The All in One Network Solution (A.I.O.N.S.)

By:

Nadder Al-Ajmi
Nathaniel DeMelo
Andrew Fletcher
Carla Warren

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

© Copyright AIONS
The author grants to the School of Information Technology permission
to reproduce and distribute copies of this document in whole or in part.

Nadder Al-Ajmi
Nathaniel DeMelo
Andrew Fletcher
Carla Warren

Advisor: Professor Mark Stockman

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2015
Acknowledgements

We would like to thank Professor Mark Stockman, Dr. Patrick Kumpf, Professor James Scott, our peers as well as the University of Cincinnati faculty for all of their help, guidance, and most of all patience in the development of our senior design project.

We would also like to thank FRCH Design Worldwide, Matt Davidson and Andrew Burgess, for their assistance as well as graciously allowing us to work countless hours in their offices.

Finally we would like to thank all our family and friends for their love and support.
Table of Contents

Abstract ........................................................................................................................................... 5
Introduction ..................................................................................................................................... 6
Problem Description ....................................................................................................................... 6
Research .......................................................................................................................................... 7
Solution .......................................................................................................................................... 9
Network Security ............................................................................................................................ 9
User Profile ....................................................................................................................................... 11
Use Case Scenarios .......................................................................................................................... 12
  1. Hotel Scenario ............................................................................................................................ 12
  2. Office Move Scenario ................................................................................................................. 13
  3. Scientific Remote Use Case ......................................................................................................... 15
Technologies ..................................................................................................................................... 16
Network Diagram ............................................................................................................................ 20
Project Budgets ............................................................................................................................... 21
Return Investment ............................................................................................................................. 22
Conclusion ......................................................................................................................................... 23
Works Sited: ....................................................................................................................................... 24
Appendices ......................................................................................................................................... 25
  Appendix A: Device Configuration ................................................................................................. 25
  Appendix B: Weekly Plan ................................................................................................................. 42
  Appendix C: Project Timeline ......................................................................................................... 46
  Appendix D: Deliverables AIONS Deliverables ............................................................................. 47
  Appendix E: Device Functionality Testing ..................................................................................... 48
  Appendix F: Customer Forms ......................................................................................................... 52
  Appendix G: Build Pictures ............................................................................................................ 57
List of Figures:
Figure 1. User Profile.................................................................................................................. 11
Figure 2. Hotel Use Case Diagram.................................................................................................. 12
Figure 3. Office Move Use Case Diagram........................................................................................ 14
Figure 4. Scientific Study Use Case Diagram................................................................................... 15
Figure 5. Initial Project Budget...................................................................................................... 21
Figure 6. Actual Project Budget..................................................................................................... 22
Abstract

The need for connectivity in today's world is vital. From schools to businesses to hospitals, connectivity helps spread information and knowledge to billions of people around the world. It is because of this reason that an affordable solution be developed to easily and readily provide this connectivity to a given area. Our solution; A.I.O.N.S. standing for All in One Network Solution, would provide portable wireless network coverage for a given area in a simple, easy to move setup, and use a small form package. AIONS would take advantage of the latest technologies to provide a high speed Wi-Fi signal for devices and computers to connect to. With minimal configuration required, AIONS aims to provide fast deployment for quick access to a wireless network in a designated area. This solution would benefit small businesses, schools, community organizations, search and rescue teams, religious institutes, and events in which require access to the Internet.
Introduction

Having your company’s network go down is the worst fear of a Network Administrator. Users are unable to work, files are lost, the company loses money, and no one is happy when this happens. A solution that can prevent this, while keeping your company up and running would be A.I.O.N.S. AIONS is an all in one network solution that was built for situations like this, as well as other detrimental situations such as natural disasters, remote location work, temporary internal wireless network connection, and network redundancy. AIONS has a simple deployment configuration depending on the deployment customization by the customer. There are different features that can be added to the device according to the needs of the customer. The default configuration of AIONS, or base configuration, would allow the customer to simply plug in an active Internet connection and power source to the system to have a wireless and/or wired network up and running in under four minutes. The customer has the power to choose the features they require making this device very compatible with all types of companies, schools, and organizations.

Problem Description

In the current market for networking solutions there are many options to choose from, with a wide range of pricing options. Most companies or organizations rely on a third party company to select, setup, and manage a networking solution. The problem with this method is that most small companies or limited budget organizations cannot afford such a costly solution. When looking for networking solutions, most small businesses, small organizations, and schools, at the very least look to acquire wireless and wired connectivity, network accessible storage, network security as well as mobility of the network. Too often though
these entities end up having to cut some added features due to budget limitations. The need for a simple, all in one solution, for creating a network that meets all client demands is the idea behind AIONS.

**Research**

There are several companies that have the ability to produce a product similar to AIONS but on a much more expensive scale. In order to come up with the best networking solution product, we researched and learned from these companies and what they are doing so we could come up with a solution that no other company has thought of. There are a few companies that are producing products that are similar to our solution that we can learn from, but hopefully surpass their product concept using a monetarily cheaper design. We found three different companies that have some type of similar product as AIONS. Those three companies are Aerohive, Extreme Networks, and Sierra Wireless. All three of these companies have pros and cons that are applicable to the AIONS device that we compared and contrasted, using the better aspects of their design and incorporating them into our solution.

Aerohive deployed a two part wireless system. The wireless network was built for the school students and employees, and a separate wireless system for the church congregation. Aerohive used a cloud based approach deployment and controller-less management architecture. This controller-less wireless network has access points that act like a firewall which is a functionality of the access point. This functionality makes it so that a NAC is not needed. The authentication of the users is based on the active directory, which would tie into the user logins. This cloud-based approach is easy to manage, centrally administered, cost effective and accommodates the increase of Wi-Fi devices while monitoring the wireless network and client activity. Our main concern with this network solution is that it is costly and lacks mobility; which is one of the aspects we targeted for in our AIONS design.
Extreme Networks is another company that uses an access point and has centralized management to be able to meet high user demands. Extreme Networks has a solution called IdentiFi Wireless that has scalable Wi-Fi, it’s adaptive, cost effective, and has high performance. For the users of this network, it is easy to use, has fast connectivity, and smart adaptation. Looking at this solution from the IT aspect, this solution is simple to manage, fast to deploy, and has smart architecture. However, this solution is more expensive than the network solution AIONS is offering. To be able to handle all of these network features would require more upfront investments to be able to get a greater return of investments. Another con of this network would be to making sure it is secure from unauthorized, unsecured, or rogue access points.

Sierra Wireless uses cellular broadband which is more reliable than secondary networks for downtime and other risks or wired architecture. Sierra Wireless has a network solution called AirVantage M2M Cloud. This solution is fast, secure, and has a reliable high volume data transmission. The wireless equipment Sierra Wireless has is a simple setup configuration and is integrated with open standards, device protocols, and network applications. There is also remote support and maintenance, along with the web based self-care for customers. A con of this network solution is the cost of managing the solution, along with the subscription and billing. To make sure the network is always running someone has to monitor the system. To have Sierra Wireless monitor the system and analytics can be quite costly depending on the type of solution you are looking to incorporate. AIONS would be a base cost solution, monthly subscriptions would only incur if the specific network solution chooses to use a local ISP and needed technical support.
Solution

The solution to this problem is a portable all in one network system that has integrated networking devices and technology to provide internet network access both physically and wirelessly to any location, remote or otherwise. Also providing additional network storage solutions for storing data and sharing files. This solution will also be affordable compared to similar competing network solutions. Our AIONS system has simple deployment requiring no advanced knowledge of IT or networking. This solution can also serve as redundancy for a network in case of a network failure, providing a fast solution to returning network functions to a disabled or damaged LAN.

Network Security

Security is a vital aspect of networking and the AIONS device is built with security in mind. AIONS encompasses different networking possibilities such as directly connecting into existing network topologies to replace a main router. An example would be hosting a small network or providing wireless access to a remote area. AIONS provides security that covers different networking configurations and scenarios. Physical security of the device is another consideration that AIONS addresses.

The AIONS device will implement the latest in wireless networking security. The default wireless networking security features that will be enabled with no additional configuration will be WPA2 with encryption protocol AES. By default, when AIONS is plugged into a power source, Wi-Fi access is available in a short time frame to use. The default configurations would include SSID name and password for connecting to the wireless network. This would allow for quick setup to provide a wireless signal for a given area with standard wireless security measures. Additionally, AIONS can be configured to have these network security settings
adjusted per the client’s need. For example, the SSID name can be changed and broadcasting of
the SSID can be turned off. WPA-Enterprise mode can be enabled and a RADIUS authentication
server can be implemented and configured for the client. MAC ID filtering can also be
preconfigured using client specified MAC address. AIONS can be configured as per client
request for specific wireless needs.

AIONS physical network security will also be configurable as per client need. By default
the AIONS device will have a preconfigured Firewall. The Firewall will be enabled with mostly
default policies and settings with slight adjustment for further security. This can be configured in
a more complex manner to limit and allow traffic on the physical network as per the client’s
need. AIONS will also include Network Security Monitoring IDS/IPS system in the form of
Security Onion. Security Onion is an OS that will reside virtually on AIONS to monitor and log
all network traffic. Security Onion will be configured with default settings with slight adjustment
to the logging settings to conserve hard disk space. However, this feature can also be customized
to client specifications to allow security alerts that can be sent directly to emails or specific hosts.
For example, logging policy adjustments and/or monitoring sensors and also packet capturing.
Analyzing tools within Security Onion such as Squert, could be accessed directly or remotely as
per the clients’ request. The AIONS device will also be physically secured by a lock and key to
protect against unauthorized access to the device’s components as well as unauthorized port
access.

Network Security techniques and technologies continue to grow and AIONS is
built with this in mind. Scalability of AIONS is possible through the upgrading of
components and updates to software. The client is not restricted from upgrading AIONS
as they see fit, AIONS can be customized to every client’s specific needs.
### User Profile

<table>
<thead>
<tr>
<th>Application: A.I.O.N.S. (All in One Network Solution)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Potential Users:</strong> Small Businesses, Community Organizations, Religious Institutes, Search and Rescue, Events.</td>
</tr>
<tr>
<td><strong>Software and Interface Experience:</strong> The user will have little to basic software and interface experience similar to a smart device (phone, tablet, and laptop). The AIONS device itself would plug in and be ready to go with little to no configuration. From there the user would need to sign into the Wi-Fi network via desired device.</td>
</tr>
<tr>
<td><strong>Experience with Similar Applications:</strong> No experience with similar applications would be necessary for the user.</td>
</tr>
<tr>
<td><strong>Task Experience:</strong> The task experience for the user would be similar to signing into a Wi-Fi connection using a mobile device or computer. Logging into the available Wi-Fi connection produced by the AIONS device. For initial configuration of the device a simple input of name for the connection and password if desired may be used.</td>
</tr>
<tr>
<td><strong>Frequency of Use:</strong> The user would be able to reuse the AIONS device as frequent as needed. AIONS would be able be reconfigured with different name and password entries as desired for reuse.</td>
</tr>
<tr>
<td><strong>Key Interface Design Requirements that the Profile Suggests:</strong> Simple to deploy physical device. Once deployed, an option for the user to deploy a basic network with no name and password configurations or a second option for the user to simply enter a name for the network and a password if desired.</td>
</tr>
</tbody>
</table>
| **Summary:**  
  - Simple deployment/activation of device  
  - Simple user input via keyboard  
  - Two network options; basic and specified (name, password)  
  - User connects device or computer to deployed network |

*Figure 1. User Profile*
Use Case Scenarios

1. Hotel Scenario

The Westin hotel has been booked for a conference for over 120 people. The Westin has a network connection that only allows 1 physical device to plug directly into the network. The wireless network that is hosted by the hotel can only host up to 20 devices on their network in the conference room. The conference room needs to be set up to allow more than 120 devices to connect to the network without the hotel having to upgrade their whole network. This would be a great time to use AIONS. AIONS in this situation would allow users to connect to the AIONS wireless network without users worrying about slow network speeds, connection drops, or user network charges.

Figure 2. Hotel Use Case Diagram
2. **Office Move Scenario**

The Spicefire Group, a growing design company of 150 employees is moving into a new office location and plans to re-use their current network as well as storage hardware components. Time is money; therefore they cannot afford any down time. Their initial plan was to power down and move all the components during a single weekend, but after much debate the IT department was able to convince upper management that this approach is simply too risky and not practical. If the team should run into any hard-stops during the weekend installation will force Mondays’ work-flow to be reduced to a crawl. The IT department needs a temporary network solution that can be setup at the new location ahead of time to allow employees access to files stored on the server. Thus giving them an overlapping time buffer to properly move as well as configure the permanent solution.

This would be the perfect application for the AIONS device. It could be setup at either location and be integrated. AIONS can be configured to meet the customers networking demands. The clients would be able to utilize the external data ports as well as the router feature to support the company until the permanent solution is in place. AIONS could also serve as a backup if the IT department should come across any issues.
Figure 3. Office Move Use Case Diagram
3. **Scientific Remote Use Case**

The scientific research team Organisms R Us is planning an extended trip to a remote location to study the behavior of microorganisms during a climate change. They will have a large base camp set up for Shelter and Research. Since the team will be on an extended trip and logging a large amount of data they have decided to implement a portable solution for storage. While researching options for their problem, the researchers realized that if they are going to invest a large amount of money, they would like to get more than just storage out of their final choice in product.

AIONS is perfect for Organisms R Us, not only would it provide the storage they need for their extended project, but also allows them to connect to the Internet if paired with a satellite wireless connection. With Internet access they could combine the research side of their project simultaneously with the data collection, as well as use email and other sources of communication to transmit data to other team members back at the home office.

![Figure 4. Scientific Study Use Case Diagram](image)
Technologies

There were many different ways that AIONS could have been configured using different combinations of hardware/software. We decided on the specific lists of hardware and software below based on personal experience obtained from various courses we had taken, such as Professor Stockman’s networking and network security course, as well as researching methodologies, advice from peers and superiors, and various articles and information obtained online.

Below is a list of the hardware and software used to create AIONS.

**Hardware:**
We were working on a limited budget, however, purchased hardware that would meet the demand for our network and storage requirements for AIONS as well as any spare hardware we personally had. Specific hardware utilized;

- Intel Core i5-4690K 3.5 GHz LGA 1150 CPU
- ASUS Z97 LGA 1150 ATX Intel Motherboard
- Ballistix Sport 16 GB RAM
- Samsung 850 Pro Series 128 GB Solid State Drive
- Seagate Barracuda 1 TB Hard Disk Drive
- Western Digital 500 GB Hard Disk Drive
- Samsung 40 GB Hard Disk Drive
- Western Digital 40 GB Hard Disk Drive x2
- Corsair CX Series CX600M ATX Modular Power Supply
- Intel EXPI9301CT Gigabit PCIe X1 Adapter
- Ethernet Coupler
- Ethernet Wall Plate
- TP-LINK TL-SG108 8 Port 10/100/100 Switch
- TP-LINK 300 Mbps Wireless N Access Point

Cooler Master Storm Trooper Full Tower Case
Software:

For software we learned more towards open source solutions. We knew early on we required routing software as well as a file server solution. Through research, trial and error, we decided on the software listed below;

**ESXi** – We required a bare metal hypervisor to manage the various virtual machines we would be working with. This allows us to take advantage of a single set of hardware listed above for multiple virtual machines and servers. VMware’s ESXi was chosen for many reasons, one being prior experience to the software in Professor Stockman’s Cloud Computing course. An alternative to this was KVM (Kernel-based Virtual Machines).

**pfSense** – We required a routing software solution to handle various routing tasks that would be done by AIONS. pfSense not only would accomplish this task but also provide excellent networking security as well. This software was chosen as well for many reasons one including prior experience from Professor Stockman’s Networking and Network Security course.

**Security Onion** – We desired to have additional thorough network security on AIONS and decided on Security Onion as it provides host and network based intrusion detection, network security monitoring, and log management. We are able to install Security Onion as a separate virtual machine on the AIONS network to aid in monitoring and alerting of any security breaches or threats.

**Windows Server 2012** – To handle file storage and file server duties, Windows Server 2012 was chosen as the OS can handle those tasks and also provide more server functionality to the client based on needs such as active directory. We are able to customize server needs with Windows Server 2012.
OpenFiler – As a suggestion made by Professor Stockman, an open source solution for file sharing and file server would be ideal due to Microsoft licensing for Windows Server 2012. As such, we integrated OpenFiler into AIONS to provide file storage and sharing as an alternative to Windows Server 2012.
Network Diagram

Below is a network diagram to portray the layout of the traffic that will occur on the system:

![Network Diagram](image-url)
**Project Budgets**

These two budgets represent the components we initially planned on using to bring this concept to actuality as well as the ones we actually utilized. Our forecasted budget was around $2,326.01 for all of the components we sought necessary as well as some cosmetic accessories.

We planned on looking into the possibility of second hand components as well as a sponsorship. We were forced to rethink our project when those resources did not provide us with the support needed. We then decided to take an alternate route, which not only cut costs dramatically but demonstrated more concepts that were acquired from the university.

**Budget 1 (Initial)**

```
<table>
<thead>
<tr>
<th>Category</th>
<th>Component</th>
<th>Cost</th>
<th>Quantity</th>
<th>Main Rig</th>
<th>R2</th>
<th>Other</th>
<th>Cost Main Rig</th>
<th>Cost R2</th>
<th>Cost Other</th>
<th>Total Component Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case</td>
<td>Case labs</td>
<td>500</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>500</td>
</tr>
<tr>
<td></td>
<td>Cooler Master Mod case</td>
<td>129.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>129.99</td>
<td></td>
<td>169.99</td>
</tr>
<tr>
<td>Processors</td>
<td>i3-4560</td>
<td>243.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>243.99</td>
<td></td>
<td></td>
<td>243.99</td>
</tr>
<tr>
<td></td>
<td>i5-4660</td>
<td>129.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>129.99</td>
<td></td>
<td></td>
<td>129.99</td>
</tr>
<tr>
<td>Cooling:</td>
<td>Akasa X6L</td>
<td>199.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>199.99</td>
<td></td>
<td></td>
<td>199.99</td>
</tr>
<tr>
<td></td>
<td>Akasa X6L</td>
<td>129.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>129.99</td>
<td></td>
<td></td>
<td>129.99</td>
</tr>
<tr>
<td>RAM:</td>
<td>Ballistic Spear 8GB</td>
<td>79.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>79.99</td>
<td></td>
<td></td>
<td>79.99</td>
</tr>
<tr>
<td></td>
<td>Ballistic Spear 8GB (single)</td>
<td>79.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>79.99</td>
<td></td>
<td></td>
<td>79.99</td>
</tr>
<tr>
<td>Storage:</td>
<td>Samsung 550GB</td>
<td>129.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>129.99</td>
<td></td>
<td></td>
<td>129.99</td>
</tr>
<tr>
<td></td>
<td>Hitachi 1TB</td>
<td>54.01</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>108.02</td>
<td></td>
<td></td>
<td>108.02</td>
</tr>
<tr>
<td>Network:</td>
<td>ASUS Switch</td>
<td>36.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>36.99</td>
<td></td>
<td></td>
<td>36.99</td>
</tr>
<tr>
<td></td>
<td>ASUS Router</td>
<td>119.99</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>119.99</td>
<td></td>
<td></td>
<td>119.99</td>
</tr>
<tr>
<td></td>
<td>Ethernet Coupler</td>
<td>1.96</td>
<td>7</td>
<td>7</td>
<td></td>
<td></td>
<td>13.02</td>
<td></td>
<td></td>
<td>13.02</td>
</tr>
<tr>
<td></td>
<td>wall Plate (Ethernet)</td>
<td>0.82</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>0.82</td>
<td></td>
<td></td>
<td>0.82</td>
</tr>
<tr>
<td>Other:</td>
<td>TVGA PS2</td>
<td>293.91</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>293.91</td>
<td></td>
<td></td>
<td>293.91</td>
</tr>
<tr>
<td>Accessories:</td>
<td>Noct Light</td>
<td>17.45</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>17.45</td>
<td></td>
<td></td>
<td>17.45</td>
</tr>
<tr>
<td></td>
<td>Protective Cap (ethernet)</td>
<td>1.99</td>
<td>50</td>
<td>10</td>
<td></td>
<td></td>
<td>10</td>
<td>50.00</td>
<td></td>
<td>50.00</td>
</tr>
</tbody>
</table>

Total: 2112.96 34 7 4 34 307.96 919.97 500.00 2526.01

Figure 6. Initial Project Budget
Budget 2 (Actual)

Below is the list of actual hardware components used to bring this network solution concept to reality:

<table>
<thead>
<tr>
<th>Senior Design Actual Cost Project:</th>
<th>Price</th>
<th>Quantity</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooler Master Storm Trooper Full Tower Case</td>
<td>159.99</td>
<td>1</td>
<td>159.99</td>
</tr>
<tr>
<td>Processors: Intel Core i5-4690K 3.5GHz LGA 1150 Boxed Processor</td>
<td>199.99</td>
<td>1</td>
<td>199.99</td>
</tr>
<tr>
<td>Motherboard: ASUS Z97 LGA 1150 ATX Intel Motherboard</td>
<td>129.99</td>
<td>1</td>
<td>129.99</td>
</tr>
<tr>
<td>RAM: Ballistix Sport 8GB</td>
<td>74.99</td>
<td>1</td>
<td>74.99</td>
</tr>
<tr>
<td>Storage:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samsung 850 Pro Series 128GB SSD</td>
<td>118.99</td>
<td>1</td>
<td>118.99</td>
</tr>
<tr>
<td>Seagate Barracuda 1 TB HDD</td>
<td>Free</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Western Digital 500GB Hard Drive</td>
<td>Free</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Samsung 40gb Hard Drive</td>
<td>7.49</td>
<td>1</td>
<td>7.49</td>
</tr>
<tr>
<td>Western Digital 40gb Hard Drive</td>
<td>7.49</td>
<td>2</td>
<td>14.98</td>
</tr>
<tr>
<td>PSU:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corsair CX Series CX600M ATX Modular Power Supply</td>
<td>69.99</td>
<td>1</td>
<td>69.99</td>
</tr>
<tr>
<td>Network:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linksys EA3600-RM AC1200 Dual Band Router</td>
<td>42.99</td>
<td>1</td>
<td>42.99</td>
</tr>
<tr>
<td>Intel EPIQ100 CT Gigabit PCIe X1 Adapter</td>
<td>39.99</td>
<td>2</td>
<td>79.98</td>
</tr>
<tr>
<td>Ethernet Coupler</td>
<td>1.86</td>
<td>6</td>
<td>11.16</td>
</tr>
<tr>
<td>Wall Plate (Ethernet)</td>
<td>0.82</td>
<td>1</td>
<td>0.82</td>
</tr>
<tr>
<td>TP-LINK TL-SG108 8Port 10/100/1000 Switch</td>
<td>29.99</td>
<td>1</td>
<td>29.99</td>
</tr>
<tr>
<td>3FT PLEXShoot Series 24AWG Cat6 550MHz</td>
<td>1.06</td>
<td>7</td>
<td>7.42</td>
</tr>
<tr>
<td>Other:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LG 24X Internal DVD Rewritable Drive SATA</td>
<td>15.99</td>
<td>1</td>
<td>15.99</td>
</tr>
<tr>
<td>Accessories: Syba 4-port SATA 1.5Gbps PCI controller with RAID</td>
<td>31.99</td>
<td>1</td>
<td>31.99</td>
</tr>
<tr>
<td>Totals:</td>
<td>973.6</td>
<td></td>
<td>$1,036.74</td>
</tr>
</tbody>
</table>

**Figure 7. Actual Project Budget**

**Return Investment**

The device’s cost of production was $1,035. This is what it cost to build the current version of AIONS. This cost includes the hardware and software needed to bring AIONS up and running. The base price for the AIONS device has been set at $4,000. We came up with this price based on our production costs, labor, and competitor pricing. To figure out our Return of Investment, we based our findings off of selling 5 AIONS devices at the base price. The cost of producing 6 AIONS devices at $1,035 per device would be $5,175. The consumer would have to pay $4,000 per device and the total cost for all 5 AIONS devices would be $20,000. To figure
out the return of investment, we would take the total cost for all 5 AIONS device ($20,000) subtract the cost of producing all 5 AIONS devices ($5,175) and divide that by the cost of producing all 5 AIONS devices ($5,175). The Return of Investment for our AIONS device is 2.78%.

**Conclusion**

In conclusion, in the information age, connectivity is a necessity. Organizations of all sizes rely on Internet connectivity to complete their day to day tasks. This reliability of Internet and network connectivity, however, comes at a cost. With many solutions and products out there trying to meet the needs of companies and organizations, there is a lack of all in one networking solutions that fulfill that need and fulfill it affordably. This and more is what we kept in mind and aimed for when we created AIONS. To meet the needs for network connectivity for any company, school, or organization looking for an affordable solution and to even meet unique mobile networking needs. AIONS incorporates all a network system needs into one portable box which can be implemented in just about every professional work environment as well as public events and more.
Works Sited:


Appendices

Appendix A: Device Configuration

AIONS Configuration Log Documentation

IP Addresses:

<table>
<thead>
<tr>
<th>Name</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi</td>
<td>192.168.0.2</td>
</tr>
<tr>
<td>PfSense</td>
<td>192.168.0.107</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>192.168.0.109</td>
</tr>
<tr>
<td>Security Onion</td>
<td>192.168.0.111</td>
</tr>
<tr>
<td>Wireless Access Point</td>
<td>192.168.0.110</td>
</tr>
<tr>
<td>OpenFiler</td>
<td>192.168.0.112</td>
</tr>
</tbody>
</table>

Boot time of AIONS to full Internet connection – 3 minutes 47 seconds
ESXi 1 Summary Tab
ESXi using NIC1, assigned automatic IP address of 192.168.0.100

Download of vSphere client to access ESXi configuration settings for virtual machines

Physically connected laptop via Ethernet cable to external Ethernet port which is connected to switch

Used vSphere Client to connect to ESXi using IP address 192.168.0.100

Added the USB hotspot device to PfSense virtual machine

Configured PfSense VM network to NIC1 on ESXi host

Changed ESXi Management Network IP address to a static IP of 192.168.0.2 to keep all networks within the same subnet

Due to VMs being down, unable to obtain IP automatically from the DHCP server on PfSense. Manually changed vSphere Client computer to static IP on same subnet 192.168.0.149

Successful connection to ESXi using vSphere Client

Started VMs PfSense and Windows Server 2012

Changed vSphere Client laptop host adapter settings back to automatically obtain IP address from the PfSense DHCP server

Changed Virtual Machine Startup/Shutdown properties to allow Virtual Machines to turn on immediately when the host starts up

Created a Virtual Port Group SPAN-LAN on vSwitch0

Created a Virtual Port Group SPAN-WAN on vSwitch2

Changed both SPAN-LAN and SPAN-WAN properties to VLAN ID All (4095)

Changed both SPAN-LAN and SPAN-WAN properties security settings to enable promiscuous mode

Added second NIC to Security Onion VM

Changed NIC1 on Security Onion VM to SPAN-LAN Port Group

Changed NIC2 on Security Onion VM to SPAN-WAN Port Group

Added three identical hard drives to datastore within Storage settings for use as RAID

Added new storage to datastore with label “OpenFileShare”

Enter OpenFiler Server IP address for new storage and entered folder location “/mnt/share1/aionshare” PfSensePfSensePfSensePfSensePfSensePfSensePfSensePfSensePfSensePfSense
ESXi 2 Loading Installer

ESXi 3 Installing ESXi
Initial configuration of pfSense LAN on NIC1 using interface em0 with a static IP address of 192.168.0.107.

Using web browser, configured WAN interface with DHCP settings and assigned NIC2 named em1. Automatic IP assigned via internal office network’s DHCP server to obtain Internet access. IP address varies each time connection is made.

Configured DHCP server to enabled on LAN to provide IP addresses within the range of 192.168.0.150 – 192.168.0.200

Configured Windows Server 2012 to static DHCP list with IP address of 192.168.0.109

Configured Security Onion to static DHCP list with IP address of 192.168.0.111

Configured OpenFiler to static DHCP list with IP address of 192.168.0.112
pfSense 2 Installing pfSense

pfSense 3 Configuring Network Interfaces
### pfSense 4 DHCP Lease List

<table>
<thead>
<tr>
<th>IP address</th>
<th>MAC address</th>
<th>Hostname</th>
<th>Start</th>
<th>End</th>
<th>Online</th>
<th>Lease Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.154</td>
<td>e:41:7f:30:0f:84d:80</td>
<td>Kasper</td>
<td>2015/04/09 22:12:30</td>
<td>2015/04/10 00:21:35</td>
<td>online</td>
<td>active</td>
</tr>
<tr>
<td>192.168.1.165</td>
<td>c:4:48:87:3c:df:69</td>
<td>CORTEKES500065</td>
<td>2015/04/09 22:09:26</td>
<td>2015/04/10 00:00:06</td>
<td>online</td>
<td>active</td>
</tr>
<tr>
<td>192.168.1.109</td>
<td>00:0c:28:4e:6e:28</td>
<td>Server12</td>
<td>n/a</td>
<td>n/a</td>
<td>online</td>
<td>static</td>
</tr>
<tr>
<td>192.168.1.111</td>
<td>00:0c:28:31:0c:3c</td>
<td>SecurityOnion</td>
<td>n/a</td>
<td>n/a</td>
<td>online</td>
<td>static</td>
</tr>
<tr>
<td>192.168.1.112</td>
<td>00:0c:28:09:0c:81</td>
<td>Openfiler</td>
<td>n/a</td>
<td>n/a</td>
<td>online</td>
<td>static</td>
</tr>
</tbody>
</table>
### Status: Interfaces

#### WAN Interface (em0)
- **Status**: up
- **MAC address**: 00:0c:29:45:66:19
- **IPv4 address**: 10.120.23.241
- **Subnet mask IPv4**: 255.255.255.0
- **Gateway IPv4**: 10.120.20.1
- **IPv6 Link Local**: fe80:20c:29ff:fe45:6619
- **ISP DNS servers**: 127.0.0.1, 10.120.20.1
- **MTU**: 1500
- **Media**: 1000baseT (<full-duplex>)
- **In/Out packets**: 137661/90177 (146.21 MB/17.79 MB)
- **In/Out packets (pass)**: 137661/90177 (146.21 MB/17.79 MB)
- **In/Out packets (block)**: 0/0 (0 KB/0 bytes)
- **In/Out errors**: 0/0
- **Collisions**: 0

#### LAN Interface (lan, em0)
- **Status**: up
- **MAC address**: 00:0c:29:45:66:0f
- **IPv4 address**: 192.168.0.107
- **Subnet mask IPv4**: 255.255.255.0
- **IPv6 Link Local**: fe80:20c:29ff:fe45:660f
- **MTU**: 1500
- **Media**: 1000baseT (<full-duplex>)
- **In/Out packets**: 94268/130711 (146.28 MB/164.28 MB)
- **In/Out packets (pass)**: 84528/113071 (146.28 MB/164.28 MB)
- **In/Out packets (block)**: 126/0 (12 KB/0 bytes)
- **In/Out errors**: 0/0
- **Collisions**: 0

#### QVT Interface (萩1, ppt1)
- **Status**: down
pfSense 6 WebGUI Dashboard
Windows Server 2012

Added new User to User Account named AIONS for users who connect to the AIONS network

Added new User to the public Share on the AIONS network labeled S:\

The new User AIONS credentials are;

Username: AIONS
Password: @i0ns

Changed network adapter settings to obtain IP address from PfSense DHCP server

Assigned a static IP address within PfSense for Windows Server 2012 to obtain as 192.168.0.109

Configured the three identical hard drives to run as RAID 5 within Disk Management

Deleted old shared labeled “S”
Created new share labeled “AIONS Share” using RAID 5 configuration
Added Security Onion ISO image to the datastore in ESXi
Installed Security Onion to the created VM using the Security Onion ISO
Ran Security Onion setup within GUI
Configured username and password as;
    Username: aions
    Password: Aions2015
Restarted SO after setup
Ran setup after boot up to configure SO sensors and tools
Assigned static IP address as 192.168.0.111
Assigned Squil username as “aions”
Assigned email address for logging into Snorby as “aions15@gmail.com”
Assigned password “Aions2015”

Enabled ELSA, running a single IDS process per interface, Snort and Bro to monitor the interface, created a Squil server and a Snorby username

IDS alerts can be viewed using Squil, Squert, Snorby, and ELSA

Bro logs can be found in ELSA

Reconfigured network interface with DHCP settings and changed PfSense DHCP leasing settings to statically assigned IP address 192.168.0.111 to Security Onion
### SO 3 Snorby Event Log

<table>
<thead>
<tr>
<th>Sev.</th>
<th>Sensor</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Event Signature</th>
<th>View Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>192.168.0.154</td>
<td>192.168.0.205</td>
<td>ET POLICY Dropbox Client Broadcasting</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>192.168.0.2</td>
<td>192.168.0.113</td>
<td>GPL RPC portmap NFS request TCP</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>192.168.0.154</td>
<td>192.168.0.154</td>
<td>ET POLICY RC EXE or DLL Windows file download</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>192.168.0.154</td>
<td>192.168.0.205</td>
<td>ET POLICY Dropbox Client Broadcasting</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>70.38.0.154</td>
<td>192.168.0.154</td>
<td>ET POLICY Executable and linking tunnel (ELT) file download</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>192.168.0.109</td>
<td>86.46.248.142</td>
<td>ET POLICY Protocol 41 IP-encapsulation potential Telnet IP5 tunnel anomaly</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>192.168.0.109</td>
<td>86.46.248.142</td>
<td>ET POLICY Protocol 41 IP-encapsulation potential Telnet IP5 tunnel anomaly</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>192.168.0.154</td>
<td>50.36.225.173</td>
<td>ET POLICY HTTP Client body contains &quot;per&quot; in checksum</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>23.1.162.225</td>
<td>192.168.0.154</td>
<td>ET SHELLCODE Excessive Use of Hashlib Objects Likely Malicious Malware</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>23.1.162.225</td>
<td>192.168.0.154</td>
<td>ET SHELLCODE Excessive Use of Hashlib Objects Likely Malicious Malware</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>23.1.162.225</td>
<td>192.168.0.154</td>
<td>ET SHELLCODE Excessive Use of Hashlib Objects Likely Malicious Malware</td>
<td>880660915</td>
</tr>
<tr>
<td>5</td>
<td>aion-virtual</td>
<td>23.1.162.225</td>
<td>192.168.0.154</td>
<td>ET SHELLCODE Excessive Use of Hashlib Objects Likely Malicious Malware</td>
<td>880660915</td>
</tr>
</tbody>
</table>
Username: root
Password: Aions2015

Access OpenFiler web based management interface via default username and password (openfiler and password respectively)

Changed administrator password to Aions2015

Relogged into OpenFiler webGUI

Enabled NFS Server under Services tab and started NFS Server

Added IP address to subnet in Network Access Configuration under System tab to give access to storage

Created partition on hard drive for use of file sharing in Block Devices under Volumes tab

Allocated full hard drive spare to partition
Added a Volume group using newly created partition label “share1” using XFS filesystem
Created share labeled “share1” under Shares tab and made share
Created subfolder labeled “aionshare” within newly created share
Enabled desktop_admin as Primary Group in Group access configuration for share
Enabled Read/Write access for network
Wireless Access Point

Connected to the AIONS network physically to access the Wireless Access Point at the address of http://tplinkap.net

Changed the Wireless Access Point’s IP address to a static address of 192.168.0.110

Changed the Wireless Security settings to WPA/WPA2 – Personal and input a password for the network of “C0nn3ct15”.

Appendix B: Weekly Plan

Weekly Plan:

Week 1 January 12: 3210 Rec Center Class begins at 6:00 pm
- Introduction of the team and review of Senior Design I and discussion of the final phase of the project.
- Discuss Gantt Chart
- Deliverables
- Signup Sheet for Pictures
- Schedule for Expo
- Expo Equipment Requirements

Week 2 January 19: UC Offices Closed, Martin Luther King Day.

Group:
- Meet with Carla co-worker for pfSense as well as project usability.
- Finalize Hotspot options, purchase.
- Add feedback/ ideas to project
- Create weekly Plan
- Finalize deliverables
- Create a new Gantt Chart

Week 3 January 26: 3210 Rec Center Class begins at 7:00 pm
- Collecting test data.
- Preparation for presentations on February 9th & 16th
- Final review/discussion of Abstracts
Assignment 1 due: Weekly plan for Spring Semester & Gantt Chart due.
This assignment is your commitment as to what you will deliver this semester as part of your project. You will need to include a separate detailed list of what you plan to accomplish (deliverables) along with milestones listed on the Gantt Chart.

Group:
- Load and Configure Hotspot
- Get the system synced to the new network.
- Speed tests
- User ability testing
- Functionality testing
- Connectivity testing

**Week 4 February 2: 3210 Rec Center 5:00 pm – 7:30 pm**

Pictures will be taken in 3210 Rec Center from 5:00 p.m. till 7:30 p.m.; additional information to follow. These are pictures taken by a professional photographer. Professional dress required; suits and tie for the men and appropriate professional dress for women. You will get copies of your picture at no cost to you.

**Group:**
- Develop presentation
- Record demonstrations
- System configuration tweaks
- Brainstorm poster ideas
- Implementation of Security Onion commences

**Week 5 February 9: 3210 Rec Center Class begins at 7:00 pm**

Presentations, Deliverables only – Networking/Security Track Presentations. Five minute presentation, with a limited number of PowerPoints; show us your deliverables. What have you accomplished based on what you committed last semester? Demonstrate you are prepared for Tech Expo. Presentations will be made in 3210 beginning at 7 p.m. All Students are required to attend. See Schedule.

Assignment 2 due: Testing plan/report due.

**Group:**
- Rewrite Abstract
- Revise Report
- Update Use cases scenarios
- Update network diagram
- Security install

**Week 6 February 16: 3210 Rec Center Class begins at 7:00 pm**

Presentations, Deliverables only – Software Track Presentations. Five minute presentation, with a limited number of PowerPoints; show us your deliverables. What have you accomplished based on what you committed last semester? Demonstrate you are prepared for Tech Expo. Presentations will be made in 3210 beginning at 7 p.m. All Students are required to attend. See Schedule.

Assignment 3 due: Abstract. Must be submitted by this Date – No Exceptions

Abstract is in “Past Tense”. 150 words maximum. You will be able to have more words in your final paper.

Final content is due to the school for the brochure on February 26th. This gives the faculty team (10) days to give you feedback and have you make adjustments/changes.
Group:
- Revise Report
- Begin Poster
- System Testing
- System backup

**Week 7 February 23: 3210 Rec Center Class begins at 7:00 pm**
- Requirements for submitting the final report to the College, Cheryl Ghosh, Senior Associate Librarian.
- Review of writing the final report and preparing your Tech Expo posters.

Group:
- Revise Report
- Finalize rough poster
- Comprehensive Testing
- System backups

**Week 8 March 2: 3210 Rec Center Class begins at 7:00 pm**
- Review of writing the final report and preparing your Tech Expo posters.
- Critique Expo Posters during class.

Group:
- Finalize Draft Report
- Complete Draft Poster
- Final tests/ configurations

**Week 9 March 9: 3210 Rec Center Class begins at 7:00 pm**
- Finalize Senior Project.
Assignment 4 due: Draft Tech Expo poster due.
Assignment 5 due: Draft report due.

Group:
- Finalize/complete poster(s)
- Revise report draft

**Week 10 March 16 (Spring Break)**

Group: TBD

**Week 11 March 23: 3210 Rec Center Class begins at 6:00 pm**
Final Presentations see presentation schedule.
Assignment 6: Final Poster due.
We will submit your posters for printing. You will be responsible for picking them up during the week of March 30th. You will pick them up at the CECH Library – 400 Teachers College (right in the breeze way as you enter the main CECH entrance).
Group:
- Booth setup ideas
- Define content and roles

**Week 12 March 30: 3210 Rec Center Class begins at 6:00 pm**
Final Presentations see presentation schedule.

Group:
- Booth setup ideas
- Revise report draft
- Revise Booth content/roles

**Week 13 April 6: 3210 Rec Center Class begins at 6:00 pm**
Final Presentations see presentation schedule.

Group:
- Finalize booth setup/layout
- System check
- Transportation there and back

**Week 14 April 13, Prepare for Tech Expo (Tuesday April 14)**
No Class this Night. Use the time to prep for setting up for the Expo.

Group: Add feedback to report.
Appendix C: Project Timeline

Below are the Gantt charts our group used throughout the course to monitor our progress and keep track of the deliverables as well as the goals we set for ourselves.

Fall semester 2014

Spring semester 2015
Appendix D: Deliverables

AIONS Deliverables

1. Connectivity
   - Devices able to connect to the device (users seeing the network on tablet, phone, pc, etc.)
   - Access World Wide Web addresses
2. Security
   - Security Onion
     - Intrusion Detections, Sensor monitoring and analyzing
     - Remote monitoring, analyzing, and administration
   - Physical Security
     - Lock & key
       - Prevent device relocation
       - Prevent inner component tampering
   - Mitigating controls
     - Administrative rights
3. Hotspot Configuration
   - ESXi/PfSense recognition and integration
   - Ensure full throughput/bandwidth utilization
4. Storage Configuration
   - Public transfer folder
   - NAS
   - Network backup
5. Use Case Possibilities- Who is going to use it and how
   - Hotel Use Case
     - Local file transfer/sharing
     - Logical diagrams
   - Business Relocation assistance device
     - Remote administration, backups, file transfer/sharing
     - Logical diagrams
   - Research Team (Archaeologist)
     - Remote administration, backups, file transfer/sharing
     - Logical diagrams
6. AIONS Configuration- device itself
   - Motherboard
   - Router
   - Processor
   - Physical storage
   - Wireless access point
   - Switch
   - Remote access (feature enabled or disabled) for support
7. Software Configuration
   - PfSense- to act as a router and firewall
   - TeamViewer/RDC- provide remote access
- Windows server- storage as well as access web GUIs
- Security Onion- monitor network traffic

8. Backups
- Back up of configuration
- Backup aspect for company’s data
- Routine backup of server/network using (backup software here) configurations

Appendix E: Device Functionality Testing

Testing for functionality is key to any product, the following is an analysis of each test case:

Test case #1: Connectivity is the most simple yet most important, without connectivity there is no AIONS. In order to test the connectivity we started with AIONS completely off and multiple wireless capable devices that had yet to connect to the network. We then plugged in and powered on AIONS, waited for the boot process to complete and then attempted to connect the wireless capable devices with success.

Test case #2: Security is also very important in the testing process. Without a sound solution for security on AIONS, we may have a working product, but certainly not a marketable product that companies would consider. In order to test the security on AIONS we tested Security Onion with testmyids.com and PfSense with Hackerwatch.org/probe/.

Test case #3: The hotspot configuration is a key component to the connectivity of AIONS. In order to test the hotspot configuration we plugged the hotspot into a laptop and selected it as the signal source. We then opened an internet browser and attempted to access a webpage. We also ran a speed test at speedtest.net.
**Test case #4:** Shared storage is a large selling point to AIONS. It allows for users connected to the device to create and share documents. In order to test the Storage configuration we accessed AIONS with a wireless device, logged on to the server with the provided AIONS shared storage credentials, created a new folder in the transfer folder, logged in to the server via vSphere and checked for the file in the shared folder.

**Test case #5:** Being able to use AIONS in a remote area is what set AIONS apart from the competition. In order to test that capability we took the device to a remote location, powered it using a generator, booted up the system, connected to the device, and checked for internet connectivity.

**Test case #6:** Infrastructure backup is another marketable selling point for AIONS. In order to test AIONS’ usability as an infrastructure backup we took AIONS to a business location, plugged into a power source, booted up the system, connected to the device, and checked for internet connectivity.

**Test Case #7:** The physical configuration is as important as anything, without the hardware there’s not AIONS at all. Starting from scratch we installed all the components into a build your own computer case, we then ran the necessary network cables and powered AIONS on.
Test Case #8: pfSense’s configuration is an extremely important software component to AIONS, PfSense controls the routing of the wireless traffic among other things. In order to test pfSense we viewed the console window for PfSense VM in ESXi, assigned at least one interface to NIC, assigned IP address to assigned interface, used web browser on computer connected to same network as PfSense VM, input IP address of assigned interface in web browser to access PfSense WebGUI, and logged into PfSense WebGUI to access configuration settings.

Test case #9: ESXI host all of our operating systems for AIONS, so naturally the configuration of ESXI is a major factor in a working AIONS device. In order to test the configuration of ESXI we turned on AIONS to boot up ESXi, hit F2 on keyboard to access settings, input static IP address under Network Management, using another computer, connected to the same network as ESXi installed vSphere Client, used static IP address and input username and password to access ESXi configuration settings.

Test case #10: Backups are important in a business environment no matter what the product. In order to test the backup solution we enabled file logging on Security Onion and create a back-up of all Virtual Machine’s configurations. There is currently no built in back-up solution for ESXi thus we had to ensure to manually create new back-ups of all Virtual Machines if any configuration changes were to made to the Virtual Machine’s hardware and/or software. There is an update for ESXi in the future that will enable a back-up feature.
**Test case #11:** OpenFiler must have the shares clients create available at any time AIONS is powered on unless specifically turned off by the client. Testing for this involved creating a share and powering off the AIONS then powering up AIONS again to ensure availability of the share on the network boot up. We changed WAN networks from our local home based to campus based network to ensure availability of the share on the network was still available upon boot up. We changed WAN interface configuration from Ethernet based to USB based to ensure availability of the share on the network upon boot up. We tested out the availability of the share on both wired and wireless connectivity. Final testing was done by turning off the OpenFiler VM then back on, turning off the share then back on, and finally testing all above with both Windows and Mac based computers. All testing was successful.
Appendix F: Customer Forms

Below are two device specifications forms as well as invoice forms examples for two of the usecases stated about.

[User Requirements Form]

Company Name: Spicefire Group
First name: James  Last name: Jackson  Date: 12/2/15
Address:

(First line) 1410 Race St.
(Second line) ________________________________
(City) Cincinnati  (State) OH  (Zip code) 45202

Contact:
Phone number (Home): 513-***-****
Phone number (Work): 513-445-6795
Email (1): jackson@spicefiregroup.com  Email (2): ______________________

Please answer the following questions to the best of your ability. Your custom unit will be constructed as well as assembled based on your responses to the following criteria questions.

1. Please state your budget? $15,000

2. Number of expected users to connect to AIoNS?
   □ 0-20
   □ 21-100
   □ 101-200
   □ 200+

3. Will existing user accounts and/or groups need to be imported? (Ex. Active Directory)
   ➕ Yes
   □ No

4. Device connectivity?
   □ Wired only
   □ Wireless only (Skip to question 6)
   ➕ Wired and Wireless
5. Number of required ports

- [ ] 1-10
- [ ] 11-25
- [ ] 26-50
- [ ] Other: ___________

6. Will you need shared network storage?

- [ ] Yes (Proceed to question 7)
- [ ] No (skip to question 9)

7. What storage software do you want to use?

- [ ] Microsoft (Licensed per user software)
- [ ] Openfiler (Open source, free)

8. How much storage will you need? 50 TB ______ (GB / TB )

9. Please select the intended device location, and then provide any and all other important information.

- [ ] Controlled Environment (ex. Server room)
- [ ] Remote Location (ex. Outdoors)
- [ ] Other: ___________

Please Explain: __________________________________________

_____________________________________________________

10. Will you need provided technical support for AIONS?

- [ ] Yes
- [ ] No
# AIONS Device Configuration Checklist

**Bill To:** SpiceFire  
**Address:** 1410 Race St.  
Cincinnati, OH 45202

**Phone:** 513-xxx-xxxx  
**Fax:** 513-345-6789  
**Email:** jackson@spicetigroup.com  
**Contact:** James Jackson

**Invoice No.:** 34568  
**Invoice Date:** 2/10/2015  
**Date Due:** 3/12/2015  
**Invoice For:** AIONS Device Configuration

<table>
<thead>
<tr>
<th>DATE</th>
<th>DESCRIPTION</th>
<th>RATE PER HOUR</th>
<th>HOURS</th>
<th>Cost</th>
<th>Quantity</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/2/2015</td>
<td>Build Session</td>
<td>$96.00</td>
<td>80</td>
<td></td>
<td></td>
<td>$2,880.00</td>
</tr>
<tr>
<td>12/2/2015</td>
<td>AIONS Device Hardware</td>
<td></td>
<td></td>
<td>$1,035.00</td>
<td>1</td>
<td>$1,035.00</td>
</tr>
<tr>
<td>12/2/2015</td>
<td>Synology 48TB RackStation 12-Bay ECSI NAS with Drives</td>
<td>$4,762.00</td>
<td>1</td>
<td></td>
<td></td>
<td>$4,762.00</td>
</tr>
<tr>
<td>12/2/2015</td>
<td>Windows Server 2012 R2 Essential Licenses - 25 seats</td>
<td>$501.00</td>
<td>6</td>
<td></td>
<td></td>
<td>$3,066.00</td>
</tr>
<tr>
<td>12/2/2015</td>
<td>Cisco 8811W Wireless Router-4Port Switch Integrated</td>
<td>$465.00</td>
<td>1</td>
<td></td>
<td></td>
<td>$465.00</td>
</tr>
<tr>
<td>12/2/2015</td>
<td>Technical Support - 1 Year</td>
<td>$900.00</td>
<td>2</td>
<td></td>
<td></td>
<td>$1,800.00</td>
</tr>
</tbody>
</table>

**Invoice Subtotal** $14,102.99  
**Deposit Amount** $7,100.00  
**Total** $7,002.99

Make all checks payable to AIONS Device Configuration Checklist.  
Total due within 30 days. Overdue accounts subject to a service charge of 20% per month.
User Requirements Form:

Company Name: Organisms R Us
First Name: James  Last Name: Mendoza  Date: 2/2/15

Address:
- (Street) 567 Walnut Lane
- (City) Nevada  (State) MO  (Zip Code) 08876

Contact:
- Phone number (Home): 432-****-****
- Phone number (Fax): 432-555-0123
- Email (1): janine@cern.com  Email (2): 

Please answer the following questions to the best of your ability. Your custom unit will be constructed as well as assembled based on your responses to the following criteria questions.

1. Please state your budget?  $7,000

2. Number of expected users to connect to AIONS?
   - 0-30
   - 31-100
   - 101-200
   - 200+

3. Will existing user accounts and/or groups need to be imported? (Ex. Active Directory)
   - Yes
   - No

4. Device connectivity?
   - Wired only
   - Wireless only (Skip to question 5)
   - Wired and Wireless

5. Number of required ports
   - 1-10
   - 11-25
   - 26-50
   - Other: ________
6. Will you need shared network storage?
   ☐ Yes (Proceed to question 7)
   ☐ No (skip to question 5)

7. What storage software do you want to use?
   ☐ Microsoft (Licensed per user software)
   ☐ Openfiler (Open source, free)

8. How much storage will you need? 2TB (GB / TB)

9. Please select the intended device location, and then provide any and all other important information.
   ☐ Controlled Environment (ex. Server room)
   ☐ Remote Location (ex. Outdoors)
   ☐ Other __________
   
   Please Explain: Will be located in a research tent
   __________________________
   __________________________

10. Will you need provided technical support for AIONS?
    ☐ Yes
    ☐ No
Appendix G: Build Pictures

A look inside the A.I.O.N.S Device: