802.11n Wireless Technology for the University of Cincinnati

By

Anthony Grismayer
Jason Maloney
Kyle Miller
Kurt Scherer

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

University of Cincinnati
College of Applied Science

May 2008
802.11n Wireless Technology
for the University of Cincinnati

By

Anthony Grismayer
Jason Maloney
Kyle Miller
Kurt Scherer

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

© Copyright 2008 Anthony Grismayer, Jason Maloney, Kyle Miller, Kurt Scherer

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

___________________________________________________  ____________________
Anthony C. Grismayer                                      Date

___________________________________________________  ____________________
Jason M. Maloney                                           Date

___________________________________________________  ____________________
Kyle C. Miller                                             Date

___________________________________________________  ____________________
Kurt S. Scherer                                            Date

___________________________________________________  ____________________
John Nyland, Faculty Advisor                                Date

___________________________________________________  ____________________
Hazem Said, Department Head                                Date
Acknowledgements

We would like to give special thanks to John Nyland, Professor and Academic Advisor for our project. Also deserving of special thanks are Mark Faulkner, Bruce Burton, Diana Noelcke, Brit Royse, and everyone at the University of Cincinnati’s Network Operations Center.

We would like to give special thanks to the vendors: Tim Cornett, Jim Vos, David Munro, and Anjan Srinivas, from Aruba Networks; Ted Franke, John O’Malley, Grant Shackelford, Michael Park, and Robb Vosefski from Cisco Systems.

We would also like to give special thanks to Bill Weed, Information Technology Analyst. We are grateful that we were able to use the resources provided by the College of Applied Science computer labs. Finally, we would like to thank GBBN Architects for allowing us to use their FTP site as a digital repository for all of our electronic documents.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>i</td>
</tr>
<tr>
<td>List of Figures</td>
<td>v</td>
</tr>
<tr>
<td>Abstract</td>
<td>vi</td>
</tr>
<tr>
<td>1. Statement of the Problem</td>
<td>1</td>
</tr>
<tr>
<td>2. Description of the Solution</td>
<td>2</td>
</tr>
<tr>
<td>2.1 User Profiles</td>
<td>3</td>
</tr>
<tr>
<td>2.1.1 UCit</td>
<td>3</td>
</tr>
<tr>
<td>2.1.2 Future Networking Students</td>
<td>3</td>
</tr>
<tr>
<td>2.1.3 Mark Faulkner</td>
<td>4</td>
</tr>
<tr>
<td>2.2 Design Protocols</td>
<td>4</td>
</tr>
<tr>
<td>2.2.1 Scorecard</td>
<td>4</td>
</tr>
<tr>
<td>2.2.2 Verification Process of the Models</td>
<td>8</td>
</tr>
<tr>
<td>3. Project Objectives</td>
<td>8</td>
</tr>
<tr>
<td>3.1 Conduct Site Surveys</td>
<td>8</td>
</tr>
<tr>
<td>3.1.1 Buildings Currently with no Wireless Coverage</td>
<td>8</td>
</tr>
<tr>
<td>3.1.2 Buildings Not Conducive to Wireless Coverage</td>
<td>9</td>
</tr>
<tr>
<td>3.1.3 Buildings Very Conducive to Wireless Coverage</td>
<td>9</td>
</tr>
<tr>
<td>3.2 OPNET Models</td>
<td>9</td>
</tr>
<tr>
<td>3.2.1 CAS Model</td>
<td>9</td>
</tr>
<tr>
<td>3.2.2 UC Core Models</td>
<td>9</td>
</tr>
<tr>
<td>3.3 Scorecard Analysis</td>
<td>10</td>
</tr>
<tr>
<td>4. Design and Development</td>
<td>10</td>
</tr>
<tr>
<td>4.1 Timeline and Accomplishments</td>
<td>10</td>
</tr>
<tr>
<td>4.1.1 Senior Design I</td>
<td>10</td>
</tr>
<tr>
<td>4.1.2 Senior Design II</td>
<td>10</td>
</tr>
<tr>
<td>4.1.3 Senior Design III</td>
<td>11</td>
</tr>
<tr>
<td>4.2 Project Budget</td>
<td>11</td>
</tr>
<tr>
<td>4.3 Software</td>
<td>12</td>
</tr>
</tbody>
</table>
8. References..........................................................................................................................147
List of Figures

Figure 1 - Project Budget................................................................. 12
Figure 2 - Sample Heatmap ............................................................ 13
Figure 3 - Low-level Model............................................................ 14
Figure 4 - Low-level Abstract Model .............................................. 15
Figure 5 - Mid-level Abstract Model .............................................. 16
Figure 6 - High-level Abstract Model ............................................. 17
Figure 7 - CAS OPNET Model......................................................... 18
Figure 8 - OPNET Subnet Detail ..................................................... 19
Figure 9 - Vendor Scorecard ........................................................... 20
Figure 10 - Aruba Equipment Testing Setup ..................................... 23
Figure 11 – Aruba AP Scorecard ..................................................... 24
Figure 12 - Aruba Controller Scorecard .......................................... 25
Figure 13 - Aruba AP125 Hardware Features ................................... 26
Figure 14 - Cisco Clean Access Setup ............................................. 41
Figure 15 - Cisco Equipment Test Setup ......................................... 66
Figure 16 - Cisco AP Scorecard Evaluation ..................................... 67
Figure 17 - Cisco Controller Scorecard Evaluation ........................... 68
Figure 18 - Cisco Support Pricing ................................................... 80
Figure 19 - Meru AP 300 ................................................................. 95
Figure 20 - Meru AP 300 (back) ....................................................... 95
Figure 21 - Meru Equipment Testing Setup ....................................... 96
Figure 22 - Basic Grand Total Chart ................................................. 121
Figure 23 - % Weight Grand Total Chart ......................................... 122
Figure 24 - Cisco Road Map Total ................................................... 123
Figure 25 - Iperf Testing Setup ....................................................... 124
Figure 26 - Cisco Systems Test 1 - TCP ........................................... 127
Figure 27 - Cisco Test 2 Results Graph ........................................... 127
Figure 28 - Aruba Test 1 Results Graph .......................................... 128
Figure 29 - Aruba Test 2 Results Graph .......................................... 128
Abstract

Senior Administration at the University of Cincinnati (UC) have set a goal to provide 100% wireless coverage campus-wide using the most advanced technologies currently available. Administration in the University of Cincinnati Information Technology support group (UCit) has included wireless internet connectivity in the strategic growth plan since 2000. The goal of this paper is to determine the feasibility of utilizing 802.11n technologies to meet the University’s goal. To answer this question, a model of the University computer network system was built using the OPNET environment to study particular use-case scenarios and the implications of traffic aggregation resulting from the new wireless capabilities. Three vendors were then compared and their equipment analyzed using a balanced-scorecard methodology. The selected vendor’s equipment was then included in the model for a final analysis and recommendation.
802.11n Wireless Technology for the University of Cincinnati

1. Statement of the Problem

The University of Cincinnati has included wireless internet connectivity in its strategic growth plan since 2000. The wireless infrastructure provides students and faculty with the freedom to access university resources and the Internet in various locations throughout the campus. Currently, 50% of the Uptown UC Campus offers a wireless connection, with close to 700 access points. With the decline in price of current technology, as well as new technologies being developed, UCit wants to provide 100% campus coverage and remain up-to-date with the latest wireless technology. UCit currently does not have a model of the wireless network infrastructure. This model is needed in order to evaluate the current infrastructure and also to allow planning for future wireless network expansions. The model will allow for simulations of the current wireless network and provide an avenue for UCit to test for and discover potential problems that may arise.

UCit would like to determine what it would take to achieve 100% wireless campus coverage, as well as the feasibility of implementing the new 802.11n technology. With this knowledge, UCit can then begin planning an upgrade of the current infrastructure to support future network technologies. An up-to-date and accurate model of the current infrastructure will be invaluable to UCit. It will allow virtual testing of any proposed future network deployments, which will allow for better planning and a smoother implementation process.

These needs required our project to evaluate the leading wireless networking vendors and to conduct site surveys of the University of Cincinnati’s campus. After these investigations, a well-researched proposal was presented to UCit, as well as an accurate working model of the current network infrastructure. From that point, UCit will be able to make an educated decision
on the feasibility of achieving 100% wireless campus coverage utilizing the new 802.11n wireless standard.

2. Description of the Solution

The possible solutions for wireless coverage of the University of Cincinnati’s Uptown campus are as follows (3):

- Keep the current 50% wireless coverage with the existing 802.11g infrastructure.
- Replace the current 802.11g infrastructure with 802.11n equipment and continue to provide only 50% wireless coverage.
- Replace the current 802.11g infrastructure with 802.11n equipment and expand the wireless coverage to 100%.

The first option represents the current wireless infrastructure which is already implemented across the University of Cincinnati’s campus. This option would result in no changes in equipment or wireless coverage and was provided simply as a comparative baseline against other two options. The model maps the existing infrastructure of the network.

The second option involves the complete replacement of the current 802.11g equipment with the emerging 802.11n hardware, while maintaining the 50% wireless coverage across the University of Cincinnati’s campus. This model utilizes the optimal placement of the access points based on site surveys, equipment evaluations, and industry recommendations. The model also includes heatmaps of the resulting wireless coverage in the surveyed buildings. Any changes to the supporting infrastructure have been included within this model and performance analyses were run against the model. Aruba and Cisco have provided a financial estimate to cover this rollout.

The final option represents the complete replacement of the 802.11g equipment and expanding the wireless coverage on the University of Cincinnati’s campus to 100% with the
emerging 802.11n equipment. The 802.11n equipment will operate in a backwards compatibility mode, to allow legacy 802.11b/g clients the ability to connect (2). The model includes the optimal placement of the access points based on site surveys, equipment evaluation, and industry recommendations. Changes to the supporting infrastructure are included in this model and performance analyses have been run against the model. Aruba and Cisco have also provided a financial estimate to cover this rollout.

2.1 User Profiles

The user profiles of this project are different for each half of the project. The OPNET portion of the project will be used by UCit and future networking students. The vendor business analysis portion of the project will be utilized primarily by Mark Faulkner and his team. The business analysis will produce a scorecard that will compare all vendors across a series of weighted criteria, per the standard decision-making process used by UCit.

2.1.1 UCit

UCit will be able to run various testing simulations against the completed OPNET models. Given the versatility of OPNET, it will prove to be extremely beneficial to planning future implementation efforts of UCit. Additionally, UCit will utilize our final proposal to make an educated decision on the future of the University’s wireless network with regard to the new 802.11n standard.

2.1.2 Future Networking Students

In much the same manner that previous OPNET models were built upon to create the final model of this project, future students will be able to build upon this project. This model will provide a working example of the capabilities of OPNET and could potentially be used in various networking classes at the College of Applied Science.
2.1.3 Mark Faulkner

Mark Faulkner (Assistant Vice President, Network & Telcom, UCit) and his team will evaluate the vendor business analysis and final recommendation provided by the project team. The vendor business analysis will be a key component of the decision process in terms of which direction the University of Cincinnati should pursue with regard to the upgrade of the wireless infrastructure.

2.2 Design Protocols

2.2.1 Scorecard

The vendor business analysis portion of the project is accomplished through the use of a scorecard to evaluate the offerings of the chosen 802.11n equipment against the requirements of UCit. The scorecard is a matrix which was developed through collaboration with UCit and is based on UCit’s traditional equipment evaluation procedure (1, 3, 5). The scorecard evaluates the hardware and security features, compatibility, the costs and overall value of the equipment. UCit’s methodology is conducted through stages which evaluate and eventually eliminate vendors. The first stage of the evaluation process focuses on the hardware, security, and compatibility of the vendor solution. Vendors which satisfy the first round of requirements are then moved the second round which looks at the equipment costs and value of each vendor’s solution followed by further market research and evaluations. The outcome of this procedure will determine whether UCit will pursue the project or not.

For this project we will expand the existing UCit model of evaluation. The scorecard will be broken up into three sections. The first two sections focus on the display of the evaluation findings, while the third section is aimed at analyzing the findings and determining the final
recommendation. The first section of the scorecard analysis provides an overview of each vendor’s performance against the scorecard in a straightforward pass or fail format.

The scorecard items which were developed through collaboration with UCit are:

- **Access Points:**

  - **Hardware/Performance Features**
    - Gigabit Interfaces (Weight: 9)
    - IPv6 Native to Hardware (Weight: 1)
    - Outdoor Capable AP (Weight: 5)
    - PoE – 802.3af (Weight: 7)
    - Power Requirement (Weight: n/a)
    - Quality of Service Capability (Weight: 9)
    - VoFI Support (Weight: 9)
    - MIMO Mode Capability (Weight: n/a)
    - Frequencies (Weight: n/a)
    - Multiple SSIDs (Weight: 9)
    - Coverage Ratio (Weight: n/a)
    - Mesh Capabilities (Weight: 5)
    - Performance Dovetail (Weight: 9)
    - 802.11i Encryption (Weight: 9)

- **Access Point Controllers:**

  - **Hardware/Performance Features**
    - Controller can Manage Mesh Networks (Weight: 5)

  - **Security Features**
- ARP Poisoning Prevention (Weight: 9)
- IP Spoofing Prevention (Weight: 9)
- Broadcast Storm Control (Weight: 9)
- ACL Support (Weight: 5)
- SNMPv3 (Weight: 9)
- TACACS+ Support (Weight: 9)
- Support SSH Connections (Weight: 9)
- Wireless IDS/IPS (Weight: 9)

- **Compatibility:**
  - Clean Access Compatible (Weight: 9)
  - 802.11b/g Compatible (Weight: 9)
  - Compatible with Existing Infrastructure (Weight: 9)
  - Non-PC WIFI Capable Devices (Weight: 9)

- **Value/Cost Features:**
  - 5 Year Life Cycle/Support (Weight: 9)
  - Free Transition to 802.11n Ratified Version/Model (Weight: n/a)
  - Reference Sites of Equivalent Size (Weight: n/a)
  - Warranty (Weight: n/a)
  - Vendor Installation Support (Weight: n/a)
  - Upgrade Controller to Support 802.11n? (Weight: n/a)
  - Cost to Replace Existing (Weight: n/a)
  - Cost for 100% Coverage (Weight: n/a)
  - Maintenance Cost (Weight: n/a)
The second section expands upon the first section and provides a detailed breakdown of each element on the scorecard. The format of the second section is:

- **Scorecard Item Name**: Indicates scorecard criterion.
- **Criteria Explanation**: Detailed explanation of the criterion and what is desired.
- **Weighted Value**: Assigned weight to the scorecard criterion by UCit.
- **Vendor Analysis**: Description of how the vendor performed for the criterion.
- **Final Rating**: Pass or Fail the evaluation for the criterion.
- **Appendix Reference**: Referenced items from the appendix of screen captures.
- **Manual Reference**: Referenced items from vendor documentation.

The third section is a complete business analysis of the findings conducted through the statistical analysis of each vendor’s performance and the weight of each criterion. The end result of this analysis will produce a decision model which scores the performance of each vendor and rates them accordingly. In preparation for this section, each scorecard criterion was assigned a weight (indicated above next to scorecard items – the possible values, listed from lowest to highest, are 1, 5, 7, and 9) and each section of the scorecard was assigned a priority weight (measured as a percentage).

The priority weights for the scorecard sections are:

- **Access Points**: 25%
- **Access Point Controllers**: 25%
- **Compatibility**: 50%
- **Value/Cost Features**: 0%
2.2.2 Verification Process of the Models

In this project we have two major models: heatmaps and the OPNET models. We created the heatmap models by performing site surveys of various buildings around campus. These surveys gave us the ranges for a given vendor’s access point and obtained an average in which to create the heatmaps. Using a Visio drawing of the campus infrastructure, we built OPNET models that mirror that infrastructure. We have a high-level model which summarizes the main nodes, as well as a model that allows us to drill down into various buildings. Using these models, we are able to simulate various scenarios and their affect on the University’s infrastructure.

3. Project Objectives

In order to solve the defined problems for our project, the following deliverables were set and presented upon project completion. Our deliverables were presented to multiple parties including: UCit, our Senior Design class, the attendees and judges of Tech Expo, and the wireless vendors we worked with throughout the duration of the project.

3.1 Conduct Site Surveys

Throughout the process of conducting site surveys, the project team was able to provide RF heatmaps for all buildings surveyed. For the feasibility of the project, we defined three building areas of the University of Cincinnati which provided the appropriate amount of information to allow the project team to extrapolate wireless needs for the remainder of the campus buildings which could not be surveyed. The buildings that were surveyed in this project are defined as follows:

3.1.1 Buildings Currently With No Wireless Coverage:

- Daniels Hall
- Calhoun Hall
3.1.2 Buildings Not Conducive to Wireless Coverage:

- Medical Services Building
- College of Law Building
- Crosley Tower
- Rieveschl Hall
- College of Applied Science Buildings
  - Administration Building
  - Science Building
  - Auditorium Building
  - North Lab Building

3.1.3 Buildings Very Conducive to Wireless Coverage:

- Baldwin Hall
- Engineering Research Center
- University Pavilion
- University Hall

3.2 OPNET Models

3.2.1 CAS Model

The OCAS model was created by a previous Senior Design project. We have added on to this model, and incorporated it into our full model of the University’s infrastructure.

3.2.2 UC Core Models

The core model provides an all encompassing view of major nodes of the University’s network.
3.3 Scorecard Analysis

The scorecard analysis consisted of two components: a technical analysis and a business analysis. The technical analysis encompassed running the hardware through various technical scenarios and tests. The business analysis was determined and documented through the scorecard that was developed between the project team and UCit for the purposes of this project. The business analysis included a criterion weighting system and a statistical analysis in which a vendor was selected that best matched the needs that UCit has set.

4. Design and Development

4.1 Timeline and Accomplishments

4.1.1 Senior Design I

- Meetings with UCit
- Meetings with Vendors
- Defined overall project schedule
- Initial Scorecard
- Proposal

4.1.2 Senior Design II

- Received equipment from vendors
- Equipment configuration
- Created testing plan
- Outlined site survey protocols
- Follow up meetings with vendors
- Provided project abstract to OPNET
- Design freeze document/presentation
4.1.3 Senior Design III

- Finished site surveys
- Finished OPNET models
- Completed vendor evaluation documents
- Completed vendor scorecard
- Composed recommendation to UCit
- Presentation to UCit
- Final Document for SD
- Final Presentation for SD
- Tech Expo

4.2 Project Budget

The project budget (Figure 2) presents all of the materials used to accomplish all of the goals of our project. The total real-world cost of the project is $353,159.80. Due to the fact that this is a project for the University; most of our materials are already purchased and on loan by UCit. An academic version of our network modeling software will be obtained for free, which brings the actual total cost of the project to $1,200.00.
Figure 1 - Project Budget

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Real-World Cost</th>
<th>Project Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPNET</td>
<td>Network Modeling Software</td>
<td>$65,000.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>1 Modeling Server (OPNET)</td>
<td>Modeling Servers</td>
<td>$5,000.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>2 Laptops</td>
<td>Site Surveys</td>
<td>$2,000.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Meru Equipment</td>
<td>Vendor provided equipment</td>
<td>$40,000.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Aruba Equipment</td>
<td>Vendor provided equipment</td>
<td>$112,802.80</td>
<td>$0.00</td>
</tr>
<tr>
<td>Cisco Equipment</td>
<td>Vendor provided equipment</td>
<td>$126,157.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Dual-Band Wireless Laptop Cards (N Compatible)</td>
<td>Hardware</td>
<td>$200.00</td>
<td>$200.00</td>
</tr>
<tr>
<td>University Grant</td>
<td>OPNET</td>
<td>$1,000.00</td>
<td>$1,000.00</td>
</tr>
<tr>
<td>Total Cost</td>
<td></td>
<td>$353,159.80</td>
<td>$1,200.00</td>
</tr>
</tbody>
</table>

4.3 Software

- **OPNET Modeler Wireless Suite**
  - The OPNET suite will be used to model the OCAS Network and the core UC network.
- **Netstumbler Wireless Scanning Software**
- **Microsoft Office Suite**
- **Iperf Testing Software**

4.4 Hardware

4.4.1 General

- **Modeling Server**
  - This is the server that will be used to model and generate data for the OPNET data.
- **Two laptops**
  - These laptops will be used to conduct site surveys across campus.

4.4.2 Meru Networks Hardware

- **Meru Controller**
- **Meru Access Point**
4.4.3 Aruba Networks Hardware

- Aruba Controller
- Aruba Access Point

4.4.4 Cisco Systems Hardware

- Cisco Controller
- Cisco Access Point

5. Proof of Design

5.1 Select Site Surveys and Heatmaps

![Figure 2 - Sample Heatmap](image)

5.2 OPNET Models

5.2.1 Low-level Model

This is the lowest level of the UC’s network. This was generated by information given to us by UCit. The core infrastructure is in the middle of the model while the distribution is at the top of the model. The distribution is comprised of various subnets, which are generally for different buildings on UC’s campus, each of these subnets contain a varying amount of switch stacks. The amount of switch stacks in each subnet was given to us by UCit so that we
could generate an accurate model of the network. Each switch stack contains 4 switches, which support up to 192 users for each switch stack. The LAN objects are 100base-T networks to the switch stacks. The connections from the switch stacks to the distribution are 1 Gigbit. The connections between the distribution to the core infrastructure is 2 Gigbit. All of the connections within the core are 4 Gigbit.

![Image of network model]

**Figure 3 - Low-level Model**

### 5.2.2 Low-level Abstract Model

This model shows the first level of abstraction we created. The core infrastructure was not changed for this abstraction. The distribution was abstracted in such a way that each of the major subnets were created into LAN objects. Each LAN objects number of workstations was determined by multiplying how many switch stacks are contained in each major subnet by 192. This provides us with how many possible available switch ports are contained in each major subnet. This gave us the ability to narrow down where bottle necks could possibly be within the
network. Also due to the limitations of the academic version of OPNET we used, no device can have more than 20 connections.

![Diagram](image)

**Figure 4 - Low-level Abstract Model**

### 5.2.3 Mid-level Abstract Model

This is the second level of abstraction we created. The core infrastructure remains the same as the previous models. The distribution was abstracted to having all of the LAN objects in the previous models combined into single LAN objects. The number of workstations in the LAN objects was determined by adding all of major subnets together. This level of abstraction was created due to the fact that there is still a limitation on how many devices can be connected at any time. Also, creating abstractions show the hierarchical aggregation of traffic, by limiting the amount of connections and actual objects in the model we are able to view the results with better accuracy as to what is specifically happening on the total network.
5.2.4 High-level Abstract Model

This is the final level of abstraction for the model of UC’s network. Since all of the connections within the core infrastructure is the same we can abstract out of the infrastructure what servers and services we would need to evaluate. The WCS and ACS are running an application called Authentication, which is a custom application that was created to simulate the traffic generated by wireless authentication. The next two servers are MSB Core Services 1 and MSB Core Services 2, which host various other applications which are hosted by the university to simulate the email, websites, etc. The Internet Sites and Services server is running external services to simulate websites and email services not hosted by the university. The distribution
was condensed again into a single LAN object for UC Main Campus Network, which contains all the distribution level objects for East and West Campus. There is another object for the College of Applied Science due to the fact the CAS uses a LAN Advantage to connect to the university’s core.

![High-level Abstract Model](image)

**Figure 6 - High-level Abstract Model**

### 5.2.5 College of Applied Science Model

The model of the College of Applied Science was provided from a previous senior design project (Figure 7). However, we needed to alter it for our needs and update some of the buildings.
We needed to add the North Lab and Auditoriums to the previous model. Each building is represented by a pink rectangle, and each floor has a subnet which contains a switch stack.

![Figure 7 - CAS OPNET Model](image)

Inside these subnets we show if there are any access points that should be placed on these subnets and if there are an approximate number of wireless laptops that would be connected to it at any given time. The diagram for the Auditorium is shown along with the diagram of the spell out floors of the Administration building. (Figure 8)
Figure 8 - OPNET Subnet Detail
5.3 Scorecard Evaluation

<table>
<thead>
<tr>
<th>802.11n Requirements</th>
<th>AP</th>
<th>Meru Networks</th>
<th>Aruba Networks</th>
<th>Cisco Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware/Performance Features</strong></td>
<td></td>
<td></td>
<td></td>
<td>25%</td>
</tr>
<tr>
<td>Gigabit Interfaces</td>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IPv6 Native to Hardware</td>
<td>1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Outdoor Capable AP</td>
<td>6</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Poe - 802.3af</td>
<td>7</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Power Requirement</td>
<td>Not Weighted</td>
<td>802.3af</td>
<td>802.3af</td>
<td>802.3af</td>
</tr>
<tr>
<td>Quality of Service Capability</td>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>VoFI Support</td>
<td>5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MIMO Mode Capability</td>
<td>Not Weighted</td>
<td>2x2</td>
<td>2x3</td>
<td>2x3</td>
</tr>
<tr>
<td>Frequencies</td>
<td>Not Weighted</td>
<td>FCC Compliant</td>
<td>FCC Compliant</td>
<td>FCC Compliant</td>
</tr>
<tr>
<td>Multiple SSIDs</td>
<td>5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Coverage Ratio</td>
<td>Not Weighted</td>
<td>10</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Mesh Capabilities</td>
<td>5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Performance Downtail</td>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>802.11i Encryption</td>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Compatibility</strong></td>
<td></td>
<td></td>
<td></td>
<td>50%</td>
</tr>
<tr>
<td>Clean Access compatible</td>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>802.11b/g compatible</td>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Compatible with existing infrastructure</td>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Non-pc with capable devices</td>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Value/Cost Feature</strong></td>
<td></td>
<td></td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td>5 year life cycle/Support</td>
<td>9</td>
<td>TBD</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Free transition to 802.11n ratified version/model</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reference sites of equivalent size</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Warranty</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>Standard</td>
<td>Standard</td>
</tr>
<tr>
<td>Vendor Installation Support</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Upgrade Controller to Support 802.11n</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cost: To replace existing</td>
<td>Not Weighted</td>
<td>TBD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost for 100% coverage</td>
<td>Not Weighted</td>
<td>TBD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintenance Cost</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>Standard</td>
<td>Standard</td>
</tr>
<tr>
<td>Product Lifecycle</td>
<td>Not Weighted</td>
<td>TBD</td>
<td>Early</td>
<td>Early</td>
</tr>
</tbody>
</table>

Figure 9 - Vendor Scorecard

5.3.1 Aruba Networks Evaluation

Aruba Networks Configuration

and Evaluation
Basic Setup Information

Controller Model: Aruba 6000 Chassis with M3 Controller

Access Point Model: Aruba AP125

Controller: 10.160.3.10 /24 (vlan 438)
10.160.3.11 /24 (loopback)

Gateway: 10.160.3.1

DNS Entries:
- aruba-master.uc.edu
- aruba-master.ucuc.edu
- aruba-master.cas-wireless2.cas.uc.edu
- aruba-master.riev.uc.edu
- aruba-master.upav.uc.edu

VLANs:
- 10.160.3.0 /24 vtag 438
- 10.160.4.0 /24 vtag 573
- 10.160.5.0 /24 vtag 573
Switch VLAN Port Mapping:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[438]</td>
<td>[438]</td>
<td>[438]</td>
<td>[573]</td>
<td>[573]</td>
<td>[573]</td>
<td>[573]</td>
<td>[572]</td>
<td>[572]</td>
<td>[572]</td>
<td>[TR]</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>[438]</th>
<th>[438]</th>
<th>[438]</th>
<th>[573]</th>
<th>[573]</th>
<th>[573]</th>
<th>[573]</th>
<th>[572]</th>
<th>[572]</th>
<th>[TR]</th>
<th>[TR]</th>
<th>[TR]</th>
<th>[TR]</th>
<th>[TR]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[2]</td>
<td>[4]</td>
<td>[6]</td>
<td>[8]</td>
<td>[10]</td>
<td>[12]</td>
<td>[14]</td>
<td>[16]</td>
<td>[18]</td>
<td>[20]</td>
<td>[22]</td>
<td>[24]</td>
<td>[438]</td>
<td>[438]</td>
</tr>
</tbody>
</table>

Radius:

IP: 10.25.5.247
Pass: caswap
Ports: 1645/1646

VoIP Clients:

Aunju (sip server) – now brekeke (60 day trial)
Sjphone (softphone)
Microsoft Netmeeting
Skype

Throughput Testing Software:

IPERF, IxChariot
Network Setup Diagram:

Aruba Equipment Testing Setup

Figure 10 - Aruba Equipment Testing Setup

Equipment Configurations:
Scorecard Evaluation – Access Point

<table>
<thead>
<tr>
<th>802.11n Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
</tr>
<tr>
<td><strong>Hardware/Performance Features</strong></td>
</tr>
<tr>
<td>Gigabit Interfaces</td>
</tr>
<tr>
<td>IPv6 Native to Hardware</td>
</tr>
<tr>
<td>Outdoor Capable AP</td>
</tr>
<tr>
<td>PoE - 802.3af</td>
</tr>
<tr>
<td>Power Requirement</td>
</tr>
<tr>
<td>Quality of Service Capability</td>
</tr>
<tr>
<td>VoFi Support</td>
</tr>
<tr>
<td>MIMO Mode Capability</td>
</tr>
<tr>
<td>Frequencies</td>
</tr>
<tr>
<td>Multiple SSIDs</td>
</tr>
<tr>
<td>Coverage Ratio</td>
</tr>
<tr>
<td>Mesh Capabilities</td>
</tr>
<tr>
<td>Performance Dovetail</td>
</tr>
<tr>
<td>802.11i Encryption</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean Access compatible</td>
</tr>
<tr>
<td>802.11b/g compatible</td>
</tr>
<tr>
<td>Compatible with existing infrastructure</td>
</tr>
<tr>
<td>Non-pc wifi capable devices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value/Cost Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 year life cycle/Support</td>
</tr>
<tr>
<td>Free transition to 802.11n ratified version/model</td>
</tr>
<tr>
<td>Reference sites of equivalent size</td>
</tr>
<tr>
<td>Warranty</td>
</tr>
<tr>
<td>Vendor Installation Support</td>
</tr>
<tr>
<td>Upgrade Controller to Support 802.11n</td>
</tr>
<tr>
<td>Cost to replace existing</td>
</tr>
<tr>
<td>Cost for 100% coverage</td>
</tr>
<tr>
<td>Maintenance Cost</td>
</tr>
<tr>
<td>Product Lifecycle</td>
</tr>
</tbody>
</table>

Figure 11 – Aruba AP Scorecard
Scorecard Evaluation – Controller

<table>
<thead>
<tr>
<th>802.11n Requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Controllers</td>
<td></td>
</tr>
<tr>
<td><strong>Hardware/Performance Features</strong></td>
<td></td>
</tr>
<tr>
<td>Controller can manage Mesh Networks</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Security Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Poisoning Prevention</td>
<td>✓</td>
</tr>
<tr>
<td>IP Spoofing Prevention</td>
<td>✓</td>
</tr>
<tr>
<td>Broadcast Storm control</td>
<td>✓</td>
</tr>
<tr>
<td>ACL support</td>
<td>✓</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>✓</td>
</tr>
<tr>
<td>Works over CAT-5 or better cabling</td>
<td>✓</td>
</tr>
<tr>
<td>TACACS + Support</td>
<td>✓</td>
</tr>
<tr>
<td>Support SSH Connections</td>
<td>✓</td>
</tr>
<tr>
<td>Wireless IDS/IPS</td>
<td>✓</td>
</tr>
</tbody>
</table>

Figure 12 - Aruba Controller Scorecard
Scorecard Detailed Analysis – Access Point

Hardware/Performance Features

![Aruba AP125 Hardware Features](image)

**Gigabit Interfaces**

**Criteria Explanation:** This criterion denotes that the vendor’s access point is capable of connecting at 1000 mbps to an edge gigabit capable switch. To test this, UCit has provided us with a Cisco 3750-G switch, which is capable of gigabit connection speeds on all switch ports.

The access point is connected to the switch, and once the two devices have auto-negotiated the link speed, the results are verified on the switch. Since UCit has no desire at this time to upgrade their edge infrastructure, this test is purely for future capabilities.

**Weighted Value:** 9
Vendor Analysis: The Aruba AP125 access points are capable of both connecting at speeds of 100mbps and 1000mbps. Additionally, the AP125 LED indicators will indicate the link speed the AP is connected at by changing the color of the ENET0 LED. If the access point is connected at 100mbps, the LED will flash an “amber” color, and if the access point is connected at 1000mbps, the LED will flash a “green” color.

Vendor Response: “The AP-124/125 access points provide dual gigabit Ethernet interfaces - 10/100/1000Base-T Ethernet (RJ45), Auto-sensing link speed and MDI/MDX – with 802.3af / 802.3at / POE+ support and ensuring AP redundancy / high availability. (2)”

Final Rating: Pass

IPv6 Native to Hardware

Criteria Explanation: This criterion denotes the ability for both the access point hardware as well as the controller hardware to operate with an IPv6 addressing scheme. Since UCit has no desire at this time to switch to an IPv6 addressing scheme, this test is purely for future capabilities.

Weighted Value: 1

Vendor Analysis: The Aruba controller/access point has the functionality to support IPv6 enabled clients. Additionally, the controller can support IPv6 clients through their hardware firewall. Since IPv6 is not a mainstream technology in industry yet, to configure the wireless controller and access points to utilize IPv6, it has to be done through the CLI.
Vendor Response: “Initial support for IPv6 is included with the latest ArubaOS version 3.3.x. With this OS release, support for wired and wireless clients using IPv6 addressing is provided with services such as firewall functionality, layer-2 authentication, and identity-based security. (2)"

Final Rating: Pass

Appendix References: Appendix A: Figure 2; ArubaOS3_3_1UG, Chapter 21 “IPv6 Client Support”

Outdoor Capable AP

Criteria Explanation: This criterion denotes whether or not the mentioned vendor has a 802.11n access point that is capable of existing outdoors to support green space at the University of Cincinnati.

Weighted Value: 5

Vendor Analysis: Currently, Aruba currently does not have an 802.11n capable access point due to the 802.11n standard still being developed. Aruba currently offers outdoor enclosures that can be placed around 802.11n access points that are going to be utilized for green space support. Additionally, external antennae’s can be utilized to support outdoor green space in the event that the access point itself cannot be placed outdoors.

Vendor Response: “The Aruba AP-124/125 access points are UL 2043 plenum rated and can be installed both in user space as well as above tile for a stealth installation. For outdoor deployments, a NEMA enclosure with the proper environmental controls would be required. Optionally, an AP-124 could be mounted on the building interior with cables passed through to externally-mounted outdoor rated antennas. (2)”
Final Rating: Conditional Pass

PoE 802.3af

Criteria Explanation: This criterion denotes the ability of the access point to operate on the PoE standard 802.3af, which is the standard power over Ethernet. To test this, we will be connecting the access point to both the 3750-G switch, which UCit provided, and connecting the access point to the edge infrastructure already in place at the University.

Weighted Value: 7

Vendor Analysis: The Aruba AP125 access point is capable of being powered on 802.3af PoE. It was able to receive power from both the 3750-G switch as well as the currently deployed switches on the edge at the university. However, the Aruba access point cannot be powered in full 3x3 MIMO mode, but can powered in 2x3 MIMO mode, which means that there are two transmitting antennas and three receiving antennas.

Vendor Response: “Aruba AP-124/125 models use intelligent power management to automatically adjust radio operation to support available Power over Ethernet (POE 802.3af, 802.3at, and PoE+) current. This feature allows the university’s existing PoE infrastructure to be used for dual-radio 802.11 a/n and 802.11 b/g/n operation without requiring one of the radios to be turned off or uninstalled and without requiring special PoE injectors; intelligent power design within the AP-120 family of APs allows for the MIMO streams to be enabled or disabled based on available power level from the closet switch. If and when PoE infrastructure is upgraded, additional MIMO streams will be brought on line until full potential performance is achieved. Due to the use of hardware acceleration, even operating with existing lower current PoE injectors, the AP 120 family offers higher throughout than fully powered 802.11n access points
from other suppliers. This intelligent management feature is in direct contrast to our competitor’s 802.11n access points which require nothing less than full power in order to function” (2).

**Final Rating:** Pass

---

**Power Requirement**

**Criteria Explanation:** This criterion denotes the actual power requirement to power an individual access point, with the vendor’s recommendation as to power it with standard 802.3af or with 802.3at.

**Weighted Value:** Not Weighted

**Vendor Analysis:** Aruba fully recommends deploying the AP125 802.11n access point with an 802.3at power capable edge network to provide full functionality in 3x3 MIMO mode. However, since the University of Cincinnati does not wish at this time to upgrade its edge infrastructure to support the 802.3at power requirement, the access point can operate in 2x3 MIMO mode off of 802.3af power.

**Vendor Response:** “Aruba 11n APs are unique within the industry in that they can be powered using standard 802.3af POE switches and/or power injectors avoiding the need for costly POE upgrades. The Aruba APs may be powered through Power-over-Ethernet (PoE) or local power may be used. The AP-124 and AP-125 Access Points can operate in full 3x3 MIMO mode using a single 802.3af PoE injector. Even with less-capable switches, Aruba AP-124/125 can still provide 2x3. (2)”

The AP-124/125 power requirements are as follows:

- **Power Profile 1:** 3x3 MIMO, 2GigE, 16 Watts
- **Power Profile 2:** 3x3 MIMO, 1GigE, 15 Watts
• Power Profile 3 2x3 MIMO, 1GigE, 13.5 Watts

Final Rating: 802.3at

Quality of Service Capability

Criteria Explanation: This criterion denotes that ability of the wireless controller and access point to provide different priority to different applications, users, and data flows. Our test is merely a verification that the ability exists in the controller software.

Weighted Value: 9

Vendor Analysis: The Aruba controller software allows the administrator to specify access points as Voice Only, or application specific. Additionally, the controller software allows the administrator to allocate bandwidth based on the type of application profile.

Vendor Response: “Application-based prioritization / QoS requires stateful inspection, and this capability is a crucial difference between an Aruba solution and competing wireless solutions. Competing solutions prioritize based on a wireless SSID, meaning that all traffic transmitted on a particular SSID is treated the same. This precludes support for voice and video applications running on multi-function devices such as laptops or PDAs, since these devices use multiple protocols. Aruba mobility controllers contain a policy enforcement firewall that statefully identifies, tracks and dynamically prioritizes traffic based on the application flow, e.g., giving higher priority to a voice or video session than an HTTP session, even from the same device. The Aruba solution supports priority queuing, DiffServ and 802.1p for QoS over the wired portion of the network.

In the downstream (e.g., AP to the device) portion of the wireless network, prioritization is handled in the AP. Delay sensitive traffic is identified by the mobility controller and tagged
with an internal header and, optionally, with an 802.1p or DSCP (DiffServ Code Point) tag. Upon receiving priority-tagged frames, the AP places these frames into a high-priority queue. Frames are transmitted using a strict queuing method, ensuring that high priority frames are always transmitted before low-priority frames. In addition, the AP can be configured to adjust the contention window backoff interval when transmitting high-priority traffic, giving this traffic preferential access to the wireless media. In the upstream (e.g., device to the AP) portion of the wireless network, devices transmitting priority-sensitive traffic can use WMM (Wi-Fi Multimedia) - a derivative of IEEE 802.11e - to provide preferential access to the wireless media. WMM also provides a mechanism for client devices to tag frames with a relative priority, allowing the AP to recognize the relative priority of the received frame.

Aruba supports those parts of 802.11e included in the Wi-Fi Alliance specifications for WMM (Wireless Multimedia) and WMM-Power Save. In 802.11e terminology, this includes the EDCA prioritization, TSpec signaling and U-APSD power-save mechanisms. If client devices are using WMM, Aruba APs will translate the WMM tag to an 802.1p or DSCP priority tag in the transport network. If client devices are not using WMM, the Mobility Controller will signal the AP when a voice call is made by a particular client device, and the AP will then tag frames from that client device to indicate high priority traffic.

Aruba APs contain eight different hardware queues where frames may be stored and a strict-queuing algorithm is implemented in order to provide the best level of application delivery and for a mixed data / video / voice deployment. Aruba APs also implement a programmable scheduler for optimized queuing and a mechanism in place to prevent starvation of the low queue. Further configurability is available to fine tune the ToS and CoS values used to map traffic into high priority queues. Because the Aruba controllers contain a stateful user-based
firewall, QoS priority can be directly matched against the user and override any requests from that client. Aruba's application aware role-based access auto-detects, classifies and prioritizes delay sensitive applications flows, such as voice, ensures appropriate prioritization in a converged network. (2)"

Final Rating: Pass

Appendix References: Appendix A: Figure 1

VoFI Support

Criteria Explanation: This criterion denotes the ability for the wireless controller to support VoIP and several different VoIP clients utilizing several different protocols such as H.323 and SIP. To test this functionality, we will be utilizing several different VoIP soft phone clients to see if the wireless controller software detects the presence of a VoIP call present on the network.

Weighted Value: 9

Vendor Analysis: After the Aruba wireless controller and associated AP125 access points, we were able to successfully able to place several VoIP calls using our clients, however the controller could not detect the actual kind of VoIP client that was being utilized and put them in an “Unknown” category. Further testing is required in this area to determine if we can configure the controller so it can recognize our clients.

Vendor Response: “For VoWLAN deployments, Aruba implements Call Admission Control (CAC) by statefully following voice signaling protocols, allowing it to count the number of active calls per AP. As the threshold is reached, other voice devices, not on-call, are load-balanced to neighboring APs. This feature is only feasible because Aruba's approach is identity-based: it identifies users, devices and roles, so the CAC function will load-balance any device
with voice included in its role, but not other devices. It also monitors signaling streams to
determine exactly which devices are on-call, a challenging task for other architectures. CAC
provides redirection of calls to another AP if necessary to improve performance, denial of calls
due to congestion and automatic provisioning of bandwidth. In addition, this level of voice
awareness enables Aruba’s APs to know that a voice call is taking place and not to scan channels
for RF management or intrusion detection purposes until the call is terminated. Aruba’s Voice
Flow Classification engine and Call Admission Control functions are stateful to Session
Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), VOCERA, and Spectralink
Voice Protocol (SVP) VoWLAN protocols. Aruba’s architecture is certified against VoWLAN
handsets from industry leading handset manufacturers such as Hitachi, DoCoMo, SpectraLink,
Vocera, Alcatel, Avaya, RIM, Miktel, Ascom, Zultys, Nortel, NEC, and Cisco.”

“Aruba’s architecture enables different type of devices/users share the same SSID while
being assigned different roles within the mobility controller’s ICSA certified stateful firewall,
providing the best level of security for UC’s WLAN implementation. For non-802.1x enabled
client devices, Aruba’s application-aware stateful firewall provides another layer of security by
providing “blacklisting” of intruders who might be associated to the WLAN utilizing stolen
device credentials, kicking them out of the network when their associated device tries to use any
other protocol than the VoWLAN protocol specified within the access rules of the VoWLAN
profile”(2).

**Final Rating:** Conditional Pass

**Appendix References:** Appendix A: Figure 1; pg. 585 ArubaOS3_3_1UG.pdf
MIMO Mode Capability

**Criteria Explanation:** This criterion denotes which MIMO mode the wireless controller and access point will operate in under standard 802.3af power. To test this, the access point will be connected to an 802.3af capable edge switch and the MIMO mode will be verified from both the client and the wireless controller.

**Weighted Value:** Not Weighted

**Vendor Analysis:** The Aruba AP125 access point currently supports MIMO 40 MHz mode of operation. However, high-throughput can be utilized on a 20 MHz channel or on a 40 MHz channel (bonded channel pair). With standard 802.3af PoE powering the access point, the Aruba AP125 access point operates in 2x3 MIMO mode.

**Vendor Response:** “Both the AP-124 and AP-125 provide support for up to 3x3 MIMO with spatial diversity offering increased throughput and coverage distances” (2).

**Final Rating:** 2x3

**Appendix References:** p.98 ArubaOS3_3_1UG.pdf

Frequencies

**Criteria Explanation:** This criterion denotes the frequencies that are currently supported by the wireless controller and associated access point. The access point and controller should be able to support multiple frequencies in the 2.4Ghz band and the 5.0Ghz band, while retaining 802.11n speeds. We are going to be testing this by putting the access point into different frequency modes and verifying the results from our dual-band wireless clients.

**Weighted Value:** Not Weighted
**Vendor Analysis:** The Aruba wireless controller and AP125 are able to operate in both the 2.4Ghz and 5.0Ghz modes, while operating at 802.11n speeds.

**Vendor Response:** “2.4 GHz - 2.5 GHz and 5.150 GHz - 5.950 GHz (2)”

**Final Rating:** FCC Compliant

---

**Multiple SSIDs**

**Criteria Explanation:** This criterion denotes the ability for the access point to broadcast multiple network SSIDs at the same time. To test this, multiple SSIDs will be configured on the wireless controller and will be verified utilizing our wireless-N clients.

**Weighted Value:** 9

**Vendor Analysis:** The Aruba AP125 was configured for both a captive portal SSID, named “11-N Test” and another SSID, which allows full access, named “ArubaTest.” We were able to both see and connect to both network SSID’s when one access point was powered on.

**Vendor Response:** “Up-to 32 unique SSIDs are supported in which any combination of encryption/authentication methods may be used per SSID. (2)”

**Final Rating:** Pass

**Appendix References:** Appendix A: Figures 3 & 4

---

**Coverage Ratio**

**Criteria Explanation:** This criterion denotes the supported client density per access point and per radio over a specific traffic type.

**Weighted Value:** Not Weighted
Vendor Analysis: From our testing, it appears that 1 Aruba AP125 access point can be installed for 2 enterprise 802.11b/g access points that exist today at the University of Cincinnati.

Vendor Response: “Although the Aruba access points are capable of scaling to a maximum 255 client associations, the practical WLAN design would be based on a reduced client/AP ratio. A design goal of roughly 25 clients per radio, or 50 clients on a dual-radio AP such as the AP-124/125 would be recommended to maintain desirable performance levels. (2)”

Final Rating: 255* (* - Cannot Test due to resource limitations)

Mesh Capabilities

Criteria Explanation: This criterion denotes the situation where access points may be several “hops” away from an access point connected to a network jack and the APs relay or bridge the connection back to the networked AP.

Weighted Value: 5

Vendor Analysis: The Aruba wireless controller and the AP125 currently do support operating in a mesh environment in an 80211a/b/g infrastructure. They currently do not support meshing capabilities with 802.11n. We have been unable to test this functionality with the Aruba Wireless Controller and access point.

Vendor Response: “Aruba’s Secure Enterprise Mesh is a soft programmable architecture, uncoupling the wireless deployment model from any specific hardware platform (can be enabled on any existing or future AP platforms that are part of Aruba's product portfolio – support for the AP-125/125 is expected in the June 2008 ArubaOS release) or software version. This provides for flexibility in allowing our customers to provision Mesh as and when they feel necessary, without having to obtain costly, dedicated Mesh hardware. Additionally, this makes sparing of
Aruba WLAN components more efficient and less costly. Secure Enterprise Mesh allows for the provision of APs where lines cannot be, or are too costly to, run -- such as architecturally challenging areas. Enterprise Mesh is designed to operate redundantly, either through overlapping RF coverage in omni-directional mode or over long haul redundant RF links, both utilizing RF signal and link metrics that are configurable, to ensure deterministic behavior in both performance and fail-over. Security is a key focus of Enterprise Mesh and includes Mesh Point authentication and validation, Mesh link encryption and centralized (user traffic stays encrypted all the way to the mobility controller as it travels through mesh points and mesh portals) user traffic encryption/decryption services on Aruba controllers”(2).

**Final Rating:** Pass

**Appendix References:** Appendix A: Figure 7; p. 64, 191 ArubaOS3_3_1UG.pdf

**Performance Dovetail**

**Criteria Explanation:** This criterion denotes the test of if a higher form of encryption is utilized on the wireless network, is there going to be a performance degradation associated with that? To test this, we will be utilizing the IPERF throughput testing software. SSIDs with and without encryption utilizing WPA2 will be set up and throughput will be tested utilizing UDP and TCP traffic. Performance degradation will be calculated based on the average throughput per SSID.

**Weighted Value:** 9

**Vendor Analysis:** The Aruba wireless controller has a dedicated built in crypto-card which is specifically used to process the encryption used on the wireless infrastructure, therefore, there should be no wireless performance degradation.
Vendor Response: “All Aruba controllers contain dedicated Cavium processors for hardware assisted centralized encrypt/decrypt functionality. This allows Aruba to gain industry leading throughput metrics (up to 8 Gbps crypto performance 3DES, AESCBC256 with the M3 module) while fully maintaining the security advantages of the centralized encryption architecture” (2).

Final Rating: Pass

Appendix References: Appendix A: Figure 8

802.11i encryption

Criteria Explanation: This criterion denotes the ability for the access point and wireless controller to support the most common wireless security methods utilized today. Those security methods include WPA2: Enterprise and 802.1x. In addition to those security methods, 802.11i uses the TKIP and AES encryption ciphers. To test this, we will be attempting to set up multiple SSIDs which utilize WPA2: Enterprise security with AES encryption, which will authenticate to the University’s RADIUS server.

Weighted Value: 9

Vendor Analysis: The Aruba wireless controller and access point were able to broadcast a SSID called “ArubaTest,” which was secured using 802.1x with WPA2: Enterprise and AES encryption authenticating to the University’s RADIUS server.

Vendor Response: “802.11i / WPA2 encryption is supported. In addition, Aruba’s new access point family uses a MIPS processor featuring hardware encryption acceleration; whereas other vendors rely on generic reference designs that offer only modest performance microprocessors. The result of Aruba’s approach is significantly improved performance for WPA, WPA-PSK, WPA2, WPA2-PSK, mixed-mode, WEP, TKIP, and AES encrypted packets. In accordance with
Trusted Computing Group recommendations, a TPM microcontroller inside of the AP 120 serves as a secure vault for all encryption and authentication keys – protecting the access point against software attack, boot sequence manipulation, and compromise in the event of physical theft. ”

**Final Rating**: Pass

**Appendix References**: Appendix A: Figures 5, 6, 8, 9, 13; p. 38 ArubaOS3_3_1UG.pdf

**Compatibility**

**Clean Access Compatible**

**Criteria Explanation**: This criterion denotes the ability for wireless clients utilizing “Clean Access” software to connect to the wireless infrastructure. The wireless controller and access points must be able to handle the integration of clean access software that is currently being utilized at the University of Cincinnati.

**Weighted Value**: 9

**Vendor Analysis**: The Aruba wireless controller and access points can operate with a clean access system in place. The wireless controller requires a special license to integrate with 3rd party clean access applications or can operate with its own clean access service.

**Vendor Response**: “While the Aruba solution provides significant Network Access Control through the use of the Endpoint Compliance System (ECS), best-of-breed partners can be integrated to offer a comprehensive solution that addresses all applications and the most stringent security policies. Aruba integrates with any number of third-party posture assessment systems including Cisco’s posture-based options, CNAC or Clean Access options when leveraging an in-band deployment model” (2).
Final Rating: Conditional Pass

**802.11b/g compatible**

**Criteria Explanation:** This criterion denotes the ability of the 802.11n access point being backwards compatible with the legacy wireless technologies, such as 802.11b and 802.11g. To test this, we will be trying to connect to the same SSID with both an 802.11n client and an 802.11b/g client.

**Weighted Value:** 9

**Vendor Analysis:** The Aruba wireless controller and AP125 access point are capable of allowing 802.11n clients as well as legacy 802.11b/g clients connecting at the same time. This was verified through our wireless clients.

**Vendor Response:** “Yes the Aruba’s AP-124 and AP-125 access point models are 802.11b/g compatible and can provide dual-radio - concurrent 802.11a/n (5 GHz) + b/g/n (2.4 GHz) – operation. (2)”

**Final Rating:** Pass

**Appendix References:** Appendix A: Figure 12
Compatible with Existing Infrastructure

**Criteria Explanation:** This criterion denotes whether or not the wireless controller and access points are compatible with the current Cisco infrastructure that is in place at the university. To test this, we will be installing the controller in the university’s network operation center and will be utilizing the university’s RADIUS for authentication.

**Weighted Value:** 9

**Vendor Analysis:** The Aruba wireless controller and AP125 are fully compatible with the current Cisco infrastructure in place at the University of Cincinnati. We have not experienced any compatibility problems throughout our testing period.

**Vendor Response:** “Yes - Aruba’s Adaptive Radio Management (ARM) features which optimizes channel assignments in real-time, without rebooting the access point to change channels or causing a convulsive domain-wide channel change, is fully 802.11n aware. Thus with the use of ARM technology, 802.11n APs can be inserted within an existing 802.11a/b/g network without incurring the expense, inconvenience, and network management issues associated with a separate parallel blanket network. ARM will select the right channel and power level for 802.11a/b/g/n access points, and will adjust their operation to accommodate local interference and adds, moves, and changes. All existing Aruba Mobility Controllers have the capacity and means to simultaneously support both 802.11n and existing 802.11a/b/g access points with enterprise class performance” (2).

**Final Rating:** Pass
Non-PC Wifi Capable Devices

Criteria Explanation: This criterion denotes the ability for non-pc wireless capable devices to connect to the wireless infrastructure. To test this, we will be using an Apple iPhone to connect to the SSID we configure. We need to verify functionality with a Blackberry.

Weighted Value: 9

Vendor Analysis: We were fully able to connect to the Aruba wireless infrastructure using an iPhone. Web browsing capabilities as well as other services were tested and passed. For this test, we were unable to acquire other dual-band devices such as Blackberries or other PDAs.

Vendor Response: “Both Aruba 802.11n AP models were recently awarded Wi-Fi Alliance certification ensuring interoperability with other leading 802.11n devices as well as other non-pc-based, Wi-Fi certified devices. Certification was awarded for the following standards” (2):

- IEEE Standard
  - 802.11a
  - 802.11b
  - 802.11g
  - 802.11n draft 2.0
  - 802.11h
  - 802.11d

- Security
  - WPA™ - Personal
- WPA™ - Enterprise
- WPA2™ - Personal
- WPA2™ - Enterprise
- EAP Type(s)
- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

- Multimedia
  - WMM

**Final Rating:** Pass

**Value/Cost Features**

**5 year life cycle/Support**

**Criteria Explanation:** This criterion denotes whether or not the vendor has a five year life cycle/support policy for their new 802.11n draft 2.0 and future equipment. This criterion is going to be verified by the documentation provided by the vendor.

**Weighted Value:** 9
Vendor Analysis: Aruba Networks provided us with documentation that stated that they have a standard lifecycle/support policy for all of their products, including the latest 802.11n draft 2.0 and beyond products.

Vendor Response:

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Description</th>
<th>Example Dates</th>
<th>Timing from EOS Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-of-Life Announcement Date</td>
<td>The date that Aruba announces the end of sale and end of life of a given product to the general public.</td>
<td>January 1, 2007</td>
<td>- 90 days</td>
</tr>
<tr>
<td>End-of-Sale (EOS) Date</td>
<td>The last date to order the product through typical sales channels. The product is no longer available for purchase after this date.</td>
<td>April 1, 2007</td>
<td>0</td>
</tr>
<tr>
<td>End of New Service Attachment Date</td>
<td>For equipment and software that is not covered by a support contract, this is the last date to order a new support contract or add the equipment and/or software to an existing support contract in order to continue support through the EOST period.</td>
<td>April 1, 2008</td>
<td>1 year</td>
</tr>
<tr>
<td>End of Service Contract Renewal Date</td>
<td>The last date to extend or renew a service contract for the product.</td>
<td>April 1, 2011</td>
<td>4 years</td>
</tr>
<tr>
<td>End of Next-Day Parts Availability</td>
<td>The last day next business day advanced parts replacement is available for customers with a Next-Day support contract (Contract terms for EOL products must be adjusted to maintain support until the End of Support date.</td>
<td>April 1, 2011</td>
<td>4 years</td>
</tr>
<tr>
<td>End of Support Notification</td>
<td>Email notification to customers with a support contract that support for EOL’d hardware will cease in 12 months</td>
<td>April 1, 2011</td>
<td>4 years</td>
</tr>
<tr>
<td>End of Support</td>
<td>The last date to receive Aruba TAC and return to factory support for the product. After this date, all support</td>
<td>April 1, 2012</td>
<td>5 years</td>
</tr>
</tbody>
</table>
Final Rating: Yes

Free transition to 802.11n ratified version/model

Criteria Explanation: This criterion denotes whether or not the vendor will provide a free transition from the draft 802.11n 2.0 standard hardware to their latest 802.11n hardware once the 802.11n standard is ratified by the IEEE. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Throughout our testing process, 802.11n draft 3.0 was finalized and all of the changes made to the standard were software related changes. With that information at hand, Aruba’s representatives were confident that no hardware changes were going to be necessary when the standard becomes fully ratified. However, in the light that there were hardware changes when the standard is ratified, they would provide a full transition process to the ratified 802.11n hardware standard.

Vendor Response: “The current Aruba Networks AP-124 and AP-125 are designed based on the IEEE 802.11n Draft 2.0 standard. Aruba Networks strives to ensure future proofing of technology and investment protection for our valued customers such as the University of Cincinnati, and we have received no indications from our radio part supplier that fully ratified 802.11n will require any further hardware changes over and above our existing pre-802.11n access points. To further emphasize this point - changes between draft 2.0 and 3.0 have not
impacted the underlying hardware. With respect to the current draft (D3.0) there were approximately 900 comments submitted against this draft – and to date none of this results in a hardware change. So -- our expectation is that the existing hardware has a high probability to be software upgradeable to ratified 802.11n - however - it is not possible for us to guarantee this or to offer a free upgrade. Aruba Networks is committed to working closely with our customers to ensure that their investment in next generation WLAN solutions is protected. For you information – the Standards update/timeline is as follows:

- IEEE 802.11n Draft 2.0 was released on 02/07/07
- IEEE 802.11n Draft 3.0 was released on 10/07/07
- IEEE 802.11n Draft 4.0 is targeted to be released in the March/April 2008 time frame.

**Final Rating**: Yes

**Reference Sites of Equivalent Size**

**Criteria Explanation**: This criterion denotes a listing of clients that the vendor currently supports that are equivalent size to the network infrastructure at the University of Cincinnati. This criterion is going to be verified by the documentation provided by the vendor.

**Weighted Value**: Not Weighted

**Vendor Analysis**: Aruba Networks currently supports several other large organizations, including the US government. The latest deployment for Aruba Networks is the wireless infrastructure for The Ohio State University.
Vendor Response: “The Ohio State University in Columbus, Ohio. All of these infrastructures are very similar in size to the infrastructure at the University of Cincinnati. Additional Sites:

- Northwestern University, Evanston, IL
  - Contact: Chris Hart
  - Phone: [redacted]
  - Email: [redacted]

Network Description – The Northwestern University 802.11n deployment today consists of 250 Aruba Networks AP125’s and an M3 Controller. 500 more AP’s are on order and will be deployed shortly – with the ultimate growth of the Network projected to be approximately 4,000 AP’s. The solution will be deployed in dorms, classroom buildings, Conference Centers and all outdoor locations where students and faculty would like wireless access. Additionally, the bus paths (mesh) and all sports venues will be covered for seamless coverage and vendor/ticket processing.

- Carnegie-Mellon University, Pittsburgh, PA
  - Contact: Dan McCarriar
  - Phone: [redacted]
  - E-mail: [redacted]

- Ohio Wesleyan University, Delaware, OH
  - Contact: Jason LaMar
  - Phone: [redacted]
  - E-mail: [redacted]
**Network Description** – The Ohio Wesleyan University 802.11n deployment will consist of 400 Aruba Networks AP125’s and redundant M3 Controllers. Project roll-out starts the last half of April with completion by mid-August. The initial application for the solution is to provide Wireless Access pervasively and securely across the Ohio Wesleyan Campus (neither of which exists today) – and ultimately – to migrate voice and other Mobility applications onto the network. (2)

**Final Rating**: Yes

**Warranty**

**Criteria Explanation**: This criterion denotes what kind of warranty the vendor provides with their 802.11n draft 2.0 and beyond compliant wireless controllers and access points. This criterion is going to be verified by the documentation provided by the vendor.

**Weighted Value**: Not Weighted

**Vendor Analysis**: During our testing period, Aruba Networks provided us with the standard warranty that they have for all of their products.

**Final Rating**: Standard

**Vendor Installation Support**

**Criteria Explanation**: This criterion denotes what kind of support the vendor will provide for a potential infrastructure upgrade to the new 802.11n standard if the University of Cincinnati would decide to move to it. This criterion is going to be verified by the documentation provided by the vendor.

**Weighted Value**: Not Weighted
Vendor Analysis: During our testing period, Aruba Networks states that they would provide several system engineer’s to ensure the proper rollout of an 802.11n deployment, in addition to working with University engineer’s and providing technical support.

Final Rating: Yes

Upgrade Controller to Support 802.11n

Criteria Explanation: This criterion denotes whether or not the wireless controller has to be upgraded to support 802.11n. That upgrade could either be a hardware or software upgrade, but should not require the replacement of a chassis. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: The wireless controller provided to us during our testing period was already 802.11n capable. The controller itself was completely modular and no chassis replacement would be necessary if an upgrade were to be necessary.

Final Rating: No

Cost to Replace Existing

Criteria Explanation: This criterion denotes the cost of upgrading the current infrastructure at the University of Cincinnati to the new 802.11n standard in areas that are currently covered by the 802.11b/g infrastructure.

Weighted Value: Not Weighted

Vendor Analysis: N/A

Final Rating: $852,476.40
Cost for 100% Coverage

**Criteria Explanation**: This criterion denotes the cost of upgrading the current infrastructure at the University of Cincinnati to the new 802.11n standard in all areas on the campus to provide 100% wireless coverage.

**Weighted Value**: Not Weighted

**Vendor Analysis**: N/A

**Final Rating**: $1,823,804.98

Maintenance Cost

**Criteria Explanation**: This criterion denotes the maintenance cost associated with the vendor’s hardware and software licensing. This criterion is going to be verified by the documentation provided by the vendor.

**Weighted Value**: Not Weighted

**Vendor Analysis**: Throughout our testing period, Aruba networks provided us with documentation that provided their standard maintenance costs that are very comparable to the other leading wireless vendors.

**Final Rating**: Standard

Product Lifecycle

**Criteria Explanation**: This criterion denotes the product lifecycle that the vendor’s current 802.11n hardware currently is in. To be more specific, is the vendor utilizing the latest chipsets/hardware in their 802.11n solution? Additionally, what is the typical EoL (End-of-Life)
time scale for their products? This criterion has been verified by the documentation provided by the vendor.

**Weighted Value**: Not Weighted

**Vendor Analysis**: The Aruba AP125 access point is in the very early stages of its product lifecycle. The product itself was announced to the public in November, 2007 and was released by Aruba Networks in January, 2008. The AP125 access point utilizes the latest Atheros chipset, which has been engineered for power and space efficiency. After speaking with Aruba representatives, they have not EoL’ed any of their products that have been deployed for more than 10 years.

**Final Rating**: Early

**Scorecard Detailed Analysis – Controller**

**Hardware/Performance Features**

**Controller can Manage Mesh Networks**

**Criteria Explanation**: This criterion denotes the ability for the controller to operate in a mesh network infrastructure. The controller can manage and deploy access points configured to act as network bridges to provide wireless connectivity in areas of the University of Cincinnati where network jacks are not available or a network edge presence does not exist.

**Weighted Value**: 5
Vendor Analysis: The Aruba Wireless controller can operate in a mesh network infrastructure, through the use of access points configured to be “Mesh Portals” and “Mesh Points.” “Mesh Portals” are the access points that are configured to be the gateway between the wireless mesh network and the enterprise wired LAN. “Mesh Points” are access points that are configured to act as wireless bridges, which in turn connect to the “Mesh Portals.”

Vendor Response: “The Aruba secure enterprise mesh solution is an effective way to expand network coverage for the university in both outdoor and indoor environments without any wires. Using mesh, UC can bridge multiple Ethernet LANs or simply extend existing wireless coverage. As traffic traverses across mesh APs, the mesh network automatically reconfigures around broken or blocked paths. This self-healing feature provides increased reliability and redundancy: the network continues to operate if an AP goes faulty or a connection fails.

In a mesh environment, the Aruba controller provides centralized provisioning, wireless and security services, policy definition, and ongoing management, similar to those provided if configured in a WLAN user-centric network. Mesh management features include configuration of Mesh Portals, Mesh Points, Mesh Clusters, Mesh Profiles, Mesh Link Metrics, etc. (2)”

Final Rating: Pass

Appendix References: Appendix A: Figure 7; pg. 64, 191 ArubaOS3_3_1UG.pdf

Security Features

ARP Poisoning Prevention

Criteria Explanation: This criterion denotes the ability for the wireless controller to defend itself against a typical ARP poisoning or “ARP Spoofing” attack on the wired infrastructure.
Weighted Value: 9

Vendor Analysis: The Aruba wireless controller can fully defend itself against ARP Poisoning or “ARP spoofing” attacks through the use of DHCP snooping to prevent ARP attacks from occurring. The rule sets for controlling this is located in the wireless controllers IDS system.

Vendor Response: “While Aruba provides mechanisms such as the ability to add static ARP entries, and also turn on proxy-ARP for voice devices, the inspection of ARP requests and entries is typically done by the infrastructure device that is performing the layer 3 routing services for the IP subnet, or the upstream router in a typical Aruba WLAN deployment” (2).

Final Rating: Pass

Appendix References: Appendix A: Figures 10 & 11

IP Spoofing Prevention

Criteria Explanation: This criterion denotes that the controller can detect and respond to IP snooping vulnerability attempts, which are very similar to the ARP Poisoning attacks mentioned above. Typically IP Spoofing is utilized in “Man-in-the-Middle” attacks.

Weighted Value: 9

Vendor Analysis: The Aruba wireless controller can fully defend itself against ARP Poisoning or “ARP spoofing” attacks through the use of DHCP snooping to prevent ARP attacks from occurring. The rule sets for controlling this is located in the wireless controllers IDS system.

Vendor Response: “The integrated firewall implementation in the Aruba Mobility Controller provides the ability to fully inspect all packets, ensuring that DHCP requests are responded to only by known and trusted servers.”

Final Rating: Pass
Broadcast Storm Control

Criteria Explanation: This criterion denotes the ability for the wireless controller to prevent wireless clients from congesting the network with a broadcast storm, which in turn would cause a network disruption to its legitimate users. To test this, we will be utilizing several different wireless clients all doing endless pings on the subnet’s broadcast address. If the controller answers every time, then the vendor does not pass this criterion. If the wireless controller does not answer at all, then the vendor passes this criterion.

Weighted Value: 9

Vendor Analysis: The Aruba wireless controller can fully prevent wireless broadcast storms from occurring. The rule sets for controlling this is located in the wireless controllers IDS/Firewall system.

Vendor Response: “The Aruba solution provides the ability to place bandwidth contracts on physical interfaces for broadcast control in addition to multicast rate optimization techniques that can be applied to wireless users” (2).

Final Rating: Pass

Appendix References: Appendix A: Figures 10 & 11

ACL Support

Criteria Explanation: This criterion denotes the ability for the wireless controller to control its wireless clients through the use of firewall ACL rules to restrict and manage network traffic. Those ACL rules should be fully configurable and highly scalable for large scale deployments.
**Weighted Value:** 5

**Vendor Analysis:** The Aruba wireless controller is fully capable of controlling its wireless clients through the use of ACL’s. The Aruba wireless controller can support several different kinds of ACLs including: standard, ether type, MAC, and session.

**Vendor Response:** “Access control lists (ACLs) are a common way of restricting certain types of traffic on a physical port. ArubaOS provides the following types of ACLs:

- **Standard ACLs** permit or deny traffic based on the source IP address of the packet. Standard ACLs can be either named or numbered, with valid numbers in the range of 1-99 and 1300-1399. Standard ACLs use a bitwise mask to specify the portion of the source IP address to be matched.

- **Extended ACLs** permit or deny traffic based on source or destination IP address, source or destination port number, or IP protocol. Extended ACLs can be named or numbered, with valid numbers in the range 100-199 and 2000-2699.

- **MAC ACLs** are used to filter traffic on a specific source MAC address or range of MAC addresses. Optionally, you can mirror packets to a datapath or remote destination for troubleshooting and debugging purposes. MAC ACLs can be either named or numbered, with valid numbers in the range of 700-799 and 1200-1299.

- **Ethertype ACLs** are used to filter based on the Ethertype field in the frame header. Optionally, you can mirror packets to a datapath or remote destination for troubleshooting and debugging purposes. Ethertype ACLs can be either named or numbered, with valid numbers in the range of 200-299. These ACLs can be used to permit IP while blocking other non-IP protocols, such as IPX or AppleTalk.
ArubaOS provides both standard and extended ACLs for compatibility with router software from popular vendors, however the use of firewall policies are recommended as they provide equivalent and greater function than standard and extended ACLs. When compared with the stateless ACL’s used in other architectures, Aruba’s stateful firewall implementation provides much stronger internal data security:

- Detect and Validate user data packet-by-packet
- Maintain session state logging information per user and monitor flow characteristics
- Prevents TCP SYN, RST Replay and ACK attacks
- Protects against session attacks per application
- Enables per-application redirection of user data traffic to 3rd party Anti-Virus Firewalls
- Reduce the window for an attack by looking at window sizes, protocol sequence numbers, etc.
- Enforces TCP handshake for packet transmission
- Enables per-packet logging for client sessions
- Enables per-application session mirroring and logging for security monitoring and troubleshooting” (2).

**Final Rating:** Pass

**Appendix References:** Appendix A: Figures 10 & 11; p. 241 ArubaOS3_3_1UG.pdf

**SNMPv3**

**Criteria Explanation:** This criterion denotes whether or not the wireless controller is compatible with SNMPv3 for device reporting and management.
Weighted Value: 9

Vendor Analysis: The Aruba wireless controller and APs support versions 1, 2c, and 3 of Simple Network Management Protocol (SNMP) for reporting purposes only. SNMP cannot be used for setting values in an Aruba system in the current ArubaOS version.

Vendor Response: “Aruba controllers and APs support versions 1, 2c, and 3 of Simple Network Management Protocol (SNMP)” (2).

Final Rating: Pass

Appendix References: Appendix A: Figure 16; pg. 522 ArubaOS3_3_1UG.pdf

Works Over CAT-5 or better cabling

Criteria Explanation: This criterion denotes whether or not the wireless controller and access points can operate with CAT-5 or better Ethernet cabling, when connected to the core infrastructure. To test this, we will be connecting the wireless controller and access points to the core infrastructure using both CAT-5e and CAT-6 cabling.

Weighted Value: 9

Vendor Analysis: The Aruba Wireless controller and access points were fully compatible with CAT-5E and CAT-6 cabling.

Vendor Response: “Supported” (2).

Final Rating: Pass

TACACS+ Support

Criteria Explanation: This criterion denotes whether or not the wireless controller is compatible with TACACS+ for user access control.
Weighted Value: 9

Vendor Analysis: The Aruba wireless controller is fully compatible with TACACS+ for user access control.

Vendor Response: “The ArubaOS may be configured to interface with external authentication servers including Terminal Access Controller Access Control System (TACACS+) as well as Remote Authentication Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP).

Alternatively, the controller’s internal database can be used to authenticate users in the event an external server is not needed or available. (2)”

Final Rating: Pass

Appendix References: Appendix A: Figures 14 & 15; p. 276 ArubaOS3_3_1UG.pdf

Support SSH Connections

Criteria Explanation: This criterion denotes whether or not the wireless controller can be managed from an encrypted SSH connection from within the network.

Weighted Value: 9

Vendor Analysis: The Aruba wireless controller can be fully managed from the CLI (Command-Line Interface), which can be access either through SSH or Telnet.

Vendor Response: “For network management via the master mobility controller, the command line interface (CLI) may be accessed through an SSH session from a remote management console or workstation” (2).

Final Rating: Pass

Appendix References: Appendix A: Figures 17 & 18; p. 494 ArubaOS3_3_1UG.pdf
Wireless IDS/IPS

Criteria Explanation: This criterion denotes whether or not the wireless controller has a built-in IDS/IPS system that scans the wireless traffic that passes through it. In addition to traffic scanning, the wireless system should be able to detect rogue access points, ad-hoc network detection and containment, and wireless bridge detection.

Weighted Value: 9

Vendor Analysis: The Aruba wireless IDS, which is built into the controller, provides for the detection of rogue access points, ad-hoc networks and wireless bridges. Additionally, the Aruba wireless controller provides functionality for misconfigured AP detection, weak WEP detection, multi-tenancy protection, and MAC OUI checking.

Vendor Response: “Aruba provides the industries only WLAN solution with integrated security from layers 1 through 7 including wireless IDP (intrusion detection and prevention) as well as an ISCA-certified stateful firewall.

Aruba provides full threat management as it pertains to the wireless network. Aruba APs continuously scan of all channels in the radio spectrum, foreign and domestic, continually feeding the state of the local radio network back to the Controller which correlates data and identifies threats.

The system will identify and classify Rogue Access Points and detect whether they are connected to the network or just in a nearby building reducing the likelihood of ‘false positives’. Rogue access points are ‘unknown’ access points and in many cases these are commercial access points brought from home and connected to the network. The WIP software can command an AP to shut down identified Rogue access points so that they cannot be used on the network and alert
the network manager that a Rogue has been identified; indicating where in the building (via a
door plan) the Rogue has been connected. In addition to rogue APs, the Aruba solution also
includes the ability to detect a variety of unauthorized devices that can potentially disrupt
network operation:

- Ad-Hoc Network
- Wireless Bridge
- Misconfigured AP
- Weak WEP
- Multi-Tenancy Protection
- MAC OUI Checking

Lastly, Aruba’s WIDP solution also works to identify attacks that occur over the wireless
network. Attacks detected include denial of service, flooding, de-authentication, man-in-the-
middle, impersonation, misconfiguration, and jamming. All attacks and suspected attacks are
logged with identifying information such as time, MAC address, and physical location by the
Mobility Controller which also instructs the AP to drop the malicious frames and blacklist the
attack originator.

To supplement the integrated WIDS feature-set discussed above, in July of 2007, Aruba formally
announced it acquisition of Network Chemistry’s line of RFprotect and BlueScanner wireless
security products which historically have been offered as a best-of-breed overlay WIDS/WIPS
solution. RFprotect uses sophisticated multi-modal, stateful techniques for anomaly detection,
vulnerability detection, and threat detection, including heuristic, behavior, statistical and
signature analysis. All of these mechanisms are completely automated and require no user
intervention. With the addition of the Network Chemistry product suite, an Aruba system provides a fully integrated WLAN+WIDP solution that can offer wireless LAN network services as well as detect and prevent wireless threats. This solution is designed for organizations that have a required for deploying large-scale wireless LANs with built-in WIDP capabilities.

Aruba's powerful RFProtect solution incorporates complete automatic threat detection, attack prevention, policy enforcement and compliance reporting” (2).

Final Rating: Pass

Appendix References: Appendix A: Figures 10 & 11; p. 453 ArubaOS3_3_1UG.pdf

5.3.2 Cisco Systems Evaluation

Cisco Systems Configuration and Evaluation
Basic Setup Information

Controller Model:

Access Point Model:

Controller: [Redacted]
Gateway: [Redacted]

VLANs:

Switch VLAN Port Mapping:

Radius:

IP: [Redacted]
Pass: [Redacted]
Ports: [Redacted]
VoIP Clients:
Sjphone (softphone)
Microsoft Netmeeting
Skype

Root password:

FTP password:

WCS IP:

Windows Server 2003 Login:

Controller A (Bottom):
Name: Cisco_controllerA
Mgmt: 
AP Mgr: 
Administrative User Name:
DHCP: 10.27.3.2
RF Group Name: Cisco

Controller B (Top):
Name: Cisco_controllerB
Mgmt: 10.160.3.18
AP Mgr: 10.160.3.19
Administrative User Name: root / paSSw0rd01
DHCP: 10.27.3.2
RF Group Name: Cisco

Location Server

SSID IP:
CiscoStudent: 10.160.4.48
CiscoFaculty: 10.160.5.48

Switch Port Channels

NTP Server:
Network Diagram:

Cisco Equipment Testing Setup

Dell m1330 Apple Macbook Pro Dell m170

Figure 15 - Cisco Equipment Test Setup

Equipment Configurations:

Catalyst 3750 Series 1 2 3 4 5 6 7 8 9 10 1X 2X 15X 16X 11 12 13 14 15 16 17X 18X 31X 32X 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 33X 34X 47X 48X 43 44 45 46 47 48

Cisco 2700 Series Wireless Location Appliance
## Scorecard Evaluation – Access Point

<table>
<thead>
<tr>
<th>802.11n Requirements</th>
<th>AP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware/Performance Features</strong></td>
<td></td>
</tr>
<tr>
<td>Gigabit Interfaces</td>
<td>✓</td>
</tr>
<tr>
<td>IPv6 Native to Hardware</td>
<td>✓</td>
</tr>
<tr>
<td>Outdoor Capable AP</td>
<td>✓</td>
</tr>
<tr>
<td>PoE - 802.3af</td>
<td></td>
</tr>
<tr>
<td>Power Requirement</td>
<td>802.3at</td>
</tr>
<tr>
<td>Quality of Service Capability</td>
<td>✓</td>
</tr>
<tr>
<td>VoFi Support</td>
<td></td>
</tr>
<tr>
<td>MIMO Mode Capability</td>
<td>2x3</td>
</tr>
<tr>
<td>Frequencies</td>
<td>FCC Compliant</td>
</tr>
<tr>
<td>Multiple SSIDs</td>
<td>✓</td>
</tr>
<tr>
<td>Coverage Ratio</td>
<td>1 to 1</td>
</tr>
<tr>
<td>Mesh Capabilities</td>
<td>✓</td>
</tr>
<tr>
<td>Performance Dovetail</td>
<td>✓</td>
</tr>
<tr>
<td>802.11i Encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Compatibility</strong></td>
<td></td>
</tr>
<tr>
<td>Clean Access compatible</td>
<td>✓</td>
</tr>
<tr>
<td>802.11b/g compatible</td>
<td>✓</td>
</tr>
<tr>
<td>Compatible with existing infrastructure</td>
<td>✓</td>
</tr>
<tr>
<td>Non-pc wifi capable devices</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Value/Cost Feature</strong></td>
<td></td>
</tr>
<tr>
<td>5 year life cycle/Support</td>
<td>Yes</td>
</tr>
<tr>
<td>Free transition to 802.11n ratified version/model</td>
<td>Yes</td>
</tr>
<tr>
<td>Reference sites of equivalent size</td>
<td>Yes</td>
</tr>
<tr>
<td>Warranty</td>
<td>Standard</td>
</tr>
<tr>
<td>Vendor Installation Support</td>
<td>Yes</td>
</tr>
<tr>
<td>Upgrade Controller to Support 802.11n</td>
<td>No</td>
</tr>
<tr>
<td>Cost to replace existing</td>
<td></td>
</tr>
<tr>
<td>Cost for 100% coverage</td>
<td></td>
</tr>
<tr>
<td>Maintenance Cost</td>
<td>Standard</td>
</tr>
<tr>
<td>Product Lifecycle</td>
<td>Early</td>
</tr>
</tbody>
</table>

Figure 16 - Cisco AP Scorecard Evaluation
Scorecard Evaluation – Controller

<table>
<thead>
<tr>
<th>Hardware/Performance Features</th>
<th>AP Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller can manage mesh networks</td>
<td>✔</td>
</tr>
</tbody>
</table>

Security Features

Gigabit Interfaces

Criteria Explanation: This criterion denotes that the vendor’s access point is capable of connecting at 1000 mbps to an edge gigabit capable switch. To test this, UCit has provided us with a Cisco 3750-G switch, which is capable of gigabit connection speeds on all switch ports. The access point is connected to the switch, and once the two devices have auto-negotiated the link speed, the results are verified on the switch. Since UCit has no desire at this time to upgrade their edge infrastructure, this test is purely for future capabilities.

Weighted Value: 9
**Vendor Analysis:** The Cisco 1250 series access point has one gigabit port available for network connectivity.

**Vendor Response:** One 10/100/1000BASE-T autosensing (RJ-45) (5)

**Final Rating:** Pass

**Appendix References:** Appendix B: Figures 3 & 4

---

**IPv6 Native to Hardware**

**Criteria Explanation:** This criterion denotes the ability for both the access point hardware as well as the controller hardware to operate with an IPv6 addressing scheme. Since UCit has no desire at this time to switch to an IPv6 addressing scheme, this test is purely for future capabilities.

**Weighted Value:** 1

**Vendor Analysis:** Currently, the Cisco 1250 Series access point and corresponding controllers can support IPv6 clients, but the hardware itself cannot be addressed in an IPv6 environment. To support IPv6 on the hardware infrastructure, a firmware update would be required for the controllers and access points.

**Vendor Response:** No* - Only Client Support Currently. (5)

**Final Rating:** Pass

**Appendix References:** Appendix B: Figure 5

---

**Outdoor Capable AP**
Criteria Explanation: This criterion denotes whether or not the mentioned vendor has a 802.11n access point that is capable of existing outdoors to support green space at the University of Cincinnati.

Weighted Value: 5

Vendor Analysis: The Cisco Systems 1250 Series Access Point can be put outdoors with the appropriate enclosure from Cisco. If the enclosures are not desired, the access point can be mounted indoors and have the antennae’s mounted outdoors to provide wireless in outdoor environments.

Vendor Response: The access point is built with a metal case and sturdy features for deployment in rugged environments such as factories, warehouses, and other industrial environments. It is outdoor capable with the appropriate NEMA enclosure. Operating temperature: -4 to +131°F (-20 to +55°C). Operating humidity: 10 to 90 percent (non-condensing). (5)

Final Rating: Pass

PoE 802.3af

Criteria Explanation: This criterion denotes the ability of the access point to operate on the PoE standard 802.3af, which is the standard power over Ethernet. To test this, we will be connecting the access point to both the 3750-G switch, which UCit provided, and connecting the access point to the edge infrastructure already in place at the University.

Weighted Value: 7

Vendor Analysis: The Cisco 1250 Series Access Point can be powered on pure 802.3af PoE, but only a single radio on the access point will be functioning. It was stated by UCit that they will
not be mounting half of an access point in order to use 802.3af PoE. In order to fully utilize both radios, a power injector is required, which will provide the appropriate 802.3at PoE power if it is not available on the current edge infrastructure.

**Vendor Response:** 802.3af switch (AP1250 with single radio only). AP1250 with two RM1252 radio modules installed: 16.9 W (5)

**Final Rating:** Fail

**Power Requirement**

**Criteria Explanation:** This criterion denotes the actual power requirement to power an individual access point, with the vendor’s recommendation as to power it with standard 802.3af or with 802.3at.

**Weighted Value:** Not Weighted

**Vendor Analysis:** The Cisco 1250 Series Access Point requires 802.3at PoE power to be fully functional. 802.3af power can be utilized but only half of the access point will be powered.

**Vendor Response:** AP1250 with two RM1252 radio modules installed: 16.9 W. AP1250 with one RM1252 radio module installed: 12.95 W. Note: For an AP1250 with two radios, 16.9 W is the maximum power required at the access point (powered device). When deployed using PoE, the power drawn from the power sourcing equipment will be higher by some amount dependent on the length of the interconnecting cable. This additional power may be as high as 1.6W, bringing the total system power draw (access point + cabling) to 18.5 W. A similar consideration applies for an AP1250 with one radio. (5)

**Final Rating:** 802.3at
Quality of Service Capability

Criteria Explanation: This criterion denotes that ability of the wireless controller and access point to provide different priority to different applications, users, and data flows. In our testing, this test is merely a verification that the ability exists in the controller software.

Weighted Value: 9

Vendor Analysis: The Cisco 1250 Series Access Point is fully capable of supporting quality of service on a per SSID basis, which is broken down into a series of differing QoS levels that are predefined. The different QoS levels are defined as: bronze, gold, platinum, and silver. The bronze QoS level is defined as for background traffic and services. The gold QoS level is defined as for video applications. The platinum QoS level is defined as for voice applications, and the silver QoS level is defined as for best effort of any application.

Vendor Response: More details can be found here:

Final Rating: Pass

Appendix References: Appendix B: Figures 8, 9, 10

VoFI Support

Criteria Explanation: This criterion denotes the ability for the wireless controller to support VoIP and several different VoIP clients utilizing several different protocols such as H.323 and SIP. To test this functionality, we will be utilizing several different VoIP soft phone clients to see if the wireless controller software detects the presence of a VoIP call present on the network.

Weighted Value: 9
**Vendor Analysis:** Currently, the Cisco 1250 Series Access Point supports voice traffic over the wireless LAN infrastructure.

**Vendor Response:** This is an AirMagnet product to specifically look at VoWLAN. As for support, since it is sniffing the airwaves, and not directly connecting to the AP's or controller we support it. There is no integration into WCS. (5)

**Final Rating:** Pass

### MIMO Mode Capability

**Criteria Explanation:** This criterion denotes which MIMO mode the wireless controller and access point will operate in under standard 802.3af power. To test this, the access point will be connected to an 802.3af capable edge switch and the MIMO mode will be verified from both the client and the wireless controller.

**Weighted Value:** Not Weighted

**Vendor Analysis:** The Cisco 1250 series Access Point supports 2x3 MIMO mode, which denotes that there are two transmitting antennae’s and 3 receiving antennas running on 802.3at PoE power.

**Vendor Response:** 2x3 MIMO with two spatial streams. Integrated RF management capabilities address the operational challenges of deploying business wireless networks. These capabilities include Radio Resource Management, MIMO, superior DFS support, SDR certification, and spectrum intelligence integration into WCS. Integrated RF management capabilities increase system capacity, improve system performance, perform automated self-healing to compensate for RF dead zones and access point failures, and provide a comprehensive way to manage one of your most precious assets, your corporate spectrum. (5)
Final Rating: 2x3

Frequencies

Criteria Explanation: This criterion denotes the frequencies that are currently supported by the wireless controller and associated access point. The access point and controller should be able to support multiple frequencies in the 2.4Ghz band and the 5.0Ghz band, while retaining 802.11n speeds. We are going to be testing this by putting the access point into different frequency modes and verifying the results from our dual-band wireless clients.

Weighted Value: Not Weighted

Vendor Analysis: The Cisco 1250 Series Access Point supports the standard FCC regulated frequencies that are allowed on the wireless LAN spectrum in the United States of America.

Vendor Response:

A (Americas (FCC)):

• 2.412 to 2.462 GHz; 11 channels
• 5.180 to 5.320 GHz; 8 channels
• 5.500 to 5.700 GHz, 8 channels (excludes 5.600 to 5.640 GHz)
• 5.745 to 5.825 GHz; 5 channels (5)

Final Rating: FCC Compliant

Multiple SSIDs

Criteria Explanation: This criterion denotes the ability for the access point to broadcast multiple network SSIDs at the same time. To test this, multiple SSIDs will be configured on the wireless controller and will be verified utilizing our wireless-N clients.
**Weighted Value:** 9

**Vendor Analysis:** The Cisco 1250 Series Access Point is capable of supporting several SSIDs.

**Vendor Response:** Up to 16 SSIDs can be configured on the 1250 AP. More details can be found here:


**Final Rating:** Pass

**Appendix References:** Appendix B: Figure 7

---

**Mesh Capabilities**

**Criteria Explanation:** This criterion denotes the situation where access points may be several “hops” away from an access point connected to a network jack and the APs relay or bridge your connection back to the networked AP.

**Weighted Value:** 5

**Vendor Analysis:** Currently, as a draft 2.0 product, the Cisco 1250 series access point does not support meshing. This is due to the fact that Cisco is waiting on the final ratification of the standard to push it out to their next generation wireless products.

**Vendor Response:** Mesh capabilities are provided in a different product. The 1250 does not support mesh. The 1520 is a mesh solution. More details on the 1520 can be found here:http://www.cisco.com/en/US/products/ps8368/index.html (5)

**Final Rating:** Pass* - Conditional on Roadmap

**Appendix References:** Appendix B: Figure 6
Performance Dovetail

**Criteria Explanation**: This criterion denotes the test of if a higher form of encryption is utilized on the wireless network, is there going to be a performance degradation associated with that? To test this, we will be utilizing the IPERF throughput testing software. SSIDs with and without encryption utilizing WPA2 will be set up and throughput will be tested utilizing UDP and TCP traffic. Performance degradation will be calculated based on the average throughput per SSID.

**Weighted Value**: 9

**Vendor Analysis**: The Cisco 1250 series Access Point and corresponding controllers utilize a decentralized encryption architecture where the hardware dedicated to the encryption and decryption of traffic is located on the access point themselves and not on the controller.

**Vendor Response**: Please provide more information. We are not sure what dovetail is being considered. (5)

**Final Rating**: Pass

802.11i encryption

**Criteria Explanation**: This criterion denotes the ability for the access point and wireless controller to support the most common wireless security methods utilized today. Those security methods include WPA2: Enterprise and 802.1x. In addition to those security methods, 802.11i uses the TKIP and AES encryption ciphers. To test this, we will be attempting to set up multiple SSIDs which utilize WPA2: Enterprise security with AES encryption, which will authenticate to the universities RADIUS server.

**Weighted Value**: 9
Vendor Analysis: The 1250 series access point and controller both support 802.11i encryption utilizing WPA2-Enterprise with the AES encryption cipher, which is authenticated from a centralized Radius environment.

Vendor Response: None

Final Rating: Pass

Appendix References: Appendix B: Figure 1

Compatibility

Clean Access Compatible

Criteria Explanation: This criterion denotes the ability for wireless clients utilizing “Clean Access” software to connect to the wireless infrastructure. The wireless controller and access points must be able to handle the integration of clean access software that is currently being utilized at the University of Cincinnati.

Weighted Value: 9

Vendor Analysis: The Cisco 1250 Series Access Point and corresponding controllers are both compatible with Clean Access, due to the fact that Clean Access is a Cisco product to begin with.

Vendor Response: More information can be found here:


Final Rating: Pass
802.11b/g compatible

Criteria Explanation: This criterion denotes the ability of the 802.11n access point being backwards compatible with the legacy wireless technologies, such as 802.11b and 802.11g. To test this, we will be trying to connect to the same SSID with both an 802.11n client and an 802.11b/g client.

Weighted Value: 9

Vendor Analysis: The Cisco 1250 Series access point is fully compatible with an 802.11b/g environment. We were able to successfully implement and connect to the access point utilizing a pure 802.11b/g client.

Vendor Response: None

Final Rating: Pass

Appendix References: Appendix B: Figure 2

Compatible with Existing Infrastructure

Criteria Explanation: This criterion denotes whether or not the wireless controller and access points are compatible with the current Cisco infrastructure that is in place at the university. To test this, we will be installing the controller in the university’s network operation center and will be utilizing the university’s RADIUS for authentication.

Weighted Value: 9

Vendor Analysis: The Cisco 1250 series access point and corresponding controller are both fully compatible with the existing infrastructure at the University of Cincinnati.

Vendor Response: None

Final Rating: Pass
Non-PC wifi capable devices

Criteria Explanation: This criterion denotes the ability for non-pc wireless capable devices to connect to the wireless infrastructure. To test this, we will be using an Apple iPhone to connect to the SSID we configure. Need to verify functionality with a Blackberry

Weighted Value: 9

Vendor Analysis: The 1250 Series Access Point is fully compatible with non-pc wifi capable devices. We were able to successfully connect to the wireless LAN via an iPhone and surf the internet.

Vendor Response: None

Final Rating: Pass

Value/Cost Features

5 year life cycle/Support

Criteria Explanation: This criterion denotes whether or not the vendor has a 5 year life cycle/support policy for their new 802.11n draft 2.0 and future equipment. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: 9

Vendor Analysis: The Cisco 1250 series access point comes with Cisco’s standard support cycle through the use of Smartnet.

Vendor Response: Smartnet maintenance is available at different service levels. Pricing varies on the desired support. Figure 18 details this pricing. (5)
Final Rating: Yes

Free transition to 802.11n ratified version/model

Criteria Explanation: This criterion denotes whether or not the vendor will provide a free transition from the draft 802.11n 2.0 standard hardware to their latest 802.11n hardware once the 802.11n standard is ratified by the IEEE. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Currently, Cisco believes that any changes to the final 802.11n standard should require a software upgrade only. Even though this is what we believe to be true at this point in time, there is no guaranteed free upgrade path to the final 802.11n standard. The AP1252 has field replaceable radio modules in the event that the final version of the 802.11n standard should require a hardware upgrade.

Vendor Response: There is not a free migration to the 802.11n capable 1250 AP. Cisco Systems does offer trade in programs for existing network gear. The trade in value varies on the type and amount of hardware traded in and purchased. (5)

Final Rating: Yes
Reference Sites of Equivalent Size

Criteria Explanation: This criterion denotes a listing of clients that the vendor currently supports that are equivalent size to the network infrastructure at the University of Cincinnati. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Currently, Cisco has 802.11n deployments at Duke University, UC Berkeley, and Concordia University, which are all deployments that are comparable to the University of Cincinnati or larger.

Vendor Response: Duke, UC Berkeley and Concordia University (5)

Final Rating: yes

Warranty

Criteria Explanation: This criterion denotes what kind of warranty the vendor provides with their 802.11n draft 2.0 and beyond compliant wireless controllers and access points. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: The 1250 Series access point comes with the Cisco standard warranty.

Vendor Response: Cisco Aironet 1250 Series access points come with the standard Cisco 90-day limited warranty for hardware and software, as described at


Final Rating: Standard
Vendor Installation Support

Criteria Explanation: This criterion denotes what kind of support the vendor will provide for a potential infrastructure upgrade to the new 802.11n standard if the University of Cincinnati would decide to move to it. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Cisco offers installation support through its Advanced Services organization or through an authorized wireless partner.

Vendor Response: Installation services are available through Cisco Advanced Services or an authorized and certified wireless partner. (5)

Final Rating: Yes

Upgrade Controller to Support 802.11n

Criteria Explanation: This criterion denotes whether or not the wireless controller has to be upgraded to support 802.11n. That upgrade could either be a hardware or software upgrade, but should not require the replacement of a chassis. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Currently, the wireless controller in place already supports 802.11n and it is merely a software upgrade to get a controller that doesn’t support 802.11n to support it.

Vendor Response: Cisco Unified Wireless Network Software Release 4.2 supports the 1250 and 802.11n. This support is for both the WISM and WLC. (5)

Final Rating: No
Cost to Replace Existing

**Criteria Explanation:** This criterion denotes the cost of upgrading the current infrastructure at the University of Cincinnati to the new 802.11n standard in areas that are currently covered by the 802.11b/g infrastructure.

**Weighted Value:** Not Weighted

**Vendor Analysis:** Cisco has quoted us the price of $839,236.05 to replace the existing wireless infrastructure at the University of Cincinnati. This was rated at 750 access points.

**Vendor Response:** Negotiable depending on the number of devices required. (5)

**Final Rating:**

---

Cost for 100% Coverage

**Criteria Explanation:** This criterion denotes the cost of upgrading the current infrastructure at the University of Cincinnati to the new 802.11n standard in all areas on the campus to provide 100% wireless coverage.

**Weighted Value:** Not Weighted

**Vendor Analysis:** Cisco has quoted us the price of $1,689,949.65 to cover the entire university’s campus. This was rated at 1500 access points.

**Vendor Response:** Negotiable depending on the number of devices required. (5)

**Final Rating:**
Maintenance Cost

Criteria Explanation: This criterion denotes the maintenance cost associated with the vendor’s hardware and software licensing. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Cisco’s maintenance costs are standard with hardware costs.

Vendor Response: See life cycle/Support section above. (5)

Final Rating: Standard

Product Lifecycle

Criteria Explanation: This criterion denotes the product lifecycle that the vendor’s current 802.11n hardware currently is in. To be more specific, is the vendor utilizing the latest chipsets/hardware in their 802.11n solution? Additionally, what is the typical EoL (End-of-Life) time scale for their products? This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: The Cisco 1250 Series access point is still very early in its product lifecycle, considering it still has a very modular design and is still pretty bulky. This is due to any design changes or hardware changes that need to be made when the standard is finally ratified.

Vendor Response: This varies for every product. There is a standard end of sale schedule that is made public for each product. Typically after a product is announced as End-of-Sale it is still supported for 5-7 years. An example EoS notice can be found here:
Final Rating: Early

Scorecard Detailed Analysis – Controller

Hardware/Performance Features

Controller can Manage Mesh Networks

Criteria Explanation: This criterion denotes the ability for the controller to operate in a mesh network infrastructure. The controller can manage and deploy access points configured to act as network bridges to provide wireless connectivity in areas of the University of Cincinnati where network jacks are not available or a network edge presence does not exist.

Weighted Value: 5

Vendor Analysis: The Cisco 4400 series wireless controller currently supports wireless network meshing, however the 1250 AP currently does not support it.

Vendor Response: Supported (5)

Final Rating: Pass

Appendix References: Appendix B: Figure 6
Security Features

ARP Poisoning Prevention

Criteria Explanation: This criterion denotes the ability for the wireless controller to defend itself against a typical ARP poisoning or “ARP Spoofing” attack on the wired infrastructure.

Weighted Value: 9

Vendor Analysis: The Cisco 4400 Series controller does not support ARP Poisoning Prevention, as it is a feature available in Cisco Ethernet switches.

Vendor Response: No. This is a feature that is available in Cisco Ethernet switches. (5)

Final Rating: Fail

IP Spoofing Prevention

Criteria Explanation: This criterion denotes that the controller can detect and respond to IP snooping vulnerability attempts, which are very similar to the ARP Poisoning attacks mentioned above. Typically IP Spoofing is utilized in “Man-in-the-Middle” attacks.

Weighted Value: 9

Vendor Analysis: The Cisco 4400 Series wireless controller does not support IP Spoofing Prevention, as it is a feature available in Cisco Ethernet Switches.

Vendor Response: No. This is a feature that is available in Cisco Ethernet switches. (5)

Final Rating: Fail
Broadcast Storm Control

Criteria Explanation: This criterion denotes the ability for the wireless controller to prevent wireless clients from congesting the network with a broadcast storm, which in turn would cause a network disruption to its legitimate users. To test this, we will be utilizing several different wireless clients all doing endless pings on the subnet’s broadcast address. If the controller answers every time, then the vendor does not pass this criterion. If the wireless controller does not answer at all, then the vendor passes this criterion.

Weighted Value: 9

Vendor Analysis: The Cisco 4400 Series wireless controller does not support Broadcast Storm Control, as it is a feature that is available in Cisco’s Ethernet switches.

Vendor Response: No. This is a feature that is available in Cisco Ethernet switches. (5)

Final Rating: Fail

ACL Support

Criteria Explanation: This criterion denotes the ability for the wireless controller to control its wireless clients through the use of firewall ACL rules to restrict and manage network traffic. Those ACL rules should be fully configurable and highly scalable for large scale deployments.

Weighted Value: 5

Vendor Analysis: The Cisco 4400 Series wireless controller fully supports access control lists.

Vendor Response: Supported. (5)

Final Rating: Pass
SNMPv3

Criteria Explanation: This criterion denotes whether or not the wireless controller is compatible with SNMPv3 for device reporting and management.

Weighted Value: 9

Vendor Analysis: The Cisco 4400 Series wireless controller fully supports management via SNMPv3.

Vendor Response: Supported. (5)

Final Rating: Pass

Works Over CAT-5 or better cabling

Criteria Explanation: This criterion denotes whether or not the wireless controller and access points can operate with CAT-5 or better Ethernet cabling, when connected to the core infrastructure. To test this, we will be connecting the wireless controller and access points to the core infrastructure using both CAT-5e and CAT-6 cabling.

Weighted Value: 9

Vendor Analysis: The Cisco 4400 Series wireless controller fully supports CAT-5 or better Ethernet cabling.

Vendor Response: Supported. (5)

Final Rating: Pass
TACACS+ Support

Criteria Explanation: This criterion denotes whether or not the wireless controller is compatible with TACACS+ for user access control.

Weighted Value: 9

Vendor Analysis: The Cisco 4400 Series wireless controller fully supports TACACS+, as it is a Cisco proprietary protocol for network device management.

Vendor Response: Supported (5)

Final Rating: Pass

Support SSH Connections

Criteria Explanation: This criterion denotes whether or not the wireless controller can be managed from an encrypted SSH connection from within the network.

Weighted Value: 9

Vendor Analysis: The Cisco 4400 Series wireless controller fully supports SSH connections for management.

Vendor Response: Supported (5)

Final Rating: Pass

Wireless IDS/IPS

Criteria Explanation: This criterion denotes whether or not the wireless controller has a built-in IDS/IPS system that scans the wireless traffic that passes through it. In addition to traffic scanning, the wireless system should be able to detect rogue access points, ad-hoc network detection and containment, and wireless bridge detection.
Weighted Value: 9

Vendor Analysis: The Cisco 4400 Series wireless controller fully supports a wireless IDS/IPS appliance. Cisco offers the Cisco IPS 4200 series to provide this function, as it is not built into the controller itself.

Vendor Response: The Wireless access points work in coordination with Cisco IPS 4200 appliances to shun unwanted network traffic. Details can be found here: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00807360fc.shtml. In addition there are built in wireless IDS security features in the 4400 WLC and WiSM. Details can be found here: http://www.cisco.com/en/US/docs/wireless/controller/5.0/configuration/guide/c5sol.html (5)

Final Rating: Pass

5.3.3 Meru Networks Evaluation

Meru Networks Configuration and Evaluation
Basic Setup Information

Controller Model: Meru MC3025 AP Controller

Access Point Model: Meru AP320 Access Point

Controller: 

Gateway: 

Switch: 

VLANs:

Switch VLAN Port Mapping:

Radius:

IP:  
Pass: caswap
Ports: 

**VoIP Clients:**
Microsoft Netmeeting
Skype

**Equipment Details**

- Meru MC3025 AP Controller
  
  - “The MC3000 is designed for large-scale enterprise deployments and provides comprehensive security, gigabit scalability in its Ethernet interface, service flexibility, and reliable performance. The MC3000 can support up to 150 Meru Access Points” (Controller_882-60034_RevA 3).
Figure 2: MC3000 Rear Panel
- 2x Meru AP 320s – (Following features from AP300_InstallGuide page 2)
  - 802.11n support with channel bonding in both 2.4GHz and 5GHz frequency bands. Channel bonding combines two 20Mhz channels into a single-wide 40Mhz channel for increased throughput.
  - Dual-band external antenna options optimized for MIMO mode.
  - Plug and Play deployment using centralized Meru Controller platforms.
  - Multi-layered security including standard WPA2, 802.11i security such as automatic traffic inspection.
  - Each of these Access points may be powered by a standard 802.3af for 2x2 MIMO Mode. For 3x3 full channel mode, use either a power supply or a 802.3at PoE device.
  - Air Traffic Control technology for 802.11n devices and legacy a/b/g devices.
  - 3x3 MIMO (Multiple Input, Multiple Output) technology with three dedicated, configurable input/output streams that deliver data rates up to 300 Mbps.
  - Software radio upgrades to 802.11n for maximum investment protection.
  - Meru channel span architecture which requires no channel planning or configuration.
  - Six standard multiband, omni-directional antennas.
  - Powered by 5 volt DC input, 802.3af compliant PoE device, or draft 802.3at compliant PoE device.
AP300 Ports and Connectors

The AP300 features the following ports and connectors:

* 10/100/1000 Ethernet port, copper
* 1 Serial console port (reserved)
* DC power input (5 Volts)

Figure 19 - Meru AP 300

Figure 20 - Meru AP 300 (back)
Network Diagram

Meru Equipment Testing Setup

Figure 21 - Meru Equipment Testing Setup

Equipment Configurations

MeruConfig.txt  cas-wireless.log
### Scorecard Evaluation – Access Point

#### 802.11n Requirements

<table>
<thead>
<tr>
<th>Hardware/Performance Features</th>
<th>AP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Interfaces</td>
<td>✓</td>
</tr>
<tr>
<td>IPv6 Native to Hardware</td>
<td>✓</td>
</tr>
<tr>
<td>Outdoor Capable AP</td>
<td></td>
</tr>
<tr>
<td>PoE - 802.3af</td>
<td>✓</td>
</tr>
<tr>
<td>Power Requirement</td>
<td>802.3at</td>
</tr>
<tr>
<td>Quality of Service Capability</td>
<td>✓</td>
</tr>
<tr>
<td>VoFi Support</td>
<td>✓</td>
</tr>
<tr>
<td>MIMO Mode Capability</td>
<td>2x2</td>
</tr>
<tr>
<td>Frequencies</td>
<td>FCC Compliant</td>
</tr>
<tr>
<td>Multiple SSIDs</td>
<td>✓</td>
</tr>
<tr>
<td>Coverage Ratio</td>
<td>1 to 1</td>
</tr>
<tr>
<td>Mesh Capabilities</td>
<td></td>
</tr>
<tr>
<td>Performance Dovetail</td>
<td>✓</td>
</tr>
<tr>
<td>802.11i Encryption</td>
<td>✓</td>
</tr>
</tbody>
</table>

#### Compatibility

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean Access compatible</td>
<td></td>
</tr>
<tr>
<td>802.11b/g compatible</td>
<td>✓</td>
</tr>
<tr>
<td>Compatible with existing infrastructure</td>
<td>✓</td>
</tr>
<tr>
<td>Non-wifi capable devices</td>
<td></td>
</tr>
</tbody>
</table>

#### Value/Cost Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Not Requested</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 year life cycle/Support</td>
<td></td>
</tr>
<tr>
<td>Free transition to 802.11n ratified version/model</td>
<td>Not Requested</td>
</tr>
<tr>
<td>Reference sites of equivalent size</td>
<td>Not Requested</td>
</tr>
<tr>
<td>Warranty</td>
<td>Not Requested</td>
</tr>
<tr>
<td>Vendor Installation Support</td>
<td>Not Requested</td>
</tr>
<tr>
<td>Cost to replace existing</td>
<td>Not Requested</td>
</tr>
<tr>
<td>Cost for 100% coverage</td>
<td>Not Requested</td>
</tr>
<tr>
<td>Maintenance Cost</td>
<td>Not Requested</td>
</tr>
<tr>
<td>Product Lifecycle</td>
<td>Not Requested</td>
</tr>
</tbody>
</table>
Scorecard Evaluation – Controller

<table>
<thead>
<tr>
<th>802.11n Requirements</th>
<th>AP Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware/Performance Features</strong></td>
<td></td>
</tr>
<tr>
<td>Controller can Manage Mesh Networks</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td></td>
</tr>
<tr>
<td>Dynamic ARP inspection</td>
<td>✓</td>
</tr>
<tr>
<td>DHCP snooping</td>
<td></td>
</tr>
<tr>
<td>Broadcast Storm control</td>
<td></td>
</tr>
<tr>
<td>ACL support</td>
<td></td>
</tr>
<tr>
<td>SNMPv3</td>
<td></td>
</tr>
<tr>
<td>Works over CAT-5 or better cabling</td>
<td>✓</td>
</tr>
<tr>
<td>TACACS + Support</td>
<td></td>
</tr>
<tr>
<td>Support SSH Connections</td>
<td></td>
</tr>
<tr>
<td>Wireless IDS/IPS</td>
<td></td>
</tr>
</tbody>
</table>

Scorecard Detailed Analysis – Access Point

**Hardware/Performance Features**

**Gigabit Interfaces**

**Criteria Explanation:** This criterion denotes that the vendor’s access point is capable of connecting at 1000 mbps to an edge gigabit capable switch. To test this, UCit has provided us with a Cisco 3750-G switch, which is capable of gigabit connection speeds on all switch ports. The access point is connected to the switch, and once the two devices have auto-negotiated the link speed, the results are verified on the switch. Since UCit has no desire at this time to upgrade their edge infrastructure, this test is purely for future capabilities.

**Weighted Value:** 9

**Vendor Analysis:** The Meru MC3025 AP controller is equipped with two 10/100/1000 Ethernet ports. The first port on the controller is used to connect to the network infrastructure where it will manage the access points while the second port is reserved but can be configured to work in
active or redundant mode. The indicator LEDs on the MC3025’s Ethernet ports display the current connection speed: Unlit = 10 Mbps, Green solid = 100 Mbps, Amber solid = 1000 Mbps. The Meru AP320 is equipped with a single 10/100/1000 Ethernet port and is capable of both 100mbps and 1000mbps connection speeds. The indicator LEDs on the AP320s do not indicate the access point’s current connection rate.

**Vendor Response:** None Requested

**Final Rating:** Pass

---

**IPv6 Native to Hardware**

**Criteria Explanation:** This criterion denotes the ability for both the access point hardware as well as the controller hardware to operate with an IPv6 addressing scheme. Since UCit has no desire at this time to switch to an IPv6 addressing scheme, this test is purely for future capabilities.

**Weighted Value:** 1

**Vendor Analysis:** Both the Meru MC3025 controller and the AP320 access points can be configured to use IPv6 for both the devices as well as the client IPs. The configuration of IPv6 on the Meru equipment can be achieved through the web GUI or through the CLI.

**Vendor Response:** None Requested

**Final Rating:** Pass

**Appendix References:** Appendix C: Figure 15
Outdoor Capable AP

Criteria Explanation: This criterion denotes whether or not the mentioned vendor has a 802.11n access point that is capable of existing outdoors to support green space at the University of Cincinnati.

Weighted Value: 5

Vendor Analysis: Meru does not currently have any outdoor 802.11n access points available at this time. Meru does offer outdoor capable 802.11 a/b/g access points and they, like most vendors, are likely awaiting the final ratification of the 802.11n standard before offering outdoor capable 802.11n access points. Because the Meru AP320 access points are equipped with removable external antennas, they can be housed indoors while the antennas are placed outside in order to service the campus green space.

Vendor Response: None Requested

Final Rating: Fail

PoE 802.3af

Criteria Explanation: This criterion denotes the ability of the access point to operate on the PoE standard 802.3af, which is the standard power over Ethernet. To test this, we will be connecting the access point to both the 3750-G switch, which UCit provided, and connecting the access point to the edge infrastructure already in place at the University.

Weighted Value: 7

Vendor Analysis: The Meru AP320 access point can be powered via the current PoE 802.3af standard, but it will operate in a degraded operational state which limits the AP to operate in a
2x2 MIMO mode. The access points can be powered in the full 3x3 MIMO mode if supplied with two PoE 802.3af powered connections.

**Vendor Response:** None Requested

**Final Rating:** Conditional Pass

**Appendix References:** Appendix C: Figure 8

---

**Power Requirement**

**Criteria Explanation:** This criterion denotes the actual power requirement to power an individual access point, with the vendor’s recommendation as to power it with standard 802.3af or with 802.3at.

**Weighted Value:** Not Weighted

**Vendor Analysis:** The Meru AP320 access point can operate in a degraded 2x2 MIMO mode with a single PoE 802.3af powered connection. For the Meru AP320 to operate in the optimal full powered 3x3 MIMO mode, the AP requires power from a 5v power adaptor, two PoE 802.3af powered connections, or one PoE 802.3at powered connection.

**Vendor Response:** None Requested

**Final Rating:** 802.3at

---

**Quality of Service Capability**

**Criteria Explanation:** This criterion denotes that ability of the wireless controller and access point to provide different priority to different applications, users, and data flows. In our testing, this test is merely a verification that the ability exists in the controller software.

**Weighted Value:** 9
Vendor Analysis: TBD

Vendor Response: The Meru MC3025 controller allows for the configuration of QoS rules in order to prioritize network traffic over the wireless network. These rules can be custom created or loaded from preset rules on the controller. The web interface of the controller provides statistics for the traffic handled under the rules.

Final Rating: Pass

Appendix References: Appendix C: Figures 1, 2, 3, 4; Page 147 ConfigGd_882-20034_RevA; Page 230 CommRef_882-10034_RevA

VoFI Support

Criteria Explanation: This criterion denotes the ability for the wireless controller to support VoIP and several different VoIP clients utilizing several different protocols such as H.323 and SIP. To test this functionality, we will be utilizing several different VoIP soft phone clients to see if the wireless controller software detects the presence of a VoIP call present on the network.

Weighted Value: 9

Vendor Analysis: The controller handles the VoFI traffic like any of the other network traffic regardless of the device type so long as the device conforms to the security standards required for authentication and network connectivity. The tests were conducted with VoIP clients on laptops over the wireless connection. The traffic is only affected by any active QoS rules running on the controller or other traffic shaping devices on the network.

Vendor Response: None Requested

Final Rating: Pass
MIMO Mode Capability

Criteria Explanation: This criterion denotes which MIMO mode the wireless controller and access point will operate in under standard 802.3af power. To test this, the access point will be connected to an 802.3af capable edge switch and the MIMO mode will be verified from both the client and the wireless controller.

Weighted Value: Not Weighted

Vendor Analysis: The Meru AP320 access point currently supports MIMO 40 MHz mode of operation. However, high-throughput can be utilized on a 20 MHz channel or on a 40 MHz channel (bonded channel pair). With standard 802.3af PoE powering the access point, the Meru AP320 access point operates in 2x2 MIMO mode.

Vendor Response: None Requested

Final Rating: 2x2

Appendix References: Appendix C: Figure 9

Frequencies

Criteria Explanation: This criterion denotes the frequencies that are currently supported by the wireless controller and associated access point. The access point and controller should be able to support multiple frequencies in the 2.4Ghz band and the 5.0Ghz band, while retaining 802.11n speeds. We are going to be testing this by putting the access point into different frequency modes and verifying the results from our dual-band wireless clients.

Weighted Value: Not Weighted

Vendor Analysis: The Meru wireless controller and AP320 are able to operate in both the 2.4Ghz and 5.0Ghz modes, while operating at 802.11n speeds. These frequencies are mandated
(in the United States) by the Federal Communications Commission (FCC) and the Meru
equipment is in accordance with these mandates.

Vendor Response: None Requested

Final Rating: FCC Compliant

Multiple SSIDs

Criteria Explanation: This criterion denotes the ability for the access point to broadcast
multiple network SSIDs at the same time. To test this, multiple SSIDs will be configured on the
wireless controller and will be verified utilizing our wireless-N clients.

Weighted Value: 9

Vendor Analysis: Multiple SSIDs were possible through the creation of various security profiles
(ESSIDs). Each SSID was then broadcasted from each of the AP320s. There does not appear to
be any method to provision certain SSIDs to a particular AP320. Generally speaking, there does
not appear to be any method to indicate an access point’s location in a usable manner nor
provision access points with a particular profile which could be used to manage access points
within a general location.

Vendor Response: None Requested

Final Rating: Pass

Appendix References: Appendix C: Figures 5, 6, 7, 13, 14

Coverage Ratio

Criteria Explanation: This criterion denotes the supported client density per access point and
per radio over a specific traffic type.
**Weighted Value**: Not Weighted

**Vendor Analysis**: Through our observation of the signal propagation throughout the buildings we have surveyed, it appears that a single Meru AP320 access point can be installed for two enterprise grade 802.11 b/g access points which are currently deployed across the University of Cincinnati’s campus. This observation does not take client density and traffic volume or types into consideration and actual signal propagation will vary due to characteristics of the individual structures.

**Vendor Response**: None Requested

**Final Rating**: TBD

---

**Mesh Capabilities**

**Criteria Explanation**: This criterion denotes the situation where access points may be several “hops” away from an access point connected to a network jack and the APs relay or bridge your connection back to the networked AP.

**Weighted Value**: 5

**Vendor Analysis**: The Meru AP320 access point does not support mesh capabilities for any of the 802.11 standards.

**Vendor Response**: None Requested

**Final Rating**: Fail
Performance Dovetail

Criteria Explanation: This criterion denotes the test of if a higher form of encryption is utilized on the wireless network, is there going to be a performance degradation associated with that? To test this, we will be utilizing the IPERF throughput testing software. SSIDs with and without encryption utilizing WPA2 will be set up and throughput will be tested utilizing UDP and TCP traffic. Performance degradation will be calculated based on the average throughput per SSID.

Weighted Value: 9

Vendor Analysis: The Meru equipment was configured to use WPA2-AES encryption to secure the wireless communication between the access points and the wireless clients. There did not appear to be any degradation to the performance of the equipment under this configuration. There was no reference to any hardware encryption modules in any of the documentation for the provided Meru equipment. The Meru equipment did not undergo throughput testing with IPERF as it did not meet enough of UCit’s requirements in order to proceed to the second round of testing.

Vendor Response: None Requested

Final Rating: Pass

802.11i Encryption

Criteria Explanation: This criterion denotes the ability for the access point and wireless controller to support the most common wireless security methods utilized today. Those security methods include WPA2: Enterprise and 802.1x. In addition to those security methods, 802.11i uses the TKIP and AES encryption ciphers. To test this, we will be attempting to set up multiple
SSIDs which utilize WPA2: Enterprise security with AES encryption, which will authenticate to the University’s RADIUS server.

**Weighted Value:** 9

**Vendor Analysis:** The Meru AP320 supports the 802.11i standard as well as legacy security configurations. The minimum security standard allowed by the 802.11n standard is WPA2. The legacy radio bands can utilize the older security methods. The Meru AP320’s were successfully configured to utilize WPA2 Enterprise which authenticated against UC’s RADIUS server.

**Vendor Response:** None Requested

**Final Rating:** Pass

**Appendix References:** Appendix C: Figure 10, 13, 16, 17, 18

### Compatibility

**Clean Access Compatible**

**Criteria Explanation:** This criterion denotes the ability for wireless clients utilizing “Clean Access” software to connect to the wireless infrastructure. The wireless controller and access points must be able to handle the integration of clean access software that is currently being utilized at the University of Cincinnati.

**Weighted Value:** 9

**Vendor Analysis:** There does not appear to be any way of directly interfacing with or directing traffic through Cisco’s Clean Access NAC solution with the Meru MC3025 controller to provide an enhanced security solution. There were no references to any third-party NAC solutions or integration there within any of the Meru MC3025 controller’s documentation we were provided. No configuration options for integration with third-party NAC solutions were found in the web
GUI of the Meru MC3025 controller. Therefore we were unable to verify that the Meru MC3025 controller is compatible with Cisco’s Clean Access NAC solution.

**Vendor Response:** None Requested

**Final Rating:** Fail

### 802.11b/g Compatible

**Criteria Explanation:** This criterion denotes the ability of the 802.11n access point being backwards compatible with the legacy wireless technologies, such as 802.11b and 802.11g. To test this, we will be trying to connect to the same SSID with both an 802.11n client and an 802.11b/g client.

**Weighted Value:** 9

**Vendor Analysis:** The Meru AP320 access points include 802.11 a/b/g radios which are fully compatible with existing wireless clients. 802.11b/g clients were able to authenticate and connect to the Meru AP320s without issue so long as they met the authentication and security requirements needed in order to join the network.

**Vendor Response:** None Requested

**Final Rating:** Pass

**Appendix References:** Appendix C: Figure 11, 16

### Compatible with Existing Infrastructure

**Criteria Explanation:** This criterion denotes whether or not the wireless controller and access points are compatible with the current Cisco infrastructure that is in place at the University. To
test this, we will be installing the controller in the University’s network operation center and will be utilizing the University’s RADIUS for authentication.

**Weighted Value**: 9

**Vendor Analysis**: The Meru test controller was configured and installed within the University’s network operations center while the AP320’s were taken across the university campus to various buildings. These factors indicate that the Meru equipment is compatible with UC’s existing network infrastructure.

**Vendor Response**: None Requested

**Final Rating**: Pass

**Non-PC WIFI Capable Devices**

**Criteria Explanation**: This criterion denotes the ability for non-pc wireless capable devices to connect to the wireless infrastructure. To test this, we will be using an Apple iPhone to connect to the SSID we configure.

**Weighted Value**: 9

**Vendor Analysis**: Devices are able to connect to the Meru AP320 access points if they comply with the 802.11 b/g standards and support the authentication and security mechanisms in place on the wireless network. This criterion was verified with the successful authentication and connection of an Apple iPhone (802.11b/g) to the Meru AP320s. To our knowledge, no non-pc WiFi devices are equipped with 802.11n at this point in time.

**Vendor Response**: None Requested

**Final Rating**: Pass
Value/Cost Features

5 Year Life Cycle/Support

Criteria Explanation: This criterion denotes whether or not the vendor has a five-year life cycle/support policy for their new 802.11n draft 2.0 and future equipment. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: 9

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being requested from Meru Networks.

Vendor Response: None Requested

Final Rating: TBD

Free Transition to 802.11n Ratified Version/Model

Criteria Explanation: This criterion denotes whether or not the vendor will provide a free transition from the draft 802.11n 2.0 standard hardware to their latest 802.11n hardware once the 802.11n standard is ratified by the IEEE. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: TBD

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being requested from Meru Networks.

Vendor Response: None Requested

Final Rating: TBD
Reference Sites of Equivalent Size

Criteria Explanation: This criterion denotes a listing of clients that the vendor currently supports that are equivalent size to the network infrastructure at the University of Cincinnati. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being requested from Meru Networks.

Vendor Response: None Requested

Final Rating: TBD

Warranty

Criteria Explanation: This criterion denotes what kind of warranty the vendor provides with their 802.11n draft 2.0 and beyond compliant wireless controllers and access points. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being collected.

Vendor Response: None Requested

Final Rating: TBD
Vendor Installation Support

Criteria Explanation: This criterion denotes what kind of support the vendor will provide for a potential infrastructure upgrade to the new 802.11n standard if the University of Cincinnati would decide to move to it. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being requested from Meru Networks.

Vendor Response: None Requested

Final Rating: TBD

Upgrade Controller to Support 802.11n

Criteria Explanation: This criterion denotes whether or not the wireless controller has to be upgraded to support 802.11n. That upgrade could either be a hardware or software upgrade, but should not require the replacement of a chassis. This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being requested from Meru Networks.

Vendor Response: None Requested

Final Rating: TBD
Cost to Replace Existing

Criteria Explanation: This criterion denotes the cost of upgrading the current infrastructure at the University of Cincinnati to the new 802.11n standard in areas that are currently covered by the 802.11b/g infrastructure.

Weighted Value: Not Weighted

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being requested from Meru Networks.

Vendor Response: None Requested

Final Rating: TBD

Cost for 100% Coverage

Criteria Explanation: This criterion denotes the cost of upgrading the current infrastructure at the University of Cincinnati to the new 802.11n standard in all areas on the campus to provide 100% wireless coverage.

Weighted Value: Not Weighted

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being requested from Meru Networks.

Vendor Response: None Requested

Final Rating: TBD
Maintenance Cost

Criteria Explanation: This criterion denotes the maintenance cost associated with the vendor’s hardware and software licensing. This criterion will be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being requested from Meru Networks.

Vendor Response: None Requested

Final Rating: TBD

Product Lifecycle

Criteria Explanation: This criterion denotes the product lifecycle that the vendor’s current 802.11n hardware currently is in. To be more specific, is the vendor utilizing the latest chipsets/hardware in their 802.11n solution? Additionally, what is the typical EoL (End-of-Life) time scale for their products? This criterion is going to be verified by the documentation provided by the vendor.

Weighted Value: Not Weighted

Vendor Analysis: Meru did not pass the first round of requirements, resulting in this information not being requested from Meru Networks.

Vendor Response: None Requested

Final Rating: Early
Scorecard Detailed Evaluation – Controller

Hardware/Performance Features

Controller Can Manage Mesh Networks

Criteria Explanation: This criterion denotes the ability for the controller to operate in a mesh network infrastructure. The controller can manage and deploy access points configured to act as network bridges to provide wireless connectivity in areas of the University of Cincinnati where network jacks are not available or a network edge presence does not exist.

Weighted Value: 5

Vendor Analysis: The Meru MC3025 controller does not include any capabilities to manage mesh networks for any of the 802.11 standards.

Vendor Response: None Requested

Final Rating: Fail

Security Features

ARP Poisoning Prevention

Criteria Explanation: This criterion denotes the ability for the wireless controller to defend itself against a typical ARP poisoning or “ARP Spoofing” attack on the wired infrastructure.

Weighted Value: 9

Vendor Analysis: The Meru MC3025 controller does not include any capabilities to prevent ARP poisoning. This capability would have to be handled by external network devices and security configurations.

Vendor Response: None Requested

Final Rating: Fail
IP Spoofing Prevention

Criteria Explanation: This criterion denotes that the controller can detect and respond to IP snooping vulnerability attempts, which are very similar to the ARP Poisoning attacks mentioned above. Typically IP Spoofing is utilized in “Man-in-the-Middle” attacks.

Weighted Value: 9

Vendor Analysis: The Meru MC3025 controller does not include any capabilities to prevent or manage IP spoofing. This capability would have to be handled by external network devices and security configurations.

Vendor Response: None Requested

Final Rating: Fail

Broadcast Storm Control

Criteria Explanation: This criterion denotes the ability for the wireless controller to prevent wireless clients from congesting the network with a broadcast storm, which in turn would cause a network disruption to its legitimate users. To test this, we will be utilizing several different wireless clients doing endless pings on the subnet’s broadcast address. If the controller answer’s every time, then the vendor does not pass this criterion. If the wireless controller does not answer at all, then the vendor passes this criterion.

Weighted Value: 9

Vendor Analysis: The Meru MC3025 controller does not include any capabilities to manage or prevent broadcast storms. This capability would have to be handled by external network devices and security configurations.

Vendor Response: None Requested
Final Rating: Fail

ACL Support

Criteria Explanation: This criterion denotes the ability for the wireless controller to control its wireless clients through the use of firewall ACL rules to restrict and manage network traffic. Those ACL rules should be fully configurable and highly scalable for large scale deployments.

Weighted Value: 5

Vendor Analysis: The Meru MC3025 controller does not include support for true firewall ACL rules based on network traffic types or ports. The controller does provide a “per-user firewall” to be applied to the access point configuration, but this does not provide any real functionality nor does it meet UCit’s requirements. The per-user firewall “restricts network usage on a per user basis by dropping/allowing traffic based on configured policies applied on a firewall tag associated with the user” (p198 – CommRef_882-10034_RevA). Network restrictions based on firewall-like ACL rules would have to be handled by external network devices and security configurations.

Vendor Response: None Requested

Final Rating: Fail

SNMPv3

Criteria Explanation: This criterion denotes whether or not the wireless controller is compatible with SNMPv3 for device reporting and management.

Weighted Value: 9
**Vendor Analysis:** The Meru MC3025 controller’s documentation indicates that it provides support for only SNMPv1 and SNMPv2c. The does not appear to be any way to manually specify SNMP versions on the Meru MC3025 controller. SNMPv3 does not appear to be supported on the Meru MC3025 controller.

**Vendor Response:** None Requested

**Final Rating:** Fail

---

**Works Over CAT-5 or Better Cabling**

**Criteria Explanation:** This criterion denotes whether or not the wireless controller and access points can operate with CAT-5 or better Ethernet cabling, when connected to the core infrastructure. To test this, we will be connecting the wireless controller and access points to the core infrastructure using both CAT-5e and CAT-6 cabling.

**Weighted Value:** 9

**Vendor Analysis:** The Meru MC3025 controller and AP320 access points were fully compatible with CAT-5E and CAT-6 cabling.

**Vendor Response:** None Requested

**Final Rating:** Pass

---

**TACACS+ Support**

**Criteria Explanation:** This criterion denotes whether or not the wireless controller is compatible with TACACS+ for user access control.

**Weighted Value:** 9

**Vendor Analysis:** The Meru controller has no support for the TACACS+ AAA protocol.
Vendor Response: None Requested

Final Rating: Fail

Support SSH Connections

Criteria Explanation: This criterion denotes whether or not the wireless controller can be managed from an encrypted SSH connection from within the network.

Weighted Value: 9

Vendor Analysis: The Meru controller offers full CLI management over a SSH session from a remote management console or workstation.

Vendor Response: None Requested

Final Rating: Pass

Wireless IDS/IPS

Criteria Explanation: This criterion denotes whether or not the wireless controller has a built-in IDS/IPS system that scans the wireless traffic that passes through it. In addition to traffic scanning, the wireless system should be able to detect rogue access points, ad-hoc network detection and containment, and wireless bridge detection.

Weighted Value: 9

Vendor Analysis: The Meru MC3025 controller does not include any capabilities to provide IDS/IPS functionality or integrate with any third-party solutions. This capability would have to be handled by external network devices and security configurations.

Vendor Response: None Requested

Final Rating: Fail
5.4 Scorecard Weighted Calculations

Description

For the scorecard defined by UCit, weighted values were assigned to each scorecard criterion in addition to weighted percentages per each differing section of the scorecard. Each section of the scorecard that is weighted as a percentage are: Access Point – Hardware/Performance Features, Access Point – Compatibility, and Controller – Hardware/Performance Features. The value/cost features are not weighted as a percentage due to the fact that most of the items are purely informational.

5.4.1 Basic Calculation

Calculation 1 – Basic Calculation: In the first calculation or basic calculation, each weighted value that was assigned was multiplied by a Boolean digit represented by a 0 or 1. As can be seen below (Table 1 and Figure 22), Aruba Networks has the most points for this calculation.

<table>
<thead>
<tr>
<th></th>
<th>Meru Networks</th>
<th>Aruba Networks</th>
<th>Cisco Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grand Total</td>
<td>116</td>
<td>199</td>
<td>165</td>
</tr>
</tbody>
</table>

Table 1 – Basic Calculation
5.4.2 Percent Weight Calculation

Calculation 2 - % Weight Calculation: In the first calculation or basic calculation, each weighted value that was assigned was multiplied by a Boolean digit represented by a 0 or 1, which is the calculation done in the first calculation scenario. However, in this scenario, that final number was then multiplied by the percentage weight for each section. As can be seen below (Table 2 and Figure 23), Aruba Networks also has the most points for this calculation.

<table>
<thead>
<tr>
<th></th>
<th>Meru Networks</th>
<th>Aruba Networks</th>
<th>Cisco Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grand Totals</td>
<td>35.75</td>
<td>56.5</td>
<td>48</td>
</tr>
</tbody>
</table>

Table 2 - % Weight Calculation
5.4.3 Cisco Roadmap Calculation

Calculation 3 – Cisco Roadmap: In the first calculation or basic calculation, each weighted value that was assigned was multiplied by a Boolean digit represented by a 0 or 1, which is the calculation done in the first calculation scenario. However, in this scenario, that final number was then multiplied by the percentage weight for each section. For the third calculation, we are comparing mostly Aruba Networks and Cisco Systems and seeing what would happen if Cisco would have most of their roadmap items completed within the next two years when the standard is ratified. As can be seen below (Table 3 and Figure 24), Aruba Networks also has the most points for this calculation.
Table 3 – Cisco Roadmap

<table>
<thead>
<tr>
<th></th>
<th>Meru Networks</th>
<th>Aruba Networks</th>
<th>Cisco Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grand Totals</td>
<td>35.75</td>
<td>56.5</td>
<td>49.75</td>
</tr>
</tbody>
</table>

Figure 24 - Cisco Road Map Total

5.5 Iperf Throughput Testing

Description

For our project, both Aruba Networks and Cisco Systems have passed, to some acceptable level, the scorecard that we developed in cooperation with the network engineers at the University. Therefore, we decided that both vendors will undergo throughput testing to see which hardware offers better performance on an enterprise scale.
To test the hardware and measure the throughput in an accurate way, the project team decided to use Iperf. Iperf is a tool to measure maximum TCP bandwidth, allowing the tuning of various parameters and UDP characteristics. Iperf reports bandwidth, delay jitter, datagram loss. Iperf uses a client and server architecture between two endpoints on a specified network (Iperf).

**Testing Setup**

For our testing setup, we are utilizing a Dell XPS m1330 notebook and a Macbook Pro notebook to serve as our client and server. As can be seen in Figure 1, the Macbook Pro is going to be utilizing a gigabit link to the Cisco 3750-G switch. The Dell XPS m1330 is going to be connected through the wireless via 802.11n to whichever vendor is being tested at the time. Both notebooks, either serving as the client or server were assigned IP addresses that are on the same subnet, to avoid packet routing through UC’s network and potentially loss of performance from that extra network hop.

![Figure 25 - Iperf Testing Setup](image-url)
Testing Results

The following are the testing results from each of the stages of testing that we performed. In each scenario, throughput reports from both the client and server are displayed. Cisco Systems access point clearly outperforms Aruba Networks access point in both scenarios. In each of the scenarios, the first test in each scenario shows that having a larger network pipe to push traffic through definitely helps with the bandwidth capabilities of each of the vendors. However, at the same time, when the Iperf client is set up on the wireless laptop client, there is a considerable bandwidth drop which can be seen in the results of the testing. We are attributing this to multiple factors of the testing environment. First, the wireless network pipe is definitely smaller than the wired one, which goes from a gigabit connection to a 300 megabyte connection. Additionally, wireless throughput suffers a lot of performance problems that do not occur in a wired environment, such as the fact that a wireless connection cannot be fully saturated due to the overhead of the wireless technology itself through the use of encryption protocols and the inherit inefficiencies of how the laptop card driver communicates with the hardware itself. Another consideration is that most of the modern wireless 802.11n laptop cards are dual band enabled, which means that they can communicate at the 2.4 ghz 802.11b/g frequencies as well as the 5ghz 802.11a frequencies, typically have three antennae’s utilized where two are for receiving network traffic and one is for transmitting. This can also be attributed to the severe performance loss in the second testing scenario.

Testing Setup Commands

- **Server:** iperf –s –w 512k
- **Client:** iperf –c <IP> -w 512k –P4 –i2
Testing Setup Definition

- Cisco Test 1: Server – XPS 1330, Client – Macbook Pro
- Cisco Test 2: Server – Macbook Pro, Client XPS 1330
- Aruba Test 1: Server - XPS 1330, Client – Macbook Pro
- Aruba Test 2: Server – Macbook Pro, Client – XPS 1330

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Trial 1</th>
<th>Trial 2</th>
<th>Trial 3</th>
<th>Trial 4</th>
<th>Trial 5</th>
<th>Trial 6</th>
<th>Trial 7</th>
<th>Trial 8</th>
<th>Trial 9</th>
<th>Trial 10</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>81.00</td>
<td>86.60</td>
<td>90.00</td>
<td>90.60</td>
<td>84.80</td>
<td>88.30</td>
<td>76.30</td>
<td>88.40</td>
<td>83.80</td>
<td>93.00</td>
<td>86.3</td>
</tr>
<tr>
<td>Client</td>
<td>104.00</td>
<td>86.80</td>
<td>90.10</td>
<td>90.80</td>
<td>84.90</td>
<td>88.50</td>
<td>76.50</td>
<td>88.50</td>
<td>84.00</td>
<td>93.30</td>
<td>88.7</td>
</tr>
<tr>
<td>Cisco 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>7.91</td>
<td>6.65</td>
<td>7.36</td>
<td>8.38</td>
<td>8.10</td>
<td>7.65</td>
<td>7.37</td>
<td>7.11</td>
<td>5.16</td>
<td>7.19</td>
<td>7.3</td>
</tr>
<tr>
<td>Client</td>
<td>7.90</td>
<td>6.65</td>
<td>7.37</td>
<td>8.38</td>
<td>8.09</td>
<td>7.64</td>
<td>7.37</td>
<td>7.11</td>
<td>5.16</td>
<td>7.19</td>
<td>7.3</td>
</tr>
<tr>
<td>Aruba 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>36.40</td>
<td>62.50</td>
<td>54.70</td>
<td>55.50</td>
<td>24.00</td>
<td>46.70</td>
<td>44.30</td>
<td>65.30</td>
<td>81.40</td>
<td>98.90</td>
<td>57.0</td>
</tr>
<tr>
<td>Client</td>
<td>46.80</td>
<td>62.50</td>
<td>54.70</td>
<td>55.60</td>
<td>24.00</td>
<td>46.80</td>
<td>44.40</td>
<td>65.40</td>
<td>81.40</td>
<td>99.00</td>
<td>58.1</td>
</tr>
<tr>
<td>Aruba 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>0.660</td>
<td>0.834</td>
<td>0.880</td>
<td>0.831</td>
<td>0.774</td>
<td>1.050</td>
<td>0.548</td>
<td>0.754</td>
<td>0.662</td>
<td>0.626</td>
<td>0.8</td>
</tr>
<tr>
<td>Client</td>
<td>0.660</td>
<td>0.834</td>
<td>0.880</td>
<td>0.831</td>
<td>0.774</td>
<td>1.050</td>
<td>0.548</td>
<td>0.754</td>
<td>0.662</td>
<td>0.626</td>
<td>0.8</td>
</tr>
</tbody>
</table>

Table 4: Result Chart
5.5.1 Cisco Systems Test 1

![Cisco Systems Test 1 - TCP Traffic](image)

**Figure 26 - Cisco Systems Test 1 - TCP**

5.5.2 Cisco Systems Test 2

![Cisco Systems Test 2 - TCP Traffic](image)

**Figure 27 - Cisco Test 2 Results Graph**
5.5.3 Aruba Networks Test 1

**Figure 28 - Aruba Test 1 Results Graph**

5.5.4 Aruba Networks Test 2

**Figure 29 - Aruba Test 2 Results Graph**

6. Conclusions and Recommendations

We recommend that UCit not be an early adopter of the 802.11n wireless network technology due to several very important factors. First, with the 802.11n standard still being in a draft status, many of the features that are prevalent in the 802.11b/g realm are still in development status as the standard continues to evolve. Many of the wireless capabilities that UCit is currently deploying, such as wireless network meshing for the University’s green space,
are not yet available in the 802.11n technology space. Second, for full functionality, the 802.11n access points require power-over-ethernet capabilities that exceed the current University infrastructure implementation. This infrastructure is currently being refreshed according to a plan developed in 2006 prior to the release of the 802.11n access point requirements.

Lastly, since the 802.11n standard remains in draft status, there do not exist wide scale implementations of 802.11n technology that allow us to independently verify the veracity of the vendors’ claims.

Should the University of Cincinnati wish to pursue the option of being an early adopter of the 802.11n standard, regardless of the status of its ratification by the IEEE, we recommend that the Aruba Networks be the vendor of choice, and the potential wireless rollout be conducted in a staged, pilot manner.

Aruba Networks is our vendor of choice for multiple reasons. First, Aruba Networks current 802.11n technology best meets the criteria established by UCit and represented on our scorecard as shown in Table 5. Second, Aruba Networks has the most capable 802.11n access point which can be powered off of the current University’s network using 802.3af power, though in a reduced feature set mode. Finally, Aruba Networks provides the most complete product roadmap and they continue to offer the features that other vendors have yet to implement, particularly regarding the hardware and security feature sets.

<table>
<thead>
<tr>
<th><strong>Criterion Met</strong></th>
<th>Aruba Networks</th>
<th>Cisco Systems</th>
<th>Meru Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Hardware/Performance Features</td>
<td>10</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>AP Compatibility</td>
<td>4</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Controller Hardware/Performance Features</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Controller Security Features</td>
<td>9</td>
<td>6</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 5 – Criterion Met per Vendor
Appendix A: Aruba Networks

Figure 1: QoS Rule Status Monitor – Active VoFI Calls

Figure 2: IPv6 Support

Figure 3: Access Point Multiple SSID Support – Client View

Figure 4: Multiple SSID Profile Configuration

Figure 5: SSID Wireless Encryption Configuration
Figure 6: SSID Wireless Encryption Configuration

Figure 7: Wireless Mesh Support

Figure 8: Performance Dovetail – 802.11i Encryption Support
Figure 9: 802.11i Support – RADIUS Configuration

- IDS
  - IDS General Profile
  - IDS Rate Thresholds Profile
  - IDS Signature Matching Profile
  - IDS Signature Profile
  - IDS Denial Of Service Profile
  - IDS Impersonation Profile
  - IDS Unauthorized Device Profile
  - IDS Profile

Figure 10: IDS Configuration

Figure 11: IDS Profile Configuration
Figure 12: Access Point Radio Configuration and Management

Figure 13: Authenticated and Active Wireless Users -- Overview

Figure 14: TACACS+ Support

Figure 15: TACACS+ Configuration

Figure 16: SNMPv3 Support
Figure 17: SSH Management Support

Figure 18: SSH Management Support
Appendix B: Cisco Systems

Figure 1: 802.11n Wireless Encryption Parameters

Figure 2: Access Point Configuration
Figure 3: Wireless Controller Gigabit Support

<table>
<thead>
<tr>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ports</strong></td>
</tr>
<tr>
<td>(Mirroring is disabled)</td>
</tr>
<tr>
<td><strong>Port No</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

Figure 4: Wireless Controller Gigabit Interface Configuration

**General**
- Port No: 1
- Admin Status: Enable
- Mirror Mode: Disable
- Physical Mode: Auto
- Physical Status: 1000 Mbps Full Duplex
- Link Status: Link Up
- Link Trap: Enable
- Power Over Ethernet: N/A

Figure 5: Controller IPv6 Support

IPv6 Enable

Figure 6: Controller Mesh Capability Configuration

**Mesh**

**General**
- Range (RootAP to MeshAP): 12000 feet
- Mac Filter List: Enabled
- Backhaul Client Access: Enabled
- Background Scan: Enabled

**Security**
- Security Mode: EAP
- Authentication Mode: Local Auth
Figure 7: SSID Profile Overview

Figure 8: QoS Rule Creation Screen

Figure 9: QoS Rule Configuration
Figure 10: QoS Profile Overview

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bronze</td>
<td>For Background</td>
</tr>
<tr>
<td>gold</td>
<td>For Video Applications</td>
</tr>
<tr>
<td>platinum</td>
<td>For Voice Applications</td>
</tr>
<tr>
<td>silver</td>
<td>For Best Effort</td>
</tr>
</tbody>
</table>
Appendix C: Meru Networks

Figure 1: QoS Traffic Flow Statistics

Figure 2: QoS Rule Configuration
Figure 3: QoS Rules Overview

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>1720</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>H.264</td>
<td>8</td>
<td>CAPTURE</td>
<td>Head</td>
<td>OFF</td>
<td>80</td>
</tr>
<tr>
<td>2</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>H.264</td>
<td>8</td>
<td>CAPTURE</td>
<td>Head</td>
<td>OFF</td>
<td>80</td>
</tr>
<tr>
<td>3</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>590</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>H.264</td>
<td>8</td>
<td>CAPTURE</td>
<td>Head</td>
<td>OFF</td>
<td>80</td>
</tr>
<tr>
<td>4</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>H.264</td>
<td>8</td>
<td>CAPTURE</td>
<td>Head</td>
<td>OFF</td>
<td>80</td>
</tr>
<tr>
<td>5</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>520</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>H.264</td>
<td>8</td>
<td>CAPTURE</td>
<td>Head</td>
<td>OFF</td>
<td>80</td>
</tr>
<tr>
<td>6</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>H.264</td>
<td>8</td>
<td>CAPTURE</td>
<td>Head</td>
<td>OFF</td>
<td>80</td>
</tr>
</tbody>
</table>

Figure 4: QoS Codec Rules

<table>
<thead>
<tr>
<th>ID</th>
<th>Code</th>
<th>Codec</th>
<th>QoS Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>H.264 Video</td>
<td>H.264 Video</td>
<td></td>
</tr>
</tbody>
</table>
Figure 5: SSID/ESS Profile Creation

Figure 6: SSID/ESS Profile Creation Continued 1
Figure 7: SSID/ESS Profile Creation Continued 2

Figure 8: Access Point Power Configuration Options
Figure 9: Access Point MIMO Mode Operation Parameters

Figure 10: Access Point Wireless Encryption Configuration Options
Figure 11: Access Point Radio Mode Configuration Options

Figure 12: Global Controller Parameter Configuration
**Figure 13:** Multiple SSID/ESS Profiles Overview

**Figure 14:** Multiple SSID Support – Client View

**Figure 15:** Option to enable IPv6 on Meru Equipment

**Figure 16:** AP Configuration – Overview
Figure 17: AP Configuration – Security Profiles

Figure 18: AP Configuration – Update
References


