $15,680) Amazon: $6,500 x 2 = $13,000

Cisco 5500 Series Wireless LAN Controller—This Cisco AireOS-based controller supports up to 500 lightweight access points and 7000 clients, making it ideal for large-site and multi-site WLAN deployments. High availability is supported through Stateful Switchover (SSO), which provides subsecond controller failover without requiring the wireless client to re-authenticate.

## ****3.2 Hardware Routers and Switches****

Cisco Nexus 5548 Layer 3 Switching Module (Part No. N55-D160L3)



(List: $6,500) router-switch.com: $3,200 x 1 = $3,200

With Software: NX-OS 5.2(1)N1(3) Layer 3 License

The 802.11ac Clear Carrier Assessment threshold values:

-82dBm -72 dBm (10 dB liberty)

-76 to -79 (3-6 dB liberty)

Any primary operating within a secondary 20 or 40 will lose contention and any secondary 20 operating in a secondary 40 will win contention over the other secondary.

## ****3.3 Hardware Security Equipment (Firewall)****



(1) Cisco ASA 5512-X IPS Edition - security appliance (ASA5512-IPS-K9).  
(List: $3,200) Amazon: $1,730 x 1 = $1,730

This is in addition to the wired LAN’s existing SonicWall Firewall

## ****3.4 Hardware Wireless Access Points****



(50) Cisco Aironet 3700 Series AP

(List: $1,495) Amazon: $720 x 30 = $36,000

**Cisco Lightweight Access Points.**

Cisco Aironet 3600 Series Access Point using the 802.11ac Wave 1 Adaptive Radio Module (AIRRM30000AC-x-K9). Installing the 802.11ac adaptive radio module for the Cisco Aironet 3600 Series Access Point provides enterprise-class reliability and wired-network-like performance by supporting three spatial streams and 80-MHz wide channels for a maximum data rate of 1.3 Gbps.

In the Cisco Unified Wireless Network architecture, access points are lightweight. This means they cannot act independently of a wireless LAN controller (WLC). The lightweight access points (LAPs) have to first discover the WLCs and register with them before the LAPs service wireless clients. The primary way that the access point can discover a WLC is by creating a DNS entry for cisco-capwap-controller that resolves to the management IP addresses of WLCs.

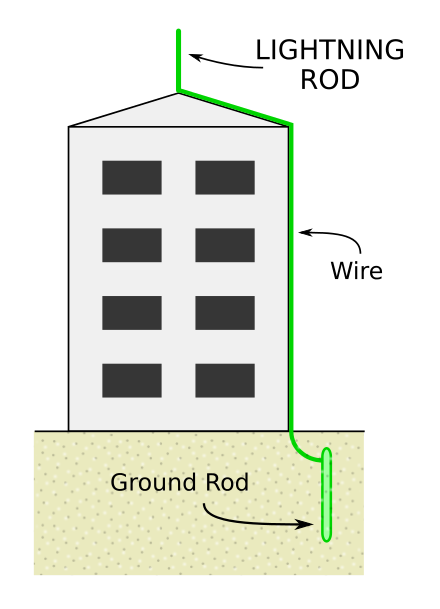
## ****3.5 Hardware Cabling and Connectors****



(2) 1000 ft. Cat.6 Plenum (CCA) Ethernet Cable, UTP 550 MHz,

(List: $72) Amazon: $225 x 2 = $450

## ****3.6 Hardware Lightening Protection Equipment****



(2) Lightening Rod Installation - [www.fixr.com](http://www.fixr.com)

Local electrician typically $2,500 x 2 buildings = $5,000

## ****3.7 Hardware Outdoor Antennas****



(2) Cisco Bridge AIR-XLTC50DA31AK9 ExtendAir r5005, 5 GHz Outdoor Bridge w/Ant, A Reg Domain

(List: $5,200) router-switch.com: $5,200 x 2 = $11,400



(2) Highly Directional Antennas (Wireless Bridge)

5.8 GHz 29aBi Die Cast Aluminum Reflector Grid Antenna

L-com Item # HG5829EG: $70 x 2 = $140

## ****3.8 Hardware Outdoor Cameras****



(2) Samsung SDE-3004N 4 Channel DVR Security System with 500 GB HDD. One for each building. (List: $400) Amazon: $250 x 2 = $500

## ****3.9 Cost-Budget (Hardware Cost Break-Down)****

(2) Cisco 5508 Wireless Controller (AIR-CT5508-50-K9) $13,000

(1) Cisco Nexus 5548 Layer 3 Switching Module (Part No. N55-D160L3) $3,200

(1) Cisco ASA 5512-X IPS Edition - security appliance (ASA5512-IPS-K9) $1,730

(50) Cisco Aironet 3700 Series AP $36,000

(2) 1000 ft. Cat.6 Plenum (CCA) Ethernet Cable, UTP 550 MHz $450

(2) Lightening Rod Installation - [www.fixr.com](http://www.fixr.com) $5,000

(2) Cisco Bridge ExtendAir r5005, 5 GHz Outdoor Bridge w/Ant $11,400

(2) Highly Directional Antennas (Wireless Bridge) Grid Antenna $140

(2) Samsung SDE-3004N 4 Channel DVR Security System with 500 GB HDD $500

Miscellaneous items and supplies $2,000

System Design, Installation, Setup, and Certification $20,000

**Total: $93,420**

# ****4 Wireless Network Installation and Setup****

## ****4.1 Routing and IP Addresses****



## ****4.2 Software Configuration and Bootstrap Files****

The Cisco Nexus 5548 Layer 3 Switching Module is controlled by Cisco software, which is included: NX-OS 5.2(1)N1(3) with a Layer 3 License. The configuration files and bootstrap files will be edited by Microsoft Power Shell®. The existing network already has all the operating-system software for the Microsoft Domain Servers and web hosting on an Apache Tomcat server.

## ****4.3 Software Licenses and Account Management****

All licenses are paid and documented by the company and maintained on site. The software licenses are generally per seat on a roaming basis to achieve the best value. The Wired LAN Controllers can simultaneously handle 50 access points with 7000 client connections.

## ****4.4 Signal Coverage Validation – Power Measurements and Adjustments****

# Signal coverage will be validated with calibrated signal-strength measuring, power meters with frequency grouping and channel isolation capabilities. All test locations and results will be recorded and evaluated to determine complete coverage validation is done. Analysis of causes of reflections and obstacles, near/far conditions, and all other sources of interferences will be considered in the expedited positioning of APs, the adjustments of antenna positioning and polarization, amplification of transmission power for the optimal signal strength for all users in all areas. ****5 Policies Implementation****

## ****5.1 Information Technology (IT) Department – Network Operations Policy****

**Objective:**

Provide appropriate guidelines for utilization of desktop, laptop, tablets, and other wireless devices under the employ of National Insurance Company.

**Applies to:**

All employees with authorized access to any or all information devices under the employ of National Insurance Company.

**Key Guidelines:**

Information devices issued to employees for the transmitting, storage, and use of employees to include internet access must be used in a responsible manner. Information garnered from clients and employees alike must be protected from outside or unauthorized sources. The internet is a very valuable tool, but also creates security implications which the company must guard against. For this reason, employees are granted use of company computers and internet access only as a means of providing support in fulfilling their job responsibilities.

**General:**

* Desktops, laptops, tablets, and other wireless devices are issued for use to employees.
* Internet accounts are setup and approved for employee use by their immediate supervisor.
* Each employee is responsible for the account issued to them.
* The sharing of internet accounts or User-ID's is prohibited.
* Organizational use of computers and/or the internet services must reflect the mission of the company and support the company's goals and objectives.
* These services must support legitimate, mission related activities of the company and be consistent with prudent operational security and privacy considerations.
* The CIO led Internet Steering Committee will take responsibility for all web site content (i.e., “The company web-site”) and format presentation to reflect the company's mission and in supporting company and departmental objectives.
* The Company has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
* Any software or files downloaded via the internet into the company network become the property of the company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

**Inappropriate Use:**

* Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.
* Company provided electronic messaging resources may not be used for the promotion or publication of one’s political or religious views, the operation of a business or for any undertaking of personal gain.
* The current configuration consists of a wired LAN with no official wireless network. The possibility of personal, ad hoc wireless transmitters are considered to be **rogue systems** and can potentially interfere with the performance of the proposed WLAN system. Such rogue wireless systems will be prohibited.

## ****5.2 IT Department – Wireless Communication Policy****

**Overview:**

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is commonly found in any organization. Insecure wireless configuration can provide an easy open door for malicious threats.

**Purpose:**

The purpose of this policy is to secure and protect the information assets owned by National Insurance Company. National Insurance Company provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. National Insurance Company grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to National Insurance Company’s. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a National Insurance Company network.

**Scope:**

All employees, contractors, consultants, temporary and other workers at National Insurance Company, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of National Insurance Company must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a National Insurance Company network or reside on a National Insurance Company site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

**Policy:**

General Requirements:

* All wireless infrastructure devices that reside at a National Insurance Company site and connect to our network, or provide access to information classified as National Insurance Company Confidential, or above must:
* Abide by the standards specified in the Wireless Communication Standard.
* Be installed, supported, and maintained by an approved support team.
* Use National Insurance Company approved authentication protocols and infrastructure.
* Use National Insurance Company approved encryption protocols.
* Maintain a hardware address (MAC) that can be registered and trscked.
* Not interfere with wireless access deployments maintained by other support organizations.

**Policy Compliance:**

Compliance Measurement: The InfoSec team will verify compliance to this policy through various methods, including but not limited to periodic walk-thru, video monitoring, business tool reports, internal and external audits, and feedbacks to policy owner.

**Exceptions:**

Any exception to the policy must be approved by the InfoSec team in advance.

## ****5.3 IT Department – Software Usage Policy****

**Objective:**

Provide guidelines on appropriate use of software products utilizing company equipment

**Applies to:** All employees

**Key guidelines:**

This policy is intended to ensure that all company employees understand that no computer software may be loaded onto or used on any computer owned or leased by the company unless the software is the property of or has been licensed by the company.

**General:**

* Software purchased by the company or residing on company owned computers is to be used only within the terms of the license agreement for that software title.
* Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to the company's Software Usage Policy.
* To purchase software, users must obtain the approval of their department manager who will follow the same procedures used for acquiring other company assets.
* All approved software will be purchased through the Purchasing Department.
* The CIO and designated members of the IT Department will be the sole governing body for defining appropriate software titles acceptable for use in the company.
* Under no circumstances will third party software applications be loaded onto company owned computer systems without the knowledge of and approval of the IT Department.
* Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any company user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.
* The company does not condone the illegal duplication of software in any form.

**Compliance:**

* We will use all software in accordance with its license agreements.
* Under no circumstances will software be used on company computing resources except as permitted in the company's Software Usage Policy.
* Legitimate software will be provided to all users who need it. Company users will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to termination.
* Each user of software purchased and licensed by the company must acquire and use that software only in accordance with the company's Software Usage Policy and the applicable Software License Agreement.
* All users acknowledge that software and its documentation are not owned by the company or an individual, but licensed from the software publisher.
* Employees of the company are prohibited from giving company acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.
* All software used by a company entity for company owned computing devices, or purchased with company funds, will be acquired through the appropriate procedures as stated in the company Software Usage Policy.
* Any user who determines that there may be a misuse of software within the organization will notify the software manager or department manager.

**Registration of Software:**

* Software licensed by the company will not be registered in the name of an individual.
* When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of the company with the job title or department name in which it is used.
* After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of the company. A copy of the license agreement will be filed and maintained by the IT Department's Software License Administrator.
* Once installed, the original installation media should be kept in a safe storage area designated by the IT Department.
* Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. The company's policy is to pay shareware authors’ fees for use of their products if the software will be used at the company. Installation and registration of shareware products will be handled the same way as for commercial software products.

**Software Audit:**

* IT will conduct periodic audits of all company owned PCs, including laptops, to insure the company is in compliance with all software licenses.
* Audits will be conducted using an auditing software product.
* Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer.
* During these audits, the software manager will search for computer viruses and eliminate any that are found.
* The full cooperation of all users is required during software audits.

## ****5.4 IT Department – Network Security Policy****

**Objective:**

Provide guidelines on maintaining the highest level of security for our physical office assets and employees.

**Applies to:** All employees

**Key guidelines:**

The company provides keys and password access for use by staff to maintain building and office security and allow access to designated areas for authorized personnel during normal business hours and after hours.

* Physical security of company employees and assets is a primary objective of the company. This policy is intended to help provide a safe and secure work environment, prevent theft, and to provide a procedure for appropriate distribution and collection of keys and maintenance of accurate security access code logs.
* The official business hours of the company buildings are Monday through Friday, 8:00 A.M. to 5:00 P.M. (except for official holidays).
* Within reason and practical limits, employees having visitors must escort them when inside the building.
* Building Security Officers may issue special permission for individuals to be in the building without the presence of a staff member. Such cases will include announced meetings held in the company Conference Room such as Policy Board Meetings, designated vendor support calls, and consultants that work with the company from time to time.
* After business hours, visitors are subject to being challenged by staff members and required to identify themselves and their purpose in the building. Employees must share in the responsibility of questioning these unescorted visitors and reporting any unauthorized personnel to the Building Security Officer.
* Company keys are the property of the company.
* Managers may request building keys for authorized employees and will be responsible for collecting the key upon an employee separating from the company.
* Keys will be assigned by employee name. Each individual assumes responsibility for protecting the security of his/her key and will report losses or situations that possibly jeopardize building security to his/her manager.
* It is each Department Head's responsibility to insure that building keys are only given to those few employees that require after-hours access to the building for business purposes.
* Lost keys must be reported to the issuing department within 24 hours of loss.

**The following actions are in violation of this policy:**

1. Loaning keys without authorization
2. Duplicating keys
3. Altering keys, locks, or mechanisms
4. Admitting unauthorized persons into building
5. Failure to return a key when requested by Security Services, authorizing department, or upon leaving the company.

* All company employees need to be concerned with building lock-up and to ensure that when entering and leaving the building, after normal business hours, the doors and office windows are locked.
* If an alarm system is present it is the responsibility of the last person leaving to set the alarm.
* Visitors are not allowed access to the IT Operations Center (computer room) without prior authorization. This advance authorization may be obtained by contacting the Manager of Operations.

Any concerns, questions or comments regarding this policy or interpretation of this policy should be directed to a member of the management team.

## ****5.5 IT Department – Security Incident Reporting and Response Policy****

**Overview:**

Information and Technology Response Procedures are in place for the protection of employees and clients of National Insurance Company. It is in place for the principle purpose of preserving the confidentiality, integrity and availability of our enterprise information assets. An effective Security Incident Response program provides a means of dealing with unexpected circumstances in such a way as to minimize impact to National Insurance Company. It also provides management with sufficient information on which to base an appropriate course of action.

**Department Responsibility in Reporting and Responding to an IT Security Incident:**

There are many different kinds of IT Security Incidents and different departments will become involved in the remediation of the incidents. It is the responsibility of the department to report an incident to the appropriate department. Anything considered criminal activity should be reported to the Company CISO.

Employee misconduct, both criminal and otherwise should also be reported to Human Resources. Incidents of a technical nature usually deriving from an external source should be reported to the CISO Director of Information Security and Privacy. All National Insurance Company data, regardless of the format or medium of the record should be classified into one of three sensitivity levels categories:

Level 1 – Protected

Level 2 – Private

Level 3 – Public

The data classification level of information involved in an incident is an important component in the process of timely risk mitigation in the response process.

**Types of IT Security Incidents reported to the CISO:**

1. Electronic transmission/storage of child pornography
2. Electronic transmission of threats to the physical safety of human beings or physical assets.
3. Harassment and other criminal offenses involving individual user accounts.
4. Loss or theft of computer device (s).
5. Use of National Insurance Company computing resources in the commission of a fraudulent activity against the Company, individual, or outside entity.
6. Incidents involving a breach of Criminal Justice Information Services information.

**Types of Minor Security Incidents:**

Virus infections on servers and end-points that do not contain data classified as “Protected” or “Private” or are not used to process “Protected” or “Private” data in a public location such as a kiosk.

**IT Security Incident Debriefing:**

One of many important issues in incident response is usually the most omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Holding a “Lessons Learned” meeting with all involved parties after major incidents, as well as periodically after lesser incidents can be extremely helpful in improving security measures and the incident handling process itself. Questions to be answered during these meetings should include:

* Exactly what happened, and at what times?
* How well did staff and management perform in dealing with the incident?
* Were the documented procedures followed?
* Were they adequate?
* What information was needed sooner?
* Were any steps or actions taken that might have inhibited the recovery?
* What would the staff and management do differently the next time a similar incident occurs?
* How could information sharing with other organizations have been improved?
* What corrective actions can prevent similar incidents in the future?
* What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

**Summary:**

Information security is paramount to National Insurance Company. It is the responsibility of every individual associated with National Insurance Company to adhere to all regulations dealing with the policies regarding Information Technology. Any incident no matter how minor should be reported to the individual’s proper reporting contact.

# ****6 Contingencies & Unforeseen Events****

## ****6.1 IT Department – Disaster Recovery (DR) Plan****

**Overview:**

An information technology (IT) disaster recovery (DR) plan provides a structured approach for responding to unplanned incidents that threaten an IT infrastructure, which includes hardware, software, networks, processes and people. Protecting the firm's investment in its technology infrastructure, and protecting the firm's ability to conduct business are the key reasons for implementing an IT disaster recovery plan.

**Audience:** All personnel involved with National Insurance Company.

**Policy and Procedures:**

***\*Due to the possible length of an actual Information Technology Disaster Recovery Plan, we will be using one of many possible templates of what would go into an actual Disaster Recovery Plan.***

According to National Institute for Standards and Technology (NIST) Special Publication 800-34, Contingency Planning for Information Technology Systems, the following summarizes the ideal structure for an IT disaster recovery plan:

**1. Develop the contingency planning policy statement:** This is a formal policy which provides the authority and guidance which is necessary to develop an effective contingency plan.

**2. Conduct the business impact analysis (BIA):**  The business impact analysis helps to identify and prioritize critical IT systems and components.

**3. Identify preventive controls:**  These are measures that reduce the effects of system disruptions and can increase system availability and reduce contingency life cycle costs.

**4. Develop recovery strategies:**  Thorough recovery strategies ensure that the system can be recovered quickly and effectively following a disruption.

**5. Develop an IT Contingency Plan:**  The contingency plan should contain detailed guidance and procedures for restoring a damaged system.

**6. Plan Testing, Training and Exercising:**  Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.

**7. Plan Maintenance:**  The plan should be a living document that is updated regularly to remain current with system enhancements.

**Step-by-step IT DR plan development:**

**1.** The plan development team should meet with the internal technology team, application team, and network administrator(s) and establish the scope of the activity, e.g., internal elements, external assets, third-party resources, linkages to other offices/clients/vendors; be sure to brief IT department senior management on these meetings so they are properly informed.

**2.** Gather all relevant network infrastructure documents, e.g., network diagrams, equipment configurations, databases.

**3.** Obtain copies of existing IT and network DR plans; if these do not exist, proceed with the following steps.

**4.** Identify what management perceives as the most serious threats to the IT infrastructure, e.g., fire, human error, loss of power, system failure.

**5.** Identify what management perceives as the most serious vulnerabilities to the infrastructure, e.g., lack of backup power, out-of-date copies of databases.

**6.** Review previous history of outages and disruptions, and how the firm handled them.

**7.** Identify what management perceives as the most critical IT assets, e.g., call center, server farms, Internet access.

**8.** Determine the maximum outage time management can accept if the identified IT assets are unavailable.

**9**. Identify the operational procedures currently used to respond to critical outages.

**10.** Determine when these procedures were last tested to validate their appropriateness.

**11.** Identify emergency response team(s) for all critical IT infrastructure disruptions; determine their level of training with critical systems, especially in emergencies.

**12.** Identify vendor emergency response capabilities; if they have ever been used; if they were did they work properly; how much the company is paying for these services; status of service contract; presence of service-level agreement (SLA) and if it is used.

**13.** Compile results from all assessments into a gap analysis report that identifies what is currently done versus what ought to be done, with recommendations as to how to achieve the required level of preparedness, and estimated investment required.

**14.** Have management review the report and agree on recommended actions.

**15.** Prepare IT disaster recovery plan(s) to address critical IT systems

**16.** Conduct tests of plans and system recovery assets to validate their operation.

**17.** Update DR plan documentation to reflect changes.

**18.** Schedule next review/audit of IT disaster recovery capabilities.

(Source: NIST SP 800-34)

**Summary:**

The Information Technology and Disaster Recovery Plan is important to all businesses and their infrastructures. These plans will cover all sorts of possible scenarios in dealing with the loss of information. From natural causes considered Acts of God, to man-made mistakes, to acts of terrorism, Disaster Recovery Plans must be made aware of to all personnel associated with their company. These plans must be adhered to and practiced for it to be effective. That being said; the best disaster recovery plan is the one never needed.

## ****7 Conclusion****

The National Insurance Company will be pleased to receive a turn-key solution to expanding their company Local Area Network with the additional of a high-speed wireless 802.11ac Local Area Network. The system will be designed for performance and value for complete customer satisfaction. The system will be implemented on schedule and on budget by timely procurement, professionally installation, and performance testing for a high-standard of system Quality of Service.

The Interceptors rely on good reputation and welcome endorsements from clients. Our customers are surveyed on all aspects of the system including, schedule, budget, quality of workmanship, courtesy, clean-up, attitude, responsive technical support, QoS of the products, suggestions and recommendations. A samples of our customers’ satisfaction can be reviewed at our website at [www.interceptors.com](http://www.interceptors.com).

*[In this proposal, all names of company and persons are fictitious.*

*If there exists any actual entities that have the same or similar names,*

*Then it should be considered just coincidental and not intentional.]*

## APPENDIX A: Project Proposal Approval

The undersigned acknowledge that they have reviewed the **Wireless Network Project Proposal** and agree with the information presented within this document. Changes to this **Wireless Network Project Proposal** will be coordinated with, and approved by, the undersigned, or their designated representatives.

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: |  | Date: |  |
| Print Name: |  |  |  |
| Title: |  |  |  |
| Role: | Project Manager |  |  |

APPENDIX B: Works Cited

|  |  |
| --- | --- |
| **Description** | **Location** |
| Cisco – Campus Wireless LAN, Technology Design Guide, April 2014 | <http://tools.cisco.com/search/results/display?url=http%3a%2f%2fwww.cisco.com%2fweb%2foffer%2fgrs%2f189097%2fen-05_campus-wireless_cvd_cte_en.pdf&pos=1&query=en-05_campus-wireless_cvd_cte_en> |
| Tech Tip- How to upgrade or extend the antennas on your WiFi access point or router | <http://www.l-com.com/content/how-to-upgrade-antennas-on-your-WiFi-access-point%20%20.html> |
| Designing and Deploying a Wireless Network | <http://www.l-com.com/content/Article.aspx?Type=L&ID=10091> |
| What is a Distributed Antenna System (DAS)? | http://www.l-com.com/customer-service?ID=4912 |
| Line of Sight (LOS) | http://www.l-com.com/content/Article.aspx?Type=L&ID=10060 |
| Low Loss Coax Cable Applications | http://www.l-com.com/content/Article.aspx?Type=L&ID=10046 |
| Common RF Coax Connectors - A Visual Guide | http://www.l-com.com/content/Article.aspx?Type=L&ID=10057 |
| 802.11 Wireless Standards | http://www.l-com.com/content/Article.aspx?Type=L&ID=10044 |
| United States Frequency Allocations Chart | http://www.ntia.doc.gov/files/ntia/publications/spectrum\_wall\_chart\_aug2011.pdf |
| dBm to Watts Conversion Chart | http://www.l-com.com/multimedia/whitepapers/dbm\_chart.pdf |
| Weatherproof NEMA Enclosure Applications | http://www.l-com.com/content/Weatherproof\_Enclosure\_Examples.html |
| Tech Tip- How to mount a WiFi antenna on the side of a building | http://www.l-com.com/content/how-to-mount-a%20wifi-antenna-on-the-side-of-a-building%20%20.html |
| Tech Tip- When Too Much Gain Is a Bad Thing | http://www.l-com.com/content/Article.aspx?Type=L&ID=10175 |
| Bandpass Filter Q & A | http://www.l-com.com/content/Bandpass\_Filters\_FAQ.html |