FRCH Design Worldwide: Wireless Network Upgrade
And Network Monitoring Solution

By

Andrew Burgess, Johnathan Riley and Jason Schuster

Submitted to
the Faculty of the Department of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

© Copyright 2013 Andrew Burgess, Johnathan Riley and Jason Schuster

The authors grant to the Department of Information Technology permission
to reproduce and distribute copies of this document in whole or in part.

Andrew Burgess, Johnathan Riley & Jason Schuster  4/16/2013
Date

Russell E' McMahon  4/16/2013
Professor Russell McMahon  Date
Acknowledgements

The project team of Andrew Burgess, Johnathan Riley and Jason Schuster would like to thank everyone who has helped us with our project over the last eight months. Without the guidance, support and input of these individuals we would have not been able to meet critical deadlines or perhaps even complete the project. First, we would like to thank Mike Rinken and Matt Davidson from FRCH for giving us an opportunity to tackle a real-world IT network project. They set clear goals and deliverables, gave us a budget and ultimately trusted us with access and the authority to make changes to critical systems on its infrastructure. Equally important, the leadership provided by the advisor faculty at the University of Cincinnati was indispensable. Patrick Kumpf made sure we were constantly and clearly aware of the next set of deliverables and provided us with the means to meet them. Russ McMahon kept us in-check and offered practical advice on how to deal with delays, scope changes and other adversity throughout the project. Finally, the following list of individuals provided us with an array of help from test equipment, to low-level product specifications, to technical insight and even directions on how to best implement some facets of our project. Thank you to: Jason Maloney, Tim Cornett, John Roberto, Todd Wind and Gerry Townsen, Dolph Smith, Kevin Lanard, Lincoln Russel, Matt Stanton, Kersean Rozier and Mike Trantham.
# Table of Contents

Acknowledgements............................................................................................................. i
Table of Contents.................................................................................................................. ii
List of Illustrations................................................................................................................. iii
List of Tables ........................................................................................................................... v
ABSTRACT............................................................................................................................... vi

1. INTRODUCTION .................................................................................................................. 1
   1.1. Background .................................................................................................................. 1
   1.2. The Problem ................................................................................................................ 3
   1.3. The Solution ................................................................................................................ 6
   1.4. Credibility ................................................................................................................... 10
   1.5. Project Goal ................................................................................................................ 10
   1.6. Overview ..................................................................................................................... 12

2. DISCUSSION ....................................................................................................................... 13
   2.1. Project Concept ........................................................................................................... 13
   2.1.1. Big Picture ............................................................................................................. 13
   2.1.2. Project Defined ....................................................................................................... 14
   2.1.3. Deliverables .......................................................................................................... 17
   2.1.4. Project Budget ....................................................................................................... 19
   2.2. Research ..................................................................................................................... 20
   2.3. Recommendation ...................................................................................................... 27
   2.4. Implementation ........................................................................................................... 30
   2.4.1. Technical Elements ............................................................................................... 34
   2.4.2. Methodology ......................................................................................................... 38
   2.4.3. User Profiles ......................................................................................................... 40
   2.5. Project Timeline ......................................................................................................... 42
   2.6. Problems Encountered .............................................................................................. 43

3. CONCLUSION .................................................................................................................... 47

4. REFERENCES ..................................................................................................................... 49

5. APENDICES ....................................................................................................................... 51
   5.1. Appendix A: List of Acronyms .................................................................................. 51
   5.2. Appendix B: Technologies List ................................................................................ 53
   5.3. Appendix C: Wireless Network Configuration Manuals ............................................ 54
   5.3.1. FortiGate Wireless Networks Configuration ........................................................... 54
   5.3.2. Access Point Configuration ................................................................................... 71
   5.3.3. RADIUS Configuration and Wireless Deployment ................................................ 79
List of Illustrations

Figure 1: Legacy FRCH Network Diagram ................................................................. 2
Figure 2: Legacy FRCH Heat Map, 3rd Floor ............................................................ 4
Figure 3: Pre-project Use Case Diagram ................................................................. 5
Figure 4: FortiGate Web Interface ........................................................................ 7
Figure 5: Fortinet FAP-320B ............................................................................. 7
Figure 6: AP Placement Design 1 ........................................................................ 9
Figure 7: AP Placement Design 2 ........................................................................ 9
Figure 8: Current FRCH Heat Map, 3rd Floor ....................................................... 9
Figure 9: Current FRCH Network Diagram .......................................................... 11
Figure 10: Team Member Responsibilities ............................................................ 16
Figure 11: Cisco 1041 AP .................................................................................. 21
Figure 12: Cisco WLC Interface ........................................................................... 21
Figure 13: Juniper WLA522 AP ......................................................................... 23
Figure 14: Juniper WLC8 Web Interface .............................................................. 23
Figure 15: Aruba IAP-105 AP ............................................................................. 25
Figure 16: Aruba IAP-105 Web Interface ............................................................. 25
Figure 17: Aruba Heap Map, FRCH 3rd Floor .................................................... 26
Figure 18: Fortinet FAP-320B ........................................................................... 28
Figure 19: FortiGate 200B Web Interface ............................................................ 28
Figure 20: AP Placement ................................................................................... 32
Figure 21: Installed Fortinet AP ......................................................................... 33
Figure 22: Current Heat Map, FRCH 3rd Floor .................................................. 34
Figure 23: Team Test Environment .................................................................... 35
Figure 24: Key Technical Elements ................................................................... 37
Figure 25: Post Project Use Case Diagram ............................................................ 41
Figure 26: Research Phase Timeline .................................................................. 42
Figure 27: Implementation Phase Timeline ............................................................ 43
Figure 28: FortiAP-320B Staged for Deployment ............................................... 45
Figure 29: FRCH 3rd Floor IDF ......................................................................... 46
Figure 30: FortiGate User Menu ......................................................................... 54
Figure 31: FortiGate RADIUS Options ................................................................. 55
Figure 32: RADIUS Test .................................................................................... 55
Figure 33: RADIUS Test Successful ................................................................... 56
Figure 34: LDAP Server Settings ........................................................................ 57
Figure 35: WLC SSID .......................................................................................... 57
Figure 36: WLC SSID Settings ............................................................................ 58
Figure 37: WLC Firewall Objects ........................................................................ 59
Figure 38: Creating Firewall Address Object for FRCH-Private SSID ............ 59
Figure 39: Creating DHCP Server on FortiGate 200B ................................................................. 60
Figure 40: DHCP Server Settings on FortiGate 200B ...................................................................... 60
Figure 41: FortiGate 200B User Menu .............................................................................................. 61
Figure 42: User Group Settings ....................................................................................................... 62
Figure 43: Guest-Admin Group Settings ......................................................................................... 63
Figure 44: System Admin Menu ...................................................................................................... 63
Figure 45: Admin Profile Options ................................................................................................... 64
Figure 46: System Admin Menu ...................................................................................................... 65
Figure 47: Administrator Settings .................................................................................................. 66
Figure 48: FRCH-Public SSID Settings .......................................................................................... 67
Figure 49: FRCH-Public Firewall Address Object .......................................................................... 67
Figure 50: DHCP Server Options for FRCH-Public SSID ............................................................... 68
Figure 51: Custom AP Profile Settings ........................................................................................... 68
Figure 52: Custom AP Profile Settings, Radio 1 ............................................................................. 69
Figure 53: Custom AP Profile Settings, Radio 2 ............................................................................. 70
Figure 54: Serial Connection to AP using Putty .............................................................................. 71
Figure 55: Managed AP List ........................................................................................................... 72
Figure 56: Authorized AP ................................................................................................................ 73
Figure 57: Setting AP Custom Profile ............................................................................................. 73
Figure 58: Managed FortiAP List .................................................................................................... 74
Figure 59: FortiGate 200B Firewall Policy ....................................................................................... 74
Figure 60: Firewall Policy Settings for FRCH-Public SSID to Access the Internet ......................... 75
Figure 61: Firewall Policy Settings for FRCH-Private SSID to Access the Internet ....................... 76
Figure 62: Firewall Policy Settings for FRCH-Private SSID to Access the Server Farm ............... 77
Figure 63: Windows Server 2008 R2 Sever Roles ......................................................................... 78
Figure 64: Network Policy and Access Services Options .............................................................. 79
Figure 65: Network Policy Server .................................................................................................. 80
Figure 66: RADIUS Client Options ............................................................................................... 81
Figure 67: Network Policy Server Wizard ...................................................................................... 82
Figure 68: Network Policy Server Wizard 802.1X ......................................................................... 82
Figure 69: Network Policy Server Wizard add RADIUS Client ...................................................... 83
Figure 70: Network Policy Server Wizard Authentication Method Selection .................................. 83
Figure 71: Network Policy Server Wizard Add User Group ............................................................ 84
Figure 72: Network Policy Server Wizard Traffic Controls ............................................................ 85
Figure 73: Network Policy Server Wizard 802.1X Completed ...................................................... 85
List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1: Cost Analysis</td>
<td></td>
<td>30</td>
</tr>
<tr>
<td>Table 2: List of Acronyms</td>
<td></td>
<td>52</td>
</tr>
<tr>
<td>Table 3: Technologies List</td>
<td></td>
<td>53</td>
</tr>
</tbody>
</table>
ABSTRACT

Until recently, FRCH Design Worldwide operated an aging and poorly protected wireless infrastructure. The award winning design and architecture firm decided that it was no longer tolerable for it and its demanding clientele to conduct business on an inconsistent and unsecured network. In the fall of 2012, it defined key deliverables, set a budget and initiated a project to replace the wireless infrastructure throughout its six-floor Cincinnati, OH headquarters. FRCH asked the project team of Andrew Burgess, Johnathan Riley and Jason Schuster to provision the critical project.

Using the criteria of cost features and ease of management, the team researched, recommended and installed an upgraded centrally managed wireless network at the downtown offices. The new wireless infrastructure, installed by the project team during the winter and early spring of 2013, not only provides uninterrupted service to users throughout the building but is also more secure by enforcing modern encryption protocols and integrating Active Directory authentication for internal authorized users. The addition of two wireless local area network controllers centralizes management of the wireless network, administration of policies and unifies the monitoring of network component health. The controllers also manage guest user authentication via simple interface that employs e-mail and text message to transmit provisional login credentials to access an internet-only connection through a captive portal. The upgraded switch gear improves network availability and also provides power to the dozen new access points. These upgraded access points provide nonstop high speed connections to dozens of simultaneous users at any point in the building. The newly implemented wireless upgrade now provides the secure and complete coverage that FRCH and its clients demand.
1. INTRODUCTION

The purpose of this report is to explain the steps taken to research and replace the wireless infrastructure and recommend network monitoring software to FRCH Design Worldwide (FRCH). This report will clarify that FRCH’s wireless infrastructure was unsound, unmonitored and could no longer be relied upon to transfer critical data for employees and clients; it needed to be replaced.

The team of Andrew Burgess, Johnathan Riley and Jason Schuster will describe the criteria that needed to be met in order to replace the old wireless network hardware and software components. The criteria included determining if the total cost of potential solutions fell within FRCH’s budget during the research phase, that the features of the solution met the requirements set forth by FRCH’s Senior Information Technology (IT) leadership and that the solution would be sufficiently easy to manage by its small IT staff.

1.1. Background

FRCH Design Worldwide is a design and architecture firm with headquarters at 311 Elm Street in downtown Cincinnati, OH. The award-winning firm has a global client list that includes major corporations like Fifth Third Bank, Tiffany & Company, Harley Davidson, Hyatt and Disney. FRCH was hit hard by the 2008 recession. The economic downturn caused its workforce to be cut from approximately 300 employees down to 150 in just over a year. Sales plummeted; companywide projects and hiring were indefinitely frozen. However, the company has begun to rebound. It has generated sales exceeding $15 million/year since 2010 and added more than thirty jobs in 2012 alone.
New hires were not the only progress frozen due to the recession; many of FRCH’s IT projects and key infrastructure upgrades were also put on hold over the last several years. One such project was the update of the headquarters’ wireless network (Figure 1).

Figure 1: Legacy FRCH Network Diagram

The wireless network infrastructure consisted of only six Foundry Ironpoint 250 wireless access points (APs) spread across five floors, two of which were located on the sixth floor in the conference rooms.
1.2. The Problem

Foundry Networks was acquired by Brocade in 2008. The network equipment installed at FRCH was no longer manufactured, making support non-existent and replacement hardware scarce. FRCH experienced this reality firsthand during the implementation phase of the wireless upgrade. One of the old Foundry FastIron Edge switches, indicated in the legacy network diagram, experienced a critical failure during the middle of a work day in February 2013. The failure dropped client network connections on one floor of the downtown offices. The IT staff scrambled to find a replacement switch and quickly opted for an HP switch. A direct replacement for the Foundry switch was initially hard to find and was later determined to be too costly, especially considering its age and outdated capabilities. The switch failure not only cost the company productivity and money, but was also a stark reminder of the critical need to replace the aging infrastructure. In point of fact, this one failure spawned a parallel project to replace all of the switch gear throughout the headquarters; a multi-phase project that will last through 2013.

In addition to the hardware being out-of-date and unstable, wireless network management at FRCH was a painstaking and unscientific exercise. One of the few indications that a wireless network issue existed was when users were dropped or unable to connect. When a problem was detected, the autonomous Foundry APs could only be managed through direct physical access via terminal cable. Johnathan Riley of the project team, a co-op at FRCH, has stood on ladders and tables to access the suspect APs in effort to troubleshoot issues. Their ranges were limited (Figure 2), dropping sessions or denying connection near the periphery of the building.
Figure 2: Legacy FRCH Heat Map, 3rd Floor

The yellow and orange zones designated by the heat map indicate that the bandwidth was agonizingly limited. The edges of the APs’ coverage were battlegrounds for connectivity. There was a constant tug-of-war between neighboring wireless signals and the neighbors regularly won, whitewashing FRCH’s signal. The “noise” in areas outside the green zone made the wireless a last resort in most instances where a wall port was available.

Finally, the old APs only supported one subnet, an internal facing subnet. Guests were given universal static credentials to access the wireless network. When they connected, guests were actually on the internal network (Figure 3). Guests could access any system that was not locked down. The project team was able to quickly and easily identify connected devices, map internet protocol (IP) addresses and access many system resources from printers to file servers to critical
infrastructure components. This type of unobstructed access to sensitive infrastructure resources and information was a clear compromise of network security best practices.

Figure 3: Pre-project Use Case Diagram

In addition to updating the legacy wireless, FRCH felt increasing pressure to monitor its network holistically. To date, it had not been able to monitor all aspects of its systems and was experiencing outages related to hardware failures. As with the APs, one of the common indicators of a problem was when a system or system component failed.

FRCH was prepared to implement some type of network monitor but considering the inflated costs of many of the commercial solutions, its focus was to find an open source network monitor solution. Its IT management had already begun the research process and whittled the list of open
source monitors down to Zenoss and Nagios. It commissioned the project team to research, test and recommend one of these two monitors.

To this end, the team was asked by senior IT leaders at FRCH to research, recommend and replace the existing wireless network infrastructure. Additionally, management requested the project team to research and recommend an open source network monitor solution. Its ultimate goal is to deploy a speedy, stable and secure wireless network befitting a company with millions in sales and a demanding high-profile client base.

### 1.3. The Solution

On the evening of December 20, 2012, after long hours of research and testing, the project team presented their findings to stakeholders at FRCH. The team presented details about wireless network solutions from Juniper, Cisco, Aruba and Fortinet. The team recommended the solution from Fortinet (Figures 4 and 5).
The Fortinet solution, as with the others, met all of the deliverables laid out by FRCH. It fell within the budget, was centrally managed, easy to use and had the capacity to entirely cover each
floor of the building while handling an impressive number of end users and their devices.

However, there was one clear reason that made the Fortinet solution stand out: FRCH already owned the Fortinet wireless LAN controller (WLC), the FortiGate 200B, in fact, it owned two of them. The FortiGate was being used as a firewall at the periphery of its network. Unknown to the IT decision makers at the time, in addition to firewall capabilities, the FortiGate 200B can also be configured as a WLC. This one factor alone cut thousands of dollars from the overall wireless upgrade project budget. Actually, FortiGate retail pricing varies but many online retailers listed it for well over $3,000, including Newegg.com, who represented the median with a price of $3,306.99 (Newegg).

When you factor in redundant devices, the team’s recommendation saved FRCH a retail average of more than $6,500. Of course, FRCH has many vendor relationships that allow it to leverage better than retail pricing. The project team is not at liberty to disclose the pricing of the FortiGate hardware due to non-disclosure clauses with FRCH’s vendors. However, the team can confirm that its decision saved FRCH thousands of dollars.

The savings allowed FRCH and the project team to do a couple of things. One, the project team was able to recommend upgraded APs and purchase more of them. The team recommended Fortinet FortiAP FAP-320b APs, a 3x3 Multi-In Multi-Out (MIMO) radio over Fortinet’s 2x2 MIMO offering. The 3x3 design has more transmit and receive antennas that increase spatial transmission and decrease packet loss over the wireless signal (Wexler).

In addition to upgraded APs, the savings allowed FRCH to purchase more APs, giving them greater coverage on each floor and the ability to accept more simultaneous client connections. The figures below indicate AP placement recommendations before and after the realization of
the cost savings afforded by the Fortinet solution (Figures 6 and 7).

The two-per-floor AP placement (Figure 7) improved coverage throughout the building. Coverage of each floor was now edge-to-edge. The heat map image of the third floor (Figure 8) was indicative of all levels at the 3rd Street and Elm headquarters:
The cost savings also freed FRCH from the constraints of the open source network monitoring solution. Its budget was opened allowing the IT leaders to negotiate with budget makers and executives for a budget increase that allowed it to consider commercial network monitoring solutions. It was in February of 2013 that FRCH decided to purchase and implement Microsoft’s System Center Operations Manager (SCOM). As a result, the project team abandoned its research of the two open source solutions, Zenoss and Nagios. Instead of giving up on the network monitor aspect of the project, the team decided to maintain the original project scope and explore SCOM’s capabilities in the team test environment.

1.4. Credibility

The team is qualified to generate the report because it is comprised of three IT professionals, each presently employed in various positions within the field. The project team includes a CCNA and an employee of FRCH. The team has surveyed, used and supported FRCH’s wireless network over the last several months. Each member has observed, first hand, the slow speeds, dropped connections, difficulty in administration and holes in the network’s security. The team understood the old system’s waning dependability and performance better than anyone else, except perhaps the senior IT management at FRCH.

1.5. Project Goal

The goal of the project, ultimately, was to upgrade FRCH’s wireless network and to recommend a network monitoring solution. After months of research, the team recommended a wireless network solution. FRCH agreed with the team’s recommendation and implemented the
solution. APs were purchased and placed. The WLC’s were configured. The wireless network was improved (Figure 9).

![Current FRCH Network Diagram](image-url)

**Figure 9: Current FRCH Network Diagram**

The cost savings achieved by the Fortinet decision freed FRCH IT to purchase more access points and to internally negotiate a budget for a commercial network monitor, leaving the concept of a difficult to implement open source solution behind. Though the scope change was unfortunate in terms of deliverables to FRCH, the project team was still able to test the commercial solution SCOM and gain priceless experience administering a common Enterprise-level network monitor.
1.6. Overview

The next sections of this report explain in greater detail exactly how the project team of Andrew Burgess, Johnathan Riley and Jason Schuster approached and completed the project. The report includes the following sections: A discussion component with sections regarding project concept, definition, deliverables, budget, research, recommendation, implementation, technical elements, methodology, user profiles, timeline, problems encountered, and conclusion. There is an additional appendices component with a list of acronyms, an equipment list with specifications and finally, several step-by-step how-to documents provided to FRCH that allow it to redeploy any of the systems that were configured by the project team.
2. DISCUSSION

2.1. Project Concept

2.1.1. Big Picture

The goal of the project was to upgrade FRCH’s wireless network and to recommend a network monitoring solution. On a broader scale, the project team was focused on completing a real-world IT network project, that is to say, to get a glimpse of similar projects that the individual team members might encounter, on some scale great or small, throughout their careers in IT.

In retrospect, the project appears to have met those real-world expectations. The project team worked with leadership at FRCH to define the scope of the project. FRCH leadership set forth clearly defined deliverables, set a timeline and laid out a concrete budget for the project team to work within. Over the months of research and implementation the project was dynamic. The deliverables changed when FRCH decided to implement SCOM; the project team no longer had the task of researching and recommending the open source network monitors Zenoss and Nagios. The scope changed when the decision was made to purchase and install a dozen APs. However, these types of changes are consistent with everyday projects and the project team’s experiences over the course of the project will be invaluable as each member goes through his career.

Regardless of changes to the scope and deliverables the project was considered a success. The wireless network was made fast and stable and FRCH had made a decision on a network
monitor. The following sections describe, in great detail, the project team’s actions and experiences during the implementation of the FRCH’s wireless network upgrade.

2.1.2. Project Defined

On the evening of September 6, 2012, Johnathan Riley introduced the rest of the project team to his manager, FRCH’s Director of Technology, Matt Davidson. He sat the project team down in a small conference room on the third floor of the 311 Elm Street headquarters and began the meeting by giving a little backstory about himself, FRCH as a company and his experiences with them over the last several years. He proceeded to discuss the recession in 2008 and the subsequent layoffs in 2009 and 2010 that decimated the staff at FRCH by half, down to approximately 150 employees. He continued by enthusiastically explaining the company’s recent resurgence, the related hiring frenzy and the renewed ability for the company to once again take on projects large and small.

One of the more important IT projects, Matt Davidson explained, was the repair or replacement of the wireless infrastructure. The recent ballooning staff and the proliferation of smart phones, tablets and the migration from workstations to laptops had put in clear relief that the wireless network, as it stood, was not up to the task of supporting so many users and devices. He invited the project team to log into the wireless network to experience, firsthand, what he was talking about. He gave Andrew Burgess and Jason Schuster the static key to the network. This was the same key given to everyone from C-level executives, to regular employees and even to contractors in order to access the network. Once connected to the wireless, he quickly pointed out that each of us was now connected to the internal network. Carefully controlled permissions were the only barriers that prevented unmitigated access to all of FRCH’s networked systems.
and resources. He was clearly upset by this and was anxious to implement a wireless network solution that not only supported the growing number of users and devices but to segregate and secure outside users from the internal employee network resources.

Matt Davidson segued from his discussion about the old wireless network to a second lurking issue. He explained that FRCH did not have a network monitor in place. The implementation of a network monitor was one of the critical IT projects that were pushed aside as the company positioned itself to survive the economic depression. Since it had seemingly rebounded and looked to expand to its former size and larger, he explained that he was once again given clearance to look into network monitoring solutions. The only caveat was that there was little to no budget to purchase commercially packaged solutions; he needed to find a free open source solution.

Matt Davidson did some independent research and spoke to his peers within the local IT community to see who was using open source, if anyone, and what they were using. His investigations kept returning the same two product names: Zenoss and Nagios. These solutions were the most widely supported and used within the open source community. He explained that, should the project team be the right fit for the wireless upgrade project, he would also like the team to configure and test Zenoss and Nagios in a virtual environment and make a clear recommendation as to which was the standout based on a few criteria.

When the problem was clear and the project team had indicated a desire to help find a solution, he quizzed Andrew Burgess and Jason Schuster about their interest in IT and qualifications to assist on the project. Andrew explained that he held a current Cisco Certified Network Associate (CCNA) certification and was a working network administrator contracted to
support Procter and Gamble’s corporate headquarters. Jason explained that he had been employed for the last three years as a Windows systems administrator with Duke Energy at its downtown Cincinnati headquarters. Of course, as an employee of FRCH, Johnathan Riley was already positioned as a key implementer of the wireless upgrade and network monitor solutions as these would be the systems he would support while employed with the company. When Matt Davidson was satisfied that the project team was able to assist him in completing the wireless project (Figure 10) he scheduled a follow-up meeting with his direct report, a key stakeholder in the project.

Figure 10: Team Member Responsibilities
2.1.3. Deliverables

On the following Wednesday, September 12, the team met with Matt Davidson and the Vice President of Technology, Michael Rinken. There, Matt Davidson and Mike Rinken provided the team with a complete description of the project including a concise list of deliverables and expectations. The deliverables laid out were:

- A wireless assessment - research how to mitigate dropped sessions
  - Are more APs needed?
  - Do the replacement APs need to be 3 MIMO or is 2 MIMO enough?
  - What are the best locations for the APs on each floor?
- Public and private wireless local area networks (WLANs)
  - Two service set identifications (SSIDs) and virtual local area networks (VLANs).
    - Internal VLAN
      - Will authenticate to Active Directory (AD).
      - Will use existing access control lists (ACLs) and other services to filter and block content to employee users.
    - Guest VLAN
      - Easy password management.
        - Password must change frequently.
        - Password must be easy to remember/type.
        - How to deliver passwords to guests?
        - Can the password be unique for each guest?
        - Can the password lease be time limited?
• WLAN must be centrally managed.
  o Wireless LAN controller
  o Cloud WLAN management service

• Research, test and recommend an open source network monitor.
  o Limit research to Zenoss and Nagios.
    ▪ Which is simplest to configure and implement?
    ▪ All required software systems must also be open source.
    ▪ Must be hosted in a virtual environment (not require standalone servers).
    ▪ Are there any hidden costs outside of host VM license?
    ▪ Which is simplest to use yet has robust feature set?

• Research and the best wireless solution.
  o What products and why?
    ▪ Cisco must be included in the research (FRCH already a quote for a Cisco solution).
    ▪ Research other products and present a total of four, including Cisco.
    ▪ What product provides the most functionality for the money?
    ▪ Provide a cost analysis.

• Present team findings to stakeholders at FRCH by the end of December 2012.
  o The presentation must be short, address each of the deliverables and clearly indicate one wireless network solution that outshone the others.

• Budget constraints must be met.
  o The team was given a maximum budget of $15,000.
2.1.4. Project Budget

FRCH Design Worldwide did not have a large IT budget. It agreed on a maximum of $15,000 to purchase and install a new wireless infrastructure. The network monitoring solution was not included in the budget, consequently the team was asked to look into wholly open source solutions. In December of 2012 the money was approved and added to FRCH’s final 2013 corporate budget.

Stakeholders demanded that the budget needed to cover all costs related to the wireless upgrade. That included the cost of the hardware, any necessary mounting equipment, product support for a minimum of 3 years (in terms of a warranty or care-pack), any contractor and material costs related to wiring configuration changes and software licenses.

Initial speculative hardware costs that the project team had to consider when comparing and endorsing available solutions included but were not limited to: WLC(s), APs and power over Ethernet (PoE) power injectors due to the older switch infrastructure throughout the building. Wiring costs included but were not limited to: cable type needed (category 5e or category 6, plenum rated), hardware to terminate the cabling, and the contractor labor to pull, run and terminate the cabling. Additionally, software license and support costs may be recurring. Any such recurrence beyond a three year limit will be out of scope for this project’s budget.

As above-mentioned, the original project budget did not include the costs associated with a commercial network monitoring solution. FRCH was eager to retain any cost savings if the wireless upgrade project came in under budget. As a result, the team was initially asked to limit its product research to open source network monitor solutions only.
Additionally, all prices/costs mentioned are retail costs available to all consumers via Internet retailers. The pricing available to FRCH and the final cost of the implemented solution are explicitly not available for disclosure. FRCH has a non-disclosure agreement with its vendor, the violation of which would have legal implications.

2.2. Research

During the second meeting the project and deliverables were reaffirmed, principal deadlines were set, the initial budget was laid out and the project was formally kicked-off. The team immediately began to research wireless network solutions. The team also began research on the two open source network monitoring solutions, Zenoss and Nagios, at this time. Details about the test environment in which the network monitors were configured are detailed in later sections. The following paragraphs are dedicated to detailing the team’s research into the wireless network solutions.

Using the budget and criteria outlined by FRCH, each member researched several centrally managed wireless network solutions. The team eventually whittled the list down to four solutions for final recommendation, per FRCH directions. The forerunners were combined hardware and software solutions by Cisco, Juniper, Aruba and Fortinet.

The Cisco solution was already on FRCH’s radar. Prior to the project team’s first meeting with FRCH, the IT management team already received a quote for a solution based on the Cisco 1041 access points and the WLC 2504 for centralized management. The AP’s had a retail cost of $300 each (Figure 11) (CDW) and the WLC with an as-configured retail price of $2,585.65 (Figure 12) (CDW).
The Cisco devices looked good on paper. The APs were very competitively priced and appeared to be up to the job, though they lacked some multi-band and redundancy features of the
other solutions. Moreover, at that price FRCH could afford to install two APs per floor and achieve excellent coverage. The team’s research also indicated that the WLC software would meet FRCH’s ease of use expectations. That was quite the revelation as Cisco is not known for its graphical user interfaces (GUI). The documentation that the team found indicated that the WLC’s GUI was easy to navigate and understand. This revelation was a distinct advantage in favor of the Cisco solution.

However, paper documentation is as far as the project team got. The team was unable to secure equipment for testing and had difficulty finding non-sales Cisco representatives to talk about the solution. The team attempted to speak to the vendor who put together the initial quote. The impetus was to determine many things including if Cisco did a site survey of FRCH and why that particular level of equipment was chosen. The team wanted hard facts on why Cisco engineers thought the recommended APs and WLC would meet FRCH’s deliverables. Also, the team wanted to find out why the Cisco quote included approximately $5,000 worth of support costs, something not found from any of the other manufacturers. No one would answer the team calls.

The next wireless solution that the team investigated was from Juniper. The Juniper WLA522 AP and WLC made it to the final research phase due to a competitive feature set and some outstanding technical consultation and support from Juniper experts. The Juniper APs had a retail price of $543.75 (CDW), almost twice the Cisco AP price (Figure 13), however, the WLC was consistently priced at $2,508.75 (CDW) (Figure 14).
As with the other finalist solutions, the Juniper hardware and software hit all of the key points that FRCH dictated. Even though the project team was unable to acquire hardware for
testing, Jon Roberto, Director of Sales - SMB at Cadre Computer Resources, was able to provide a live demonstration of the Juniper products. The team met with him at his offices where the WLA522 and WLC8 were put through their paces. The team was put in the driver’s seat of the WLC’s user interface, recently acquired by Trapeze, as Jon Roberto explained in great detail the full feature set of the Juniper solution.

The project team was impressed by the Juniper products, to say the least. The demoed solution had features to meet FRCH’s deliverables and more. One of the only detractors was the AP price-point. The AP was priced almost twice that of the Cisco AP, yet had almost identical specifications. Nevertheless, Juniper made the team’s final list of potential wireless network upgrade solutions.

Next, the team looked at solutions by Aruba. The team was initially interested in the Aruba solution because that’s what was currently being used at the University of Cincinnati (UC). UC implemented Aruba wireless because of a former Senior Design project team headed by Jason Maloney. The project team contacted Jason Maloney, now an adjunct professor in the Information Technology IT program, for his Aruba contact. The team was put into contact with Tim Cornett, Territory Manager of Aruba Networks.

Tim Cornett was very knowledgeable and accommodating. He readily offered an Aruba IAP 105 AP for testing (Figure 15). The Aruba solution uniquely stood out from the others as the only solution that did not require a WLC. The IAP 105 was the WLC. Any IAP 105 could be configured as the WLC and in so doing, be the single centralized point of configuration and management for other IAPs in the FRCH headquarters (Figure 16).
**Research**

**Aruba IAP 105**

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Aruba</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>IAP</td>
</tr>
<tr>
<td>Model Number</td>
<td>105 or 104</td>
</tr>
<tr>
<td>Cost</td>
<td>$583.80</td>
</tr>
<tr>
<td>RF power output</td>
<td>23 dBm (both bands limited by Govt reg)</td>
</tr>
<tr>
<td># of redundant ports</td>
<td>0</td>
</tr>
<tr>
<td>Antennas</td>
<td>2X2 MIMO Internal</td>
</tr>
<tr>
<td>Radio</td>
<td>Dual</td>
</tr>
<tr>
<td>Speed</td>
<td>300Mb/s</td>
</tr>
<tr>
<td>Power</td>
<td>PoE (802.11at)</td>
</tr>
<tr>
<td>Port speed</td>
<td>1X1Gb/s</td>
</tr>
<tr>
<td></td>
<td>High-Density (~25 users)</td>
</tr>
</tbody>
</table>

Figure 15: Aruba IAP-105 AP

**Research**

**Aruba IAP 105 (WLC Functionality)**

Figure 16: Aruba IAP-105 Web Interface
The built-in WLC capability instantly made the Aruba solution the forerunner in the team’s research, due in great part to the implied cost savings. At an average estimated savings of $2,500, the Aruba solution freed up funds to increase the total number of APs if needed. The extra funds could even have been rolled back into FRCH’s 2013 budget for use in another project.

Additionally, the team’s ability to physically test the product in FRCH’s headquarters was extremely beneficial and very telling. Testing showed that the IAP-105 could easily provide the complete edge-to-edge coverage required by stakeholders. The heat map (Figure 17) shows just how impressive the coverage of only one Aruba AP was.

Figure 17: Aruba Heap Map, FRCH 3rd Floor
Aruba had what appeared to be a complete and cost effective solution. However, further research exposed what turned out to be a single flaw in the product. FRCH had a key deliverable requirement that the end solution have a guest password management system to control guest access to the public wireless network. As configured, the IAP-105s had an overly simplified system for guest user management. The simple interface did not allow for Short Message Service (SMS) or e-mail communication of passwords to guest users nor provide for lifecycle limitations. In order to obtain the full feature set, FRCH would need to pay an additional $5,500 for Aruba’s Enterprise Starter Bundle which included the Clear Path guest management software license. That cost did not reflect an additional cost of $9,000 for one year of support and quickly pushed Aruba over budget and off the team’s radar for acceptable solutions.

**2.3. Recommendation**

The team’s research eventually led to one clear standout solution that met all of the needs and expectations of FRCH. The team met again with Mike Rinken and Matt Davidson on the evening of December 20 to present its findings. The team presented, in detail, all of the research that it conducted over the previous 12 weeks and then iterated through each of the aforementioned potential solutions’ positive features and their shortcomings. Finally, the team presented its recommendation, Fortinet.

The Fortinet solution consisted of the FortiAP FAP-320b (Figure 18) access points and the FortiGate 200B WLC (Figure 19). These two products combined to meet all of the deliverables originally laid out by Mike Rinken and Matt Davidson. The solution was centrally managed, easy to manage, able to provide complete coverage throughout the building, able to support dozens of simultaneous load-balanced connections and provided a full-featured guest password
management solution that was easy enough for the receptionists to use. The team worked closely with Fortinet Channel Account Manager Dolph Smith to verify that the Fortinet solution was indeed capable of delivering on its promises.

![Recommendation: Fortinet FortiAP FAP-320b](image1)

**Figure 18: Fortinet FAP-320B**

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Fortinet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>FortiAP</td>
</tr>
<tr>
<td>Model Number</td>
<td>FAP-320b</td>
</tr>
<tr>
<td>Cost</td>
<td>$729.65</td>
</tr>
<tr>
<td>RF power output</td>
<td>23 dBm (both bands limited by Gov't reg)</td>
</tr>
<tr>
<td># of redundant ports</td>
<td>2</td>
</tr>
<tr>
<td>Antennas</td>
<td>3x3 MIMO Internal</td>
</tr>
<tr>
<td>Radio</td>
<td>Dual</td>
</tr>
<tr>
<td>Speed</td>
<td>450Mb/s</td>
</tr>
<tr>
<td>Power</td>
<td>PoE(802.11at)</td>
</tr>
<tr>
<td>Port speed</td>
<td>2x 10/100/1000</td>
</tr>
<tr>
<td></td>
<td>Fast roaming for uninterrupted Wi-Fi</td>
</tr>
</tbody>
</table>

![Recommendation: Fortinet FortiGate 200B](image2)

**Figure 19: FortiGate 200B Web Interface**

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Fortinet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>FortiGate</td>
</tr>
<tr>
<td>Model Number</td>
<td>200B</td>
</tr>
<tr>
<td>Cost</td>
<td>None - already installed (have redundant devices)</td>
</tr>
<tr>
<td># of APs</td>
<td>32 (would also depend on the firewall)</td>
</tr>
<tr>
<td># of connections</td>
<td>4(10/100/1000)</td>
</tr>
<tr>
<td>Configure interface</td>
<td>web interface</td>
</tr>
<tr>
<td>Authentication</td>
<td>AD through Radius</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>yes</td>
</tr>
<tr>
<td>Guest access</td>
<td>yes</td>
</tr>
<tr>
<td>VLAN Support (802.11q)</td>
<td>yes</td>
</tr>
</tbody>
</table>
These two products combined to meet all of the deliverables originally laid out by Mike Rinken and Matt Davidson. The solution was centrally managed, easy to manage, able to provide complete coverage throughout the building, able to support dozens of simultaneous load-balanced connections and provided a full-featured guest password management solution that was easy enough for the receptionists to use. The team worked closely with Fortinet Channel Account Manager Dolph Smith to verify that the Fortinet solution was indeed capable of delivering on its promises.

So why did the team recommend Fortinet? In retrospect, all of the finalist solutions were able to meet the same demands, in one configuration or another, that Fortinet was able to meet. The fundamental point that set the Fortinet solution apart from the others was that FRCH already owned the FortiGate 200B. FRCH was currently using the FortiGate as the primary firewall. It owned a second as a passive failover 200B should there be an outage with the primary FortiGate firewall. Through its research, the team discovered that the FortiGate was designed with many functions that only needed to be enabled to implement. One of those functions was that of a WLC.

By simply leveraging existing hardware, the project team saved FRCH approximately $6,500 (retail cost) in redundant WLC costs. The team used these paper savings, and Dolph Smith’s recommendation, to endorse the upgraded FAP-320b APs, a 3x3 MIMO design that decreased packet loss and increased reliability of the wireless network for a small per-AP price premium over the Fortinet 220b’s 2x2 MIMO design. The final cost comparison shows that Fortinet was one of the most cost effective solutions (Table 1), even with the inclusion of 12 of the upgraded APs, a total of 5 APs more than were originally budgeted and planned for.
Table 1: Cost Analysis

The project team found a solution that saved FRCH thousands of dollars. For that reason, Mike Rinken and Matt Davidson elected to move away from the open source network monitors and to open their search to include commercial network monitoring software. They quickly decided on Microsoft’s SCOM. FRCH, already a heavy Microsoft user, selected SCOM because most of the required component software, like SQL, was already in production in its environment.

2.4. Implementation

FRCH was impressed with the project team’s presentation and final recommendation. However, Mike Rinken and Matt Davidson were ultimately unwilling to proceed with the Fortinet solution until it was fully tested. They reached out to their Fortinet vendor and requested two FortiAP 320B access points to test and verify the team’s recommendation. It also provided
the team with a FortiGate 300B, similar to the FortiGate 200B, for the team to use in its test environment.

The team immediately set up the FortiGate and FortiAP in its test environment to begin validating the steps for implementation in FRCH’s production environment. The team’s Microsoft environment closely mimicked that of FRCH, allowing the team to configure critical components like Remote Authentication Dial In User Service (RADIUS) and test key deliverable functionality like Active Directory integration. The team used the FortiGate and APs to investigate implementation both in their team test environment and on FRCH campuses. The sections within Appendix C are the result of the team’s configuration efforts within the test environment. The team was able to create detailed deployment guides, in a step-by-step format demanded by Matt Davidson. Though the team configured the FRCH network during physical deployment, these guides will serve FRCH as disaster recovery documentation, in case it needs to reconfigure and re-implement the wireless network at any phase, on any configured element.

In parallel with the work in the test environment, Matt Davidson gave the team access to the FRCH headquarters to begin testing AP placement in the end physical environment. The team consulted with Dolph Smith regarding best practices for AP placement. The Fortinet engineer pointed the team to FortiPlanner, a Fortinet software specifically designed to help determine AP placement in a variety of environments. FortiPlanner allowed the team to upload individual floor plans of FRCH’s Elm Street headquarters. The software then allowed the team to manipulate dozens of environmental variables including construction materials for individual walls, elevator shaft location and more. All of the input variables helped the software to guide the project team to the best AP locations throughout the building (Figure 20).
The figure above, however, does not fully explain the final placement of the access points. When viewed from above, the access points were placed on opposite alternating corners of each floor. Dolph Smith explained that each AP’s signal would radiate through the ceiling above its location and provide coverage to that quadrant of the floor above. In this way, the team recommended to FRCH a placement that would optimize the signal coverage on each floor (Figure 21).

Figure 20: AP Placement
Figure 21: Installed Fortinet AP

The composite heat map (Figure 22) indicates the final placement of the access points on the 3rd floor at FRCH headquarters. This illustrates the caddy-corner placement of the APs recommended for every other floor. The green color indicates excellent coverage and the speeds seen at the lower left clearly met the expectations Mike Rinken and Matt Davidson laid out in the project beginning.
From the start of the project, the team saw a need to set up a robust testing environment to assess and validate various deliverables set in the initial meetings with FRCH. Specifically, the team saw an immediate need to test and verify functionality of the open source network monitoring solutions Zenoss and Nagios. The team saw a future need, after the completion of the wireless network solution research, to use the test environment to configure and implement the wireless solution before rolling it out on FRCH’s production network. For these reasons the team
deployed a test environment consisting of a variety of hardware, virtual hardware and software (Figure 23).

Figure 23: Team Test Environment

The environment sits on Andrew Burgess’ high speed home network. The team uses WebSSL (for Secure Socket Layer) virtual private network (VPN) on a FortiGate 300B, courtesy of FRCH, for remote access to the test environment both for network management and project-related demonstration purposes. The VPN is managed via the FortiSSL VPN Client interface and is configured with administrative roles for each of the project team members.

The physical test environment consists of the aforementioned FortiGate 300B which acts as not only the VPN server, but the network firewall and the WLC. It is no coincidence that the
team ended up with the FortiGate appliance. FRCH provided them with a spare device to aid in development of protocols for implementation in the FRCH production environment.

Moving further into the network, the team has two HP ProLiant DL380 G6 servers. The first physical server is a standalone server running Windows Server 2008 SE R2 with Active Directory services. In addition to AD, RADIUS is also configured on the network. Again, this specific implementation of the operating system (OS) and services was selected to mimic FRCH’s production configuration.

The second physical server hosts the virtual environment and is configured with VMware ESXi 5.0. The virtual leg of the environment was originally used to test open source network monitors. It was configured with VMware ESXi 5.0 and is hosting two CentOS VMs, one loaded with Zenoss, the other with Nagios.

Because of FRCH’s decision to move forward with a commercial network monitoring solution, the team was no longer required to continue testing Zenoss and Nagios. The change in project scope at the midway point was unexpected and the team felt simultaneously excited for testing the Fortinet solution but deflated at the prospect of losing a key element of the project. Instead of abandoning the network monitor research altogether, the team decided to stand up and test SCOM.

The team configured the core of SCOM in the virtual portion of its test environment. One VM is running Windows Server 2008 and is configured with SCOM. A second VM is configured with Microsoft SQL Server 2008 R2 database, per SCOM deployment guidelines. By the end of the project SCOM was configured to detect simple network management protocol (SNMP)
traffic, the internet protocol standard by which managed network-attached devices communicate system health statuses to the network management system.

The figure below (Figure 24) visually encapsulates the majority of the technical elements that the project team worked with over the course of the project. Appendix B gives a full rundown of the technical specifications of each of the hardware and software technical elements that the team interfaced with from the project's beginning.

Figure 24: Key Technical Elements
2.4.2. Methodology

The project team used an exhaustive methodology to conceptualize, plan and test its code and configurations before any modifications were made. After all, FRCH does not have a test environment; all of the changes were to be made on a production infrastructure and mistakes could have been costly. To minimize network disruptions and downtime, almost all of the changes were made after business hours. System configurations were saved only after connectivity and functionality were verified. Additionally, the team created the following documentation to test and verify configuration changes on paper before implementation began:

1. The FortiGate (firewall) will be upgraded to 5.0 OS - Screenshot. Can FRCH still connect to outside world?
   a. Ping Google.com or other external websites. (Screen Shot)

2. The FortiGate will have WLC functionality enabled (Firewall + WLC) - Can you access WLC interface?
   a. Screen shot of the interface

3. Add 3 new virtual local area networks (VLANs) to the network Internal, Management and Guest VLANs to switches throughout the building.
   a. Screen shot of a show run on switches

4. Each VLAN will have a limited number of available IPs. Configured in Dynamic Host Configuration Protocol (DHCP).
   a. Screen shot of DHCP scopes

5. The wireless system will connect to the Internet.
   a. Connectivity:
i. Internal Wireless
   1. Correct IP
   2. Screen shot of ipconfig

b. Internal connectivity
   i. Screen shot of ping to internal server

c. External connectivity
   i. Screen shot of ping to Google

6. Verify Enterprise authentication works.
   a. Screen shot of authenticated user
      i. Guest
         1. Correct IP
         2. Screen shot of ipconfig
      ii. Internet access only
          1. Screen shot of ping to internal server
          2. Screen shot to external site

7. The wireless system should cover the whole of each floor - Heat map.
   a. Screen shot of heat map

8. The wireless system should allow access to authorized employee users - AD authentication.
   a. Screen shot of:
      i. Non-authorized = Failed access
      ii. Authorized = Successful access

9. The WLC should allow access to authorized wireless network management users - Password controlled.
a. Verify that only Network admins can get to the WLC section of the FortiGate 200b.

10. The wireless system should allow access to authorized guest users only – WPAx (802.1X).
   a. Screen shot of guest users authenticating with provided credentials
   b. Screen shot of guest failing to authenticate due to the lack of credentials

11. The WLC should manage access for authorized guest users - Guest pass management system/software.
   a. Screen shot of receptionist access to local user group for Guest management

**2.4.3. User Profiles**

The main users of the wireless network fall into two general categories: FRCH employees and guests (Figure 25). All employees and guests must have proper credentials to access the network. FRCH employees will authenticate to the private internal network via Active Directory. Upon authentication, employees will be able to use the system at any time. Guests will request a key to the public wireless network from the receptionist or a network administrator. Guest keys will be valid only for a limited time (This policy will be determined by FRCH IT leaders at a later date). Upon authentication, all users will be allowed to connect to the wireless network with any 802.11 n/g/b capable device. There will be no restrictions on device types.
The main users of the wireless network fall into two general categories: FRCH employees and guests. All employees and guests must have proper credentials to access the network. FRCH employees will authenticate to the private internal network via Active Directory. Upon authentication, employees will be able to use the system at any time. Guests will request a key to the public wireless network from the receptionist or a network administrator. Guest keys will be valid only for a limited time (details of this policy will be defined by FRCH IT leaders at a later date).

Figure 25: Post Project Use Case Diagram
date). Upon authentication, all users will be allowed to connect to the wireless network with any 802.11 n/g/b capable device. There will be no restrictions on device types.

The primary users of the centralized wireless network management system are limited to network administrators. Network administrators will authenticate via Active Directory to access the centralized wireless network management system. From there the administrator will access the wireless network management console. Administrators will use this system to change configurations and monitor all APs.

The central users of the network monitor are limited to network administrators. Network administrators will authenticate via Active Directory to access the network monitor. Upon authentication, the administrator will access the network monitor console. Administrators will use this system to troubleshoot the network. The system will be configured to send alerts (alert-level policies will be defined by FRCH IT leaders at a later date) to administrators via SMS and e-mail.

### 2.5. Project Timeline

![Figure 26: Research Phase Timeline](image-url)

<table>
<thead>
<tr>
<th>Task #</th>
<th>Task Name</th>
<th>Duration</th>
<th>Start</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 Research</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1.1 Wireless Audit</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1.2 Network Audit</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1.3 Test Environment</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1.4 Testing with FRCH</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1.5 Testing with FRCH</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1.6 Elevator Speech</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8 Problem Area 1</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>8 Problem Area 2</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>8 Problem Area 3</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>8 Problem Area 4</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>10 Prepare for FRCH</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>11 FRCH Presentation</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>12 FRCH Furniture</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>12 FRCH Furniture</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>16 Presentation to SO Class</td>
<td>16 days</td>
<td>Mon 11/26/12 to Wed 11/28/12</td>
<td></td>
</tr>
</tbody>
</table>

Figure 26: Research Phase Timeline
2.6. Problems Encountered

There were many problems encountered over the course of the project. This was a multifaceted IT infrastructure undertaking and the project team had no notions of the job concluding without some form of change. The team handled the adversity well, and with the assistance of both leadership at FRCH and guidance by the team’s project advisor Russ McMahon, were able to overcome many of the difficulties over the 8 months of project work.

The changes that caused the biggest impact were the changes in scope, and of those the greatest was FRCH’s move away from the open source network monitor. To the team, the network monitor represented a robust feature that justified the need for three people to complete all of the required tasks, at least from the perspective of the capstone requirements. When the open source network monitor deliverable was removed in favor of SCOM, in great part due to the cost savings that the team’s wireless network solution provided, the team worried if it had
enough collective responsibility remaining to stay in good standings with the IT capstone requirements.

Rather than just passively wait for judgment from the IT faculty, the team decided to make the most of the adversity and stand up SCOM on its test environment. With the Microsoft Software Development Network (MSDN) academic license, the team was able to secure all the necessary software components to implement a full functioning, albeit small-scale, implementation of SCOM. This effort ultimately displayed the team’s mobility in the face of diversity and its commitment to meeting any and all University based requirements.

There were many other problems encountered over the course of the project, though in comparison, none of them were of the same scale as the network monitor deliverable change. Among the other difficulties was the general complication of having two sets of deliverables; those for UC and those for FRCH. Many times, the two sets of deliverables and their accompanying schedules overlapped each other, much to the dismay of the project team. Another stress was FRCH’s decision to purchase the Fortinet APs in piecemeal fashion. It decided to purchase two access points per month to “mask” the purchase costs from the executive staff. Rather than having one big rollout, the project team was left with a rationed arrival of hardware that staggered out deployment over months (Figure 28).
The deployment was further delayed when FRCH decided to upgrade the switches throughout every floor of the downtown headquarters (Figure 29). The new switches will have PoE, saving the company hundreds of dollars in power injector costs for the dozen APs, but the switch upgrade will be done in phases over the entirety of 2013.
Lastly, Fortinet is in the process of developing an operating system version upgrade for the FortiGate. The newest software version will have upgraded functionality and patch some security gaps of the previous version. Because of this, FRCH has decided to keep a deprecated OS running on the FortiGates. The old software is not able to natively support VLANs and does not have many of the guest password management features originally demanded by FRCH and promised by the project team (Fortinet). In fact, as of this writing, the wireless deployment is only complete on one floor of the building.
3. CONCLUSION

In conclusion, this project has been an amazing learning experience. The team owes great thanks to not only FRCH’s VP of Technology, Mike Rinken and Director of IT, Matt Davidson, but also technical advisor, Russell McMahon, and project management advisor Dr. Patrick Kumpf and many, many more.

Over the last 8 months the project team had successes and also had setbacks. There were major changes to project deliverables, like FRCH’s move away from the open source network monitor detailed above. There was scope creep, like FRCH’s decision to upgrade all the switchgear throughout their headquarters, which the team was involved in. But the team is sure that all of the change and adversity is analogous of IT projects it will face as each member goes through his career.

Through all of this, the big takeawaay is that the team was able to complete a real-world IT network infrastructure project for a local multi-million dollar business. The project has had an immediate impact on FRCH’s ability to conduct business. The wireless upgrade has allowed it to begin to improve client experience and enhance its ability to provide excellent client services while on the FRCH campus. The success of the project has also enabled the quickly growing company to accommodate the explosion of wireless devices like iPads and iPhones that are universal among the design crowd.

On top of all that, the team had an amazing experience sharing its project and results by presenting at Tech Expo. The team had live demonstrations of the wireless test network and the SCOM environment for attendees to observe and even test drive. FRCH provided some of its old and new AP hardware for an impactful visual and physical comparison of the disparate
technologies. Most importantly, the team had dozens of opportunities to share its story with a variety of attendees from high school students to peers, family, friends and local IT leaders and professionals. It was a proud and exciting moment that allowed the team to represent its college and program. Again, final heartfelt thanks go out to everyone who has supported the team during the course of the project. Thank you.
4. REFERENCES


<http://www.arubanetworks.com/products/instant-access-points/>


   <http://www.fortinet.com/solutions/wireless.html>


   20 October 2012.
   <http://www.networkworld.com/newsletters/2008/042808wireless2.html>
### 5.1. Appendix A: List of Acronyms

<table>
<thead>
<tr>
<th>Acronyms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLs</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>APs</td>
<td>Access Points</td>
</tr>
<tr>
<td>Cat</td>
<td>Category</td>
</tr>
<tr>
<td>CCNA</td>
<td>Cisco Certified Network Associate</td>
</tr>
<tr>
<td>C-level</td>
<td>Chief Executives</td>
</tr>
<tr>
<td>Config</td>
<td>Configuration</td>
</tr>
<tr>
<td>Co-op</td>
<td>Cooperative</td>
</tr>
<tr>
<td>dBm</td>
<td>Decibel per milliwatt</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DL</td>
<td>Direct Link</td>
</tr>
<tr>
<td>ESXi</td>
<td>Elastic Sky X Integrated</td>
</tr>
<tr>
<td>FortiSSL</td>
<td>FortiGate Secure Sockets Layer</td>
</tr>
<tr>
<td>FRCH</td>
<td>FRCH Design Worldwide</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HP</td>
<td>Hewlett Packard</td>
</tr>
<tr>
<td>IAP</td>
<td>Internet Access Provider</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>Mb/s</td>
<td>Megabytes per Second</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multi-In-Multi-Out</td>
</tr>
<tr>
<td>MSDN</td>
<td>Microsoft Developer Network</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>R2</td>
<td>Release 2</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In-User Service</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>SCOM</td>
<td>System Center Operations Manager</td>
</tr>
<tr>
<td>SE</td>
<td>Standard Edition</td>
</tr>
<tr>
<td>SMB</td>
<td>Small and Medium Business</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>Sr.</td>
<td>Senior</td>
</tr>
<tr>
<td>SSIDs</td>
<td>Service Set Identifications</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>UC</td>
<td>University of Cincinnati</td>
</tr>
<tr>
<td>VLANs</td>
<td>Virtual Local Area Networks</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VP</td>
<td>Vice President</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WebSSL</td>
<td>World Wide Web Secure Sockets Layer</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WLC</td>
<td>Wireless LAN Controller</td>
</tr>
<tr>
<td>WPAx</td>
<td>Wi-Fi Protected Access 802.1X</td>
</tr>
</tbody>
</table>

Table 2: List of Acronyms
### 5.2. Appendix B: Technologies List

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba AP</td>
<td>IAP-105</td>
</tr>
<tr>
<td>Camtasia</td>
<td>Version 8</td>
</tr>
<tr>
<td>CentOS</td>
<td>6.3</td>
</tr>
<tr>
<td>Dell</td>
<td>Poweredge 1950</td>
</tr>
<tr>
<td>Ekahau</td>
<td>HeatMapper</td>
</tr>
<tr>
<td>Fortinet</td>
<td>FortiGate 200B</td>
</tr>
<tr>
<td>Fortinet</td>
<td>FortiAP FAP320B</td>
</tr>
<tr>
<td>Fortinet</td>
<td>FortiGate 300A</td>
</tr>
<tr>
<td>FortiNet</td>
<td>FortiPlanner</td>
</tr>
<tr>
<td>FortiOS</td>
<td>4.3.7</td>
</tr>
<tr>
<td>Foundry</td>
<td>FastIron Edge X448</td>
</tr>
<tr>
<td>Foundry</td>
<td>FastIron Edge X424</td>
</tr>
<tr>
<td>Foundry AP</td>
<td>Ironpoint 250</td>
</tr>
<tr>
<td>HP</td>
<td>E8212zl</td>
</tr>
<tr>
<td>HP</td>
<td>E5412zl</td>
</tr>
<tr>
<td>HP</td>
<td>ProLiant DL380 G6</td>
</tr>
<tr>
<td>HP</td>
<td>ProLiant DL380 G5</td>
</tr>
<tr>
<td>Juniper WLC (demo)</td>
<td>WLC8</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows Server 2008 R2 w/ SP1</td>
</tr>
<tr>
<td>Microsoft</td>
<td>System Center Operations Manager 2012</td>
</tr>
<tr>
<td>Microsoft</td>
<td>SQL Server 2008</td>
</tr>
<tr>
<td>Nagios</td>
<td>Version 3.0</td>
</tr>
<tr>
<td>OpenVPN</td>
<td>Version 2.3.1</td>
</tr>
<tr>
<td>PFSense</td>
<td>Version 2.0.3</td>
</tr>
<tr>
<td>Putty</td>
<td>Version .6</td>
</tr>
<tr>
<td>Team Viewer</td>
<td>Version 8</td>
</tr>
<tr>
<td>Verizon</td>
<td>MiFi 4G LTE</td>
</tr>
<tr>
<td>Wi-Fi Analyzer</td>
<td>Version 3.5.2</td>
</tr>
<tr>
<td>Zenoss</td>
<td>Version 4.2</td>
</tr>
</tbody>
</table>

Table 3: Technologies List
5.3. Appendix C: Wireless Network Configuration Manuals

*The manuals that appear in the following sections are for FRCH’s use. The project team created these by personal request of Matt Davidson as Disaster Recovery documentation.

5.3.1. FortiGate Wireless Networks Configuration

This deployment guide will create two SSIDs. One SSID will be for employees and the other SSID will be for Guest Internet Access. It also covers the basic setup of the FortiAP FAP320B.

1. Create RADIUS Server on FortiGate

NOTE: Firewall rules may need to be created to allow the FortiGate to communicate with the RADIUS server.

Click on Users then expand Remote

![FortiGate User Menu](image)

Figure 30: FortiGate User Menu

- Click on RADIUS then Create New and enter the appropriate information. Leave the Authentication Scheme set to default.
NOTE: the Primary server Secret is the same secret created on the RADIUS server client.

Figure 31: FortiGate RADIUS Options

- After the appropriate information has been filled out, click on Test on the Primary Server section. Input a valid username and password.

Figure 32: RADIUS Test

- Successful message is returned. If not, check the event viewer on the RADIUS server for insight to why the connection failed. Firewall policies may need to be created to allow
ports 1812 and 1813. Also a policy might need to be created to allow 1645 and 1646. Ports 1645 and 1646 were used for RADIUS at one point but the official ports are 1812 and 1813.

Figure 33: RADIUS Test Successful


- An LDAP server will also need to be added for the management of Administrators that are allowed to add guest to the Public SSID. This will be used later on in the process for setting up the Public SSID
- While still under Remote in the Users Section, click on LDAP.
- Fill in the appropriate IP address for the Active Directory Server and a name, leave everything else at their defaults, and then click OK.
3. Internal Wireless

- Click on Wi-Fi Controller then expand Wi-Fi Network and click on SSID

- Select Create New and configure appropriate fields as below (Settings will not be the same as below but similar).
NOTE: Block Intra-SSID Traffic can be selected if wanted.

Figure 36: WLC SSID Settings

4. Create Firewall Address Object for FRCH-Private

NOTE: The Firewall Address Object will be used in creating firewall rules later.

- Click on Firewall Object, expand Address and select Address
59

Figure 37: WLC Firewall Objects

- Select Create New and enter Address Name, Type Subnet/IP Range and the interface (FRCH-Private in this case)

Figure 38: Creating Firewall Address Object for FRCH-Private SSID

5. Create DHCP Server Relay

- Click on system then expand Network and click on DHCP Server
Figure 39: Creating DHCP Server on FortiGate 200B

- Select Create New and fill in appropriate values

**NOTE**: Mode will be Relay and Interface Name will be interface for the FRCH-Private SSID

![DHCP Server Settings on FortiGate 200B](image)

Figure 40: DHCP Server Settings on FortiGate 200B

- The DHCP Relay is now configured for the FRCH-Private SSID.

6. **Create Public SSID**
• Now it is time to create the FRCH-Public SSID which will use a captive portal for authentication.

• FRCH-Public

• Create a local group to manage guest access to FRCH-Public.

• Select Users then expand User Group

![FortiGate 200B User Menu]

Figure 41: FortiGate 200B User Menu

• Select Create New, Enter name and type (Firewall in this case) no need to add any users to the group yet and click OK
7. **Guest Administrator**

- Now that the Group is created for the Public access, an administrator profile and administrator needs to be created to manage the users in the Guest group. This will include using an LDAP security group. Use the same steps above but add a Remote Authentication Server (this is the LDAP server added earlier). Also select Specify under Group Name for added security (an Active Directory security group will need to be added in AD with the same name and the correct users in the group.)
Create an administrator with only access to the User tab which will authenticate through the AD/LDAP security group. The first step is to create an Admin Profile that will be restricting access to the Users section.

- Go to System, then expand Admin and click on Admin Profile
• Select Create New. Enter a name for the profile. Leave all the permission set to none other than Auth Users. In the case of Auth Users, click Read-Write then click OK.

![New Admin Profile](image)

Figure 45: Admin Profile Options

8. **LDAP Administrator**

• Now that the Guest-Admins Profile is set up, it is time to create an Administrator that will use LDAP authentication and will be part of the Guest-Admins profile.

• Still under System with the Admin section expanded, click on Administrators.
Select Create New, Input a user name that is the same as a valid AD/LDAP user, Set the Type to Remote, Select User Group created earlier, set a backup password in case AD/LDAP goes down, select the Guest Admin Profile and if wanted restrict the host in which this user can log in from via IP address (the computer would have to have a static IP address for this to work well). Click ok.
9. **Create Public SSID**

- Using the steps used when the FRCH-Private with the exception of the security type. Captive Portal will be used for the Security. Once you set the Security Mode to Captive Portal, you can customize the Captive Portal Messages. Also add the FRCH-Public Guest List to the Selected User Groups and check the Block Intra-SSID Traffic.
Figure 48: FRCH-Public SSID Settings

- Now a new Firewall Object will need to be created for FRCH-Public IP address range.

  Follow the steps used earlier to create the Firewall Object.

Figure 49: FRCH-Public Firewall Address Object

- Create a DHCP relay Server using the same steps as outlined earlier.
10. Create AP Profile

- Click on Wi-Fi Controller, then expand Managed Access Points and click on Custom AP Profile. There is a lot going on in this step.
- Click on Create New.
- Give the Profile a Name, and select the Platform (AP Model). In this example the platform is set to FAP320B.
Since the FAP320B has two radios the settings are configured by radio number. Settings for Radio 1 to be set as pictured for this case. Each Wireless implementation is different so set these settings accordingly. The settings that have been changed from their defaults are Radio Resource Provision, the TX power has been dropped to 50% and the FRCH-Private and FRCH-Public SSIDs have been selected to transmit on this radio. The settings for Radio 2 are identical except for the Channels.

![Radio 1 settings](image)

**Figure 52: Custom AP Profile Settings, Radio 1**

- Radio 2 Settings for the Channel are different from Radio 1. Channels 1, 6, and 11 are the only channels that don’t overlap. So it is best practice to only allow these channels.
Figure 53: Custom AP Profile Settings, Radio 2

- Click OK to create the Custom AP profile

**NOTE:** If rogue AP scanning is wanted, then the Background Scan option needs to be set on both Radios
5.3.2. Access Point Configuration

- The APs have several methods for finding the WLC on the FortiGate Firewall. In this example the Static method will be used.
- Connect to the FAP320B via a console cable with a Serial to USB adapter.
- Open Putty and configure as shown below. Make sure to select the correct COM port and click open.

![Putty Configuration](image)

Figure 54: Serial Connection to AP using Putty

- A static IP address and WLC address will be set.
- If this is the first time logging into the AP, the user name will be admin and the password is left blank.
- Use the commands below to set the Discovery mode to Static. Set the appropriate IP address, subnet mask and gateway.
  - `cfg -a ADDR_MODE=STATIC`
  - `cfg -a AP_IPADDR=172.16.X.X`
- Now set the IP address for FortiGate Firewall
  - `cfg -a AC_IPADDR_1=172.16.X.X`
- Change the admin password.
  - `cfg -a passwd`
- Save the configuration
  - `cfg -c`
- To verify the settings on the FortiAP use the following command.
  - `cfg -s`
- Reboot the AP
- Log in to the WLC
- The configuration changes only take effect after the AP is rebooted. Now unplug the AP and install in its permanent location. Once the AP is powered on and plugged back into the network the WLC built into the FortiGate unit will display the AP in the Managed FortiAP list under Wi-Fi Controller.

![Managed AP List]

Figure 55: Managed AP List
- The AP has to be authorized on the WLC. Select the AP and click Edit. Name the AP and click Authorize. After clicking Authorize, More settings are available for configuration.

![Edit Managed Access Point](image)

**Figure 56: Authorized AP**

- Under AP Profile, Click Change and select the custom profile created previously. The AP will implement the settings from the custom AP profile. Click OK
Figure 57: Setting AP Custom Profile

- The AP Status will now be “Connected.”

Figure 58: Managed FortiAP List

- Now the firewall policies need to be created so the SSIDS function desired.
- Select Policy then expand Policy.
Figure 59: FortiGate 200B Firewall Policy

- First create the firewall policy to allow the FRCH-Public SSID to access only the Internet.
• Select Create New. Set the configuration as below. Make sure to select Enable NAT and set NAT to “Use Destination Interface Address”. This policy will restrict the traffic on FRCH-Public to the Internet only.

![Firewall Policy Settings](image)

Figure 60: Firewall Policy Settings for FRCH-Public SSID to Access the Internet
• Now create another policy identical to the previous policy but the Source Interface will be set to FRCH-Private.

![New Policy](image)

Figure 61: Firewall Policy Settings for FRCH-Private SSID to Access the Internet

• More firewall policies will be created to allow FRCH-Private to access internal resources. Below is an example of allow the FRCH-Private SSID access to a server network on port 3 of the FortiGate device.
Figure 62: Firewall Policy Settings for FRCH-Private SSID to Access the Server Farm
5.3.3. RADIUS Configuration and Wireless Deployment

- Install Network Policy and Access Service

![Windows Server 2008 R2 Sever Roles](image)

**Figure 63: Windows Server 2008 R2 Sever Roles**

- Click Next
- Select “Network Policy Server” then click install

![Role services selection](image)

**Figure 64: Network Policy and Access Services Options**

- Once installed go to Network Policy Server under Administrative Tools
- Expand RADIUS Clients and Servers

![Network Policy Server interface](image)

**Figure 65: Network Policy Server**

- Right Click RADIUS Client and Select New
- Fill in appropriate fields as below (IP address will be different)
NOTE: The Shared secret will be used later in creating the RADIUS server on the FortiGate firewall.

Figure 66: RADIUS Client Options

- Click on NPS(Local) then Select from the drop down “RADIUS Server for 801.1X Wireless or Wired Connections” then select Configure 802.1X
Figure 67: Network Policy Server Wizard

- Select “Secure Wireless Connections” and fill in and Name then click next.

Figure 68: Network Policy Server Wizard 802.1X

- Select the RADIUS client created earlier then click Next.
Select Microsoft Protected EAP (PEAP) then click Next.
• At the Specify User Groups screen click Add, and then type “Domain Users” in the text box then click check names, then click OK.

![Figure 71: Network Policy Server Wizard Add User Group](Image)

• Click Next on the Configure Traffic Controls screen.
Figure 72: Network Policy Server Wizard Traffic Controls

- Click Finish on the Configure IEEE 802.

Figure 73: Network Policy Server Wizard 802.1X Completed

- RADIUS is now configured on the server side.