



Network Rightsizing Best Practices Guide

A Methodology for Reducing Network Costs
and Improving Services



Solution Guide

Copyright

© 2009 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, Bluescanner, For Wireless That Works®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect, The All Wireless Workplace Is Now Open For Business, Green Island, and The Mobile Edge Company® are trademarks of Aruba Networks, Inc. All rights reserved. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (“GPL”), GNU Lesser General Public License (“LGPL”), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.



www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Chapter 1	Network Rightsizing Overview	7
	Key Principles of Rightsizing	7
	Shift Users to the Lowest-Cost Access Method	8
	Eliminate Unnecessary Infrastructure	8
	Reduce Complexity and Operating Cost	8
	Increase Employee Productivity	9
	802.11n Makes Rightsizing Possible	9
	Higher Throughput	9
	Reduced Latency	10
	Improved Reliability	10
	Widespread Adoption	11
	Other Key Enabling Technologies for Rightsizing	11
	Reliability	11
	Manageability	11
	Security	11
	Scalability	11
	The Rightsizing Methodology	12
	Analyze	12
	Justify	12
	Implement	12
	Validate	12
	Rightsizing Windows of Opportunity	12
	Greenfield Network	13
	Closet Refresh	13
	Add/Move/Change Planning	13
	Hoteling	13
Chapter 2	Rightsizing Methodology Overview	15
	Step One – Analyze	15
	Step Two – Justify	15
	Strategy #1 – Reducing Future Access-Layer Capital Expenses and Maintenance Fees	15
	Strategy #2 – Reducing Distribution-Layer Capital Expenses and Maintenance Fees	16
	Strategy #3 – Reducing Current Network Administration Operating Expenses	16
	Strategy #4 – Reducing Electrical Utility Costs	16
	Strategy #5 – Improving Productivity Through Mobility	16
	Selecting the Optimal Strategy	16
	Step Three – Implement	17
	Step Four – Validate	17
Chapter 3	Analyze	19
	Infrastructure Analysis	19
	Statseeker Installation and Configuration	20
	Installing Statseeker	20
	Configuring Statseeker for Device Discovery	20
	Discovering Devices on the Network	24

	Port Usage and Utilization	26
	Traffic Analysis	30
	User Categorization for Rightsizing	30
	Method A – Assign by Usage Type or Job Function	30
	Method B – Assign by Port Utilization	31
	Method C – Assign by Network Traffic Analysis	33
	Network Consolidation	33
	Closet Layout	33
	Stacked Switches	33
	Blade Switches	34
	802.11n Implementation Plan	34
	Capacity Planning	34
	Aruba RF Plan	36
	Financial Analysis	40
	Building Your Own Financial Model	40
	Creating Financial Models for Future Capital Expenses	40
	Creating Financial Models for Future Operating Expenses	40
	Projecting Capital Expenses and Operational Expenses for a Pervasive WLAN	40
	Computing Rightsizing Savings	41
	Using the Aruba Return on Investment Calculator	41
	Existing Enterprise Network Environment Values Section (Input & Summary Results Sheet)	41
	Questions About Typical Costs Section (Editable Defaults Sheet)	42
Chapter 4	Justify	43
	Reducing Future Access-Layer Capital Expenses and Maintenance Fees	43
	Reducing Future Distribution-Layer Capital Expenses and Maintenance Fees	43
	Reducing Current Network Administration Operating Expenses	44
	Reducing Electrical Utility Costs	44
	Improving Employee Productivity Through Mobility	44
	Summarizing Cumulative Cost Savings	44
	Case Studies of Successful Justifications	45
	The California State University	45
	KPMG	45
	Aruba Networks	46
Chapter 5	Implement	47
	Step 1 – Develop a Transition Plan for Migrating Users to the WLAN	47
	Step 2 – Bring Up the Pervasive WLAN	47
	Step 3 – Upgrade Target Population Devices (NICs, drivers)	47
	Step 4 – Move Groups Sequentially to WLAN	48
	Step 5 – Decommission Selected LAN Segments	48
	Step 6 – Dispose of Decommissioned Equipment Properly	48
Chapter 6	Validate	49
	Validation Against Justification	49
	How to Confirm/Prove that the Projected Return on Investment was Achieved	49

Chapter 7	Sample Rightsizing Scenarios	51
	Scenario 1 – 500-Employee Publishing Company	51
	Scenario 2 – Investment Bank with 8,000 Employees	53
	Scenario 3 – Technology Company with 1,000 Employees	55
Chapter 8	Conclusion	57
	Ongoing Analysis	57
	Infrastructure Analysis	57
	Network Utilization	57
	Traffic Analysis	58
Appendix A	ROI Calculator Worksheet	59
Appendix B	Key 802.11n Technologies that Enable Rightsizing	61
	Reliability	61
	ARM	61
	ARM Config	61
	Band Steering	62
	Spectrum Load Balancing	62
	Traffic Shaping for Airtime Fairness	63
	Multicast Traffic Optimization	63
	Adjacent and Co-Channel Interference	63
	Redundancy	64
	Manageability	65
	Aruba Operating System	65
	AWMS	65
	Security	67
	Endpoint-to-Core Authentication and Encryption	68
	Identity-Based Security	69
	Network Admission Control	71
	Wireless Intrusion Protection	71
	Scalability	71
	Performance	72
	Overlay Architecture	72
	L2/L3 Mobility Design Considerations	72
Appendix C	Aruba Contact Information	75
	Contacting Aruba Networks	75

Network rightsizing is a capacity planning and cost reduction strategy based on the principle that wired and wireless LANs should be sized and structured to meet current and future demand. As organizations have increasingly migrated toward using laptop computers, mobile handheld computers, and smart phones, network utilization has shifted away from wired Ethernet for edge access in favor of Wi-Fi. Despite this migration, in many organizations the wired Ethernet edge network is overbuilt relative to actual use, while the Wi-Fi network is often straining under quickly growing loads. This imbalance comes at a steep cost: mobile users are underserved and, therefore, potentially less productive and efficient than they might otherwise be; closet switches are under-utilized, yet are still covered by expensive support contracts; the under-used Ethernet LAN infrastructure is consuming electricity, generating heat, and presenting a load on the air conditioning system; and IT budgets that could fund needed programs are being diverted. Network rightsizing solves these problems and ensures that you pay only for the network capacity and infrastructure that you use today and will require moving forward.

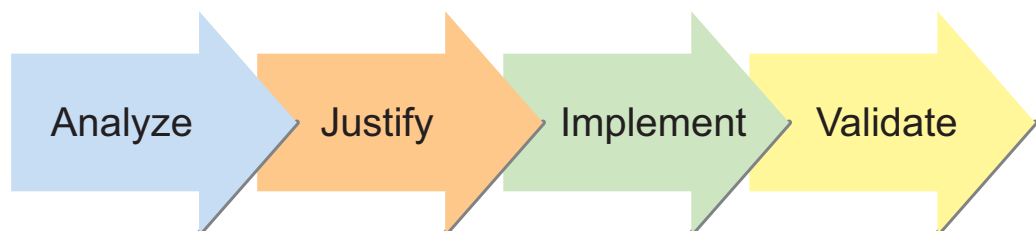
This document provides an overview of network rightsizing. After explaining the principles of network rightsizing and how it can benefit your organization, the methodology for analyzing and planning a rightsized network will be discussed. Finally, you will learn how to implement a rightsized yet scalable Aruba 802.11n network.

Key Principles of Rightsizing

Network rightsizing is grounded on four key principles.

- The first principle is the importance of providing a network connection that meets current and future needs, at the lowest cost to the company.
- The second principle is the importance of eliminating unnecessary equipment that costs money to run and maintain.
- The third principle is the value of minimizing complexity by reducing the time and cost of managing the network.
- The fourth principle is driving employee productivity improvement through mobility.

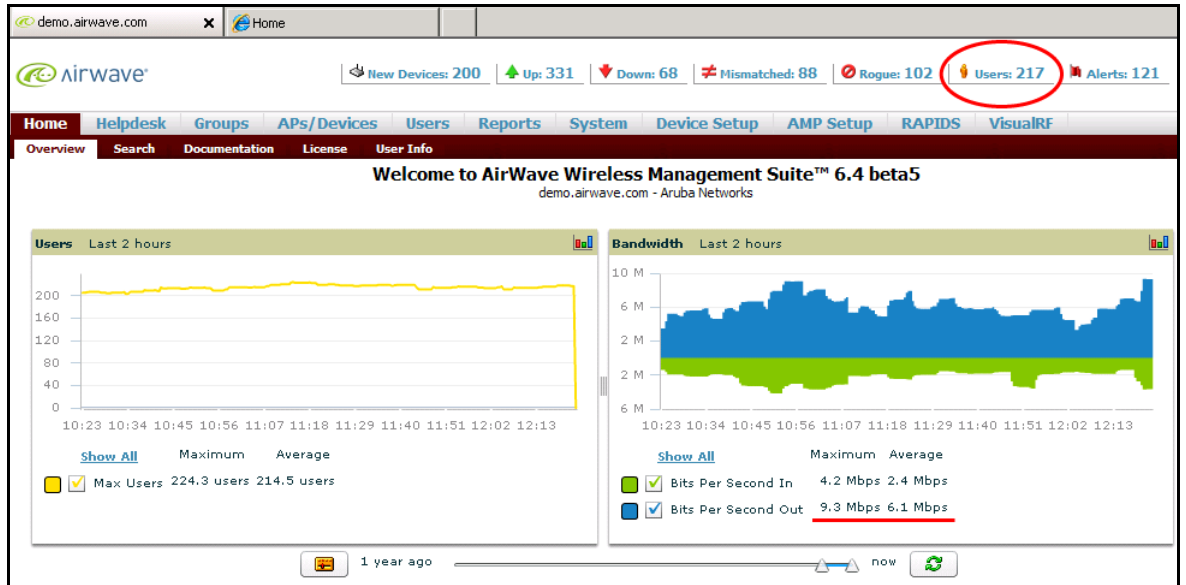
In the following sections these four basic principles will be discussed separately and then in tandem to demonstrate how to build a more streamlined, economical, and extensible network.



Shift Users to the Lowest-Cost Access Method

One of the objectives of network rightsizing is to reduce networking costs, and that can most effectively be accomplished by designing the network to use the lowest-cost access method. Most users do not need gigabit Ethernet to the desktop because “thin” enterprise applications such as HTTP/HTTPS Web-based and virtualized remote applications work well with 1–2 Mbps connections. Many typical office applications use the network for data saves and retrieves that can be easily transferred at 1–2 Mbps speed. Even voice and video applications require far less bandwidth than was the case in the past because of advancements in data compression technology. As a result, most office users can thrive with just 1–3% of the typical 100 Mbps network connection.

Figure 1 Example: AirWave Screen Showing Aruba’s Corporate Network with 215 Users (2-hour activity and aggregate bandwidth of 2.9 Mbps in/8.7 Mbps out)



Driven by demand from mobile workers, the computer industry has been transitioning to laptop computers from desktop machines. Recent sales figures show that crossover has already happened in the consumer market and is in process in the enterprise market. Whereas a single Ethernet port typically serves one user, when connected to a dual-radio 802.11n wireless access point delivering 300 Mbps of shared throughput, that same port will support 25 or more standard office users.

Your enterprise is likely to have a large and growing percentage of laptops among the user base. Laptop users, and their port equivalents, are using a very large percentage of the existing switch ports. Previous wireless standards were not fast enough to allow users to consider cutting the laptop cord except in conference rooms. The advent of 802.11n and Aruba’s reliable, manageable, secure, and scalable WLAN infrastructure made this transition practical.

Eliminate Unnecessary Infrastructure

Historically, most offices have over-provisioned the wired infrastructure by providing between two and four wired ports *per user*. Over-provisioning resulted from the need to support different client types (desktops, phones, and so on) and accommodate future growth. Monitoring software allows you to analyze the percentage of unused ports and significantly reduce their number, thereby reducing refresh, maintenance, and utility costs.

Reduce Complexity and Operating Cost

Additionally, with each 802.11n access point capable of typically supporting 25 or more standard office users, installing an 802.11n network reduces the number of switches and ports needed in the edge network. Decommissioning these ports reduces hardware maintenance, electrical power consumption,

and cooling costs. Organizations facing a network edge upgrade to Power Over Ethernet (PoE) and/or gigabit Ethernet can significantly reduce future capital expenditures by aligning port counts to actual wired port usage. While it may not be possible to switch all users to a wireless LAN, if a significant percentage can shift then some of the savings extracted from the wired LAN can be used to upgrade wireless LAN. A reduction in the number of switches and ports is accompanied by a reduction in the complexity of the network and its management. Many IT departments report that the reduction in the number of adds, moves, and changes resulting from the switch to Wi-Fi allows staff resources to be refocused on other IT cost-saving and performance-enhancing initiatives. Although the installation of an Aruba 802.11n wireless LAN will introduce new networking equipment, these devices are designed to integrate with any Ethernet network, intelligently self-optimize, and be managed from one central interface thereby minimizing the impact on IT staffing.

Increase Employee Productivity

Unlike wired networks that tether a user to a physical port, an 802.11n wireless LAN provides users with almost immediate access to business-critical applications regardless of where they are working. Instead of hunting for a live Ethernet port and cable, users have the freedom to work at the point of service where they're needed most. This capability enhances productivity by facilitating workgroup collaboration and providing instant access to data and services.

Since users often roam off-site, Aruba created Virtual Branch Networking solutions to deliver the network to teleworkers, branch offices, and other remote sites. The security features of the network are designed to provide a uniform user experience regardless of where the network is accessed—in the office, at home, in branch offices – without compromising network integrity.

802.11n Makes Rightsizing Possible

Over the past decade, Wi-Fi technology has advanced to the point that new 802.11n networks can operate at speeds surpassing Fast Ethernet. The incorporation of new OFDM encoding allows 802.11n to pack more bits onto the carrier, increasing the raw half-duplex MAC-layer speed from 54 Mbps to 65 Mbps. Multiple-In Multiple-Out (MIMO) technology provides antenna diversity and improves the reliability and distance of 802.11n wireless LANs. The wire-like performance of 802.11n, coupled with the client-to-core security and scalability of Aruba's wireless LAN infrastructure, makes rightsizing feasible since it provides a viable, cost-effective alternative to Ethernet for edge access.

Higher Throughput

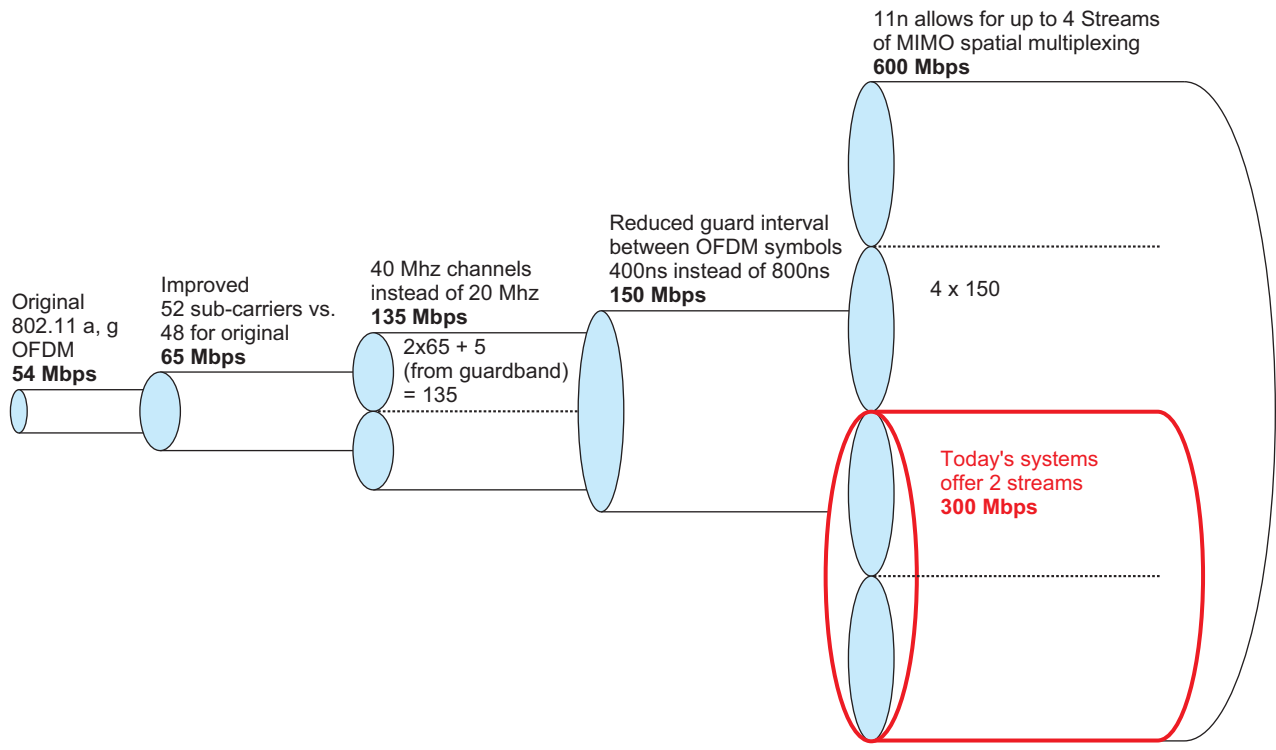
802.11n incorporates many technological enhancements, the first of which is MIMO technology, which involves the use of multiple transmit (Tx) and receive (Rx) antennas in each wireless device, client, and access point. Each Tx antenna transmits a uniquely encoded data stream, known as a “spatial stream” (SS). Each MIMO device is defined with an Tx (N) x Rx (M) antenna matrix. For example, 3x3 signifies 3 transmit and 3 receive antennas, while 2x3 refers to 2 transmit and 3 receive antennas. The 802.11n standard specifies up to 4 transmit and 4 receive antennas. Most current access points use either 2x2 or 3x3 MIMO.

Another significant enhancement embodied in 802.11n is channel bonding. Instead of using a single 20-MHz channel, channel bonding allows the use of two side-by-side channels, more than doubling the data rate. 802.11n operates in both the 2.4 GHz and the 5 GHz spectrums, and offers up to 23 5-GHz non-overlapping 20-MHz channels and 11 non-overlapping channel-bonded 40-MHz channels.

The last 802.11n enhancement we will discuss is the optional 400nsec short guard interval (SGI). Not all clients support SGI, but those that do can boost throughput up to 10 percent.

The illustration below shows how these enhancements can affect the performance of 802.11n as compared to 802.11a and 802.11g. Channel bonding doubles the transmission speed, and since both channels are used together, the guard band that separates the channels can be eliminated, thereby

increasing the MAC-layer transmission speed to 135 Mbps. Reducing the SGI to 400nsec from 800nsec increases the raw transmission speed to 150 Mbps—the maximum transmission rate of a single spatial stream. Access points and most clients are capable of transmitting two separate spatial streams of 150 Mbps each, giving a theoretical maximum PHY rate half-duplex transmission speed of 300 Mbps. This high MAC-layer performance is immediately visible at the application layer. Throughput testing in production environments has shown that application-layer end-to-end throughput ranges from 120 Mbps to 170 Mbps, with a typical throughput of about 150 Mbps at close ranges to the infrastructure and in average environments.



Reduced Latency

802.11n introduces other changes that help improve performance and throughput, and reduce latency. Enhancements made at the MAC layer enable the aggregation of data using a single transmitted frame instead of the multiple frames required by previous 802.11 technologies. 802.11n also incorporates block acknowledgments, a feature that allows receipt of up to 32 frames before sending an acknowledgement; previous techniques required an 802.11 acknowledgement after every wireless frame.

Voice and video applications are time-sensitive and benefit in particular from the additional speed and reduced latency of 802.11n.

Improved Reliability

In previous versions of 802.11, access points or clients that had two antennas used them for diversity, selecting the antenna with the fewest errors to improve throughput. MIMO generates multiple spatial streams and uses multiple antennas to receive these streams. This technique obviates the negative effects of multipath, a phenomenon that occurs when a radio signal reaches the receiving antenna over two or more paths. The net result of MIMO is more reliable communications over a larger coverage area.

Widespread Adoption

The 802.11n standard was formally ratified in September 2009, however, 802.11n shipments achieved critical mass before that date and the installed base of devices is large and growing. 802.11n wireless cards are available for most laptop computers, and 802.11n radios are embedded in many other wireless devices.

Other Key Enabling Technologies for Rightsizing

Although 802.11n delivers robust, high-speed Wi-Fi, an enterprise network requires more than just Wi-Fi connectivity. This section presents other components necessary to effectively implement a rightsized network and discusses capabilities and features, *unique to Aruba*, that ensure that rightsized networks perform and function as expected. [Appendix B on page 61](#) contains additional information about the features discussed briefly below.

Reliability

Networks must be reliable under all operating conditions: environments with a high density of clients; with latency-sensitive applications like voice and video; in the presence of both 802.11n and legacy 802.11abg clients; in the presence of noise and impairments; and in the event of a single point of failure. Aruba's Adaptive Radio Management (ARM) technology ensures that the wireless network is always optimized for local conditions and will automatically adjust power, channel, band, access point loading, and other parameters to ensure reliable high-speed operation, even in extremely crowded and challenging environments.

Manageability

A network must also be straightforward and inexpensive to manage. Network performance must be easily monitored and diagnosed, alerts promptly registered, and compliance reporting available for review. Additionally, best practices must be established to expedite troubleshooting and problem remediation.

If the user wishes to retain legacy networks already in use, then a means must be provided to homogeneously manage old, new, and future networks. Aruba's AirWave Wireless Management Suite provides centralized management of multi-vendor networks from a single integrated console. Many of the world's largest Cisco wireless LAN deployments are managed using the AirWave suite.

Security

Mobility without comprehensive security would be for naught. Aruba's controllers provide an ICSA-certified policy enforcement firewall, client-to-core encryption, user authentication, and a host of other security features to ensure privacy and protect network integrity for local and roaming users. Rogue detection, Wireless Intrusion Detection Services (WIDS), and Wireless Intrusion Protection Services (WIPS) can identify client and access point attacks and, in many instances, prevent them from continuing. Endpoint compliance ensures that only devices in compliance with established anti-virus, operating system patch, and other specified parameters are allowed on the network. Since users are sometimes transitory or temporary, a secure, role-based, guest access feature allows visitors and contractors to connect to the network, but tightly controls all aspects of their connection, including how much network bandwidth they can consume and what they can connect to.

Scalability

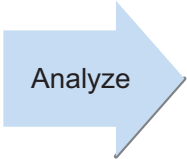
The last key technical component of network rightsizing is scalability. A rightsized network must meet availability and capacity service levels that could increase over time. Some organizations may grow by branching out to regional and satellite offices, others by expanding within an office building or campus. Aruba's centralized architecture is massively scalable and field-proven to accommodate even the

largest enterprises. The controller will automatically download updates to local and remote devices as they are added, and logical support of Layer 3 domains ensures uninterrupted roaming as the system grows in size.

The Rightsizing Methodology

The network rightsizing methodology encompasses four primary phases:

- Analyze
- Justify
- Implement
- Validate



Analyze

Analyze

The first step in network rightsizing is to analyze your network and financial environment. This analysis provides the foundation of network rightsizing and helps validate the necessity of the rightsizing process. There are five essential parts to this initial analysis:

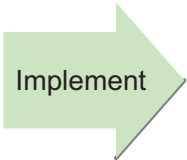
1. infrastructure analysis
2. traffic analysis
3. network consolidation
4. 802.11n implementation
5. baseline financial analysis



Justify

Justify

Strategies and reasons for rightsizing a network are numerous. Every organization is different and will have unique reasons for rightsizing network infrastructure. With budgets being scrutinized and companies looking to reduce costs while improving productivity, rightsizing your network can help you achieve both of these goals. Justification is an important step in evaluating expected financial and other benefits in relation to near-term implementation costs.



Implement

Implement

After the initial analysis has been completed, you will need to plan and perform the implementation of the rightsizing process. This includes installing a pervasive 802.11n network and removing surplus equipment that will no longer be needed.



Validate

Validate

Following the implementation phase, there are three elements to be completed for the validation phase. First, during and after the installation of the 802.11n network, you will want to perform tests to ensure that the redesigned network addresses user needs. Second, you will want to perform usage analysis measurements to provide a baseline for future capacity planning or additional network rightsizing activities. Finally, you will want to document the financial savings realized by the rightsizing effort to demonstrate that the decision to rightsize was well-founded.

Rightsizing Windows of Opportunity

Cost reduction is one of the key drivers of network rightsizing, but there are also predictable business events that can heighten interest in the rightsizing process. In this section you will learn about four

common IT infrastructure drivers that prompt rightsizing: Greenfield Network, Closet Refresh, Add/Move/Change Planning, and Hoteling.

Greenfield Network

One of the most opportune times to rightsize a corporate standard network design is when a new network is being contemplated for a new building or when departments move. Greenfield networks afford the opportunity to start from scratch and to lay out an architecture that will meet current and future needs while minimizing capital expenditures and ongoing operating expenses.

Companies have historically overbuilt networks by pulling three to four Ethernet cables per user to pave the way for future expansions. At a typical cost of US\$200 per drop for Cat5E, and up to twice that for Cat6, this approach is very costly. The extra cables are rarely used and ultimately fill landfills when site changes are made. Network rightsizing offers a blend of wired and wireless access that can typically cut the number of required wired ports and cables in half. Not only will this reduce the number of ports and the amount of cable used, it will also reduce the number of switches needed, saving on maintenance and the ongoing cost of powering, maintaining, and cooling the equipment. The savings from the reduction of the wired infrastructure can be used to subsidize expansion and operation of the wireless network.

Closet Refresh

Closet refreshes are typically performed every four to six years. Rightsizing a network during a refresh period can reduce the cost of a closet refresh by thousands of dollars and recover precious rack and wall space. During the planning stage of a closet refresh, taking an inventory of equipment, including active and inactive ports, will provide useful information about how the wired network can be consolidated, and the wireless network expanded, based on usage patterns. Typically, laptop users benefit significantly from the transition to a wireless LAN.

Depending on the specifics of your network, rightsizing will lower maintenance fees, adds/moves/changes will become easier, and life-cycle costs will fall. An access point uses about one twentieth the power of a switch and up to 90% less heat, and rightsizing customers have reported reducing ongoing edge operating costs by 40%.

Add/Move/Change Planning

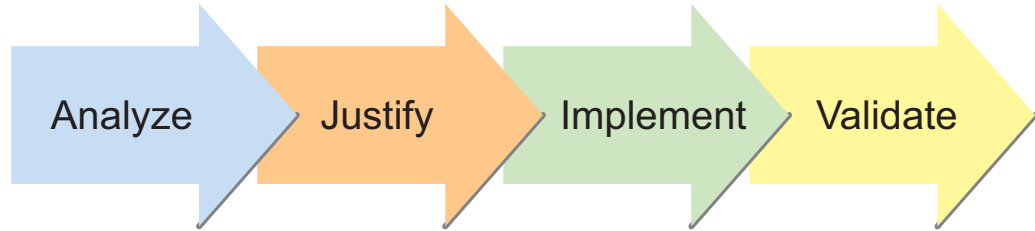
If your organization has high staff turnover, or if employees frequently switch offices, the annual operating cost of wired ports can equal or exceed that of the original network. Adds, moves, and changes are more cumbersome with static ports because of the need to activate, deactivate, and troubleshoot ports. In this environment, a rightsized network would simplify and reduce the cost of network changes.

The wired network does not vanish in this scenario. Rather, the overall port and switch count falls. Subsequent relocation of users would appear as just a roaming event and can be accomplished without the assistance of the IT staff. The resulting cost savings would apply most directly to the subset of users for whom the wireless network is the primary form of edge access.

Hoteling

Network rightsizing can reduce the upfront and ongoing cost of converting cubicles into a shared office pool, also known as hoteling. Depending on the size of the project and the frequency of turnover, hoteling has benefits similar to a greenfield or an add/move/change network. Consider the scale and background of the project in order to determine how best to analyze and implement a rightsized network.

The network rightsizing methodology consists of four essential phases:



NRBPG_232

Step One – Analyze

The first step in network rightsizing is to analyze your network within the context of your budgetary and cost-cutting targets. This analysis provides a quantitative foundation for your objectives, and serves as one factor to be considered when financially justifying network rightsizing. During the analysis phase of the methodology you will focus on the five key components mentioned earlier: infrastructure analysis, traffic analysis, network consolidation, 802.11n implementation, and financial analysis.

You will learn how to complete each of these steps in detail in [Chapter 3, “Analyze” on page 19](#).

Step Two – Justify

The next step is to select one or more of the justification strategies for network rightsizing. While there are many reasons why you may be considering rightsizing your network, a management justification will typically be required. The summary below captures the most common strategies that are used to justify network rightsizing. These are considered in more detail in [Chapter 4, “Justify” on page 43](#).

Strategy #1 – Reducing Future Access-Layer Capital Expenses and Maintenance Fees

IT organizations have traditionally overbuilt network infrastructure to provide flexibility and support anticipated future needs. It is also less expensive to initially install multiple network connections than to add connections in the future. Network overbuilding has led to wiring closets with a large percentage of unused connections. Prior to rightsizing, some Aruba customers report that more than 50% of switch ports were found to be unused. Network rightsizing will decommission most of the unused ports and consolidate the active ports on fewer access-layer switches. If you are installing a new network, rightsizing results in fewer switches to purchase and fewer cables to run. If you are rightsizing an existing network, the result will be fewer switches to upgrade in the future and lower operating expenses on a continual basis. Switches that have been removed from service can be placed in a spare parts pool and used as replacements or for future expansions, conserving future budget funds. Excess switches can also be sold for cash.

In addition to reducing capital expenditures, decommissioning access layer switches also lowers operating expenses. Annual maintenance contracts for switches typically fall around 15% of the original purchase price. Decommissioned switches don't require annual service contracts, so every switch that is added to the spare parts pool saves money.

Strategy #2 – Reducing Distribution-Layer Capital Expenses and Maintenance Fees

With the reduction of access layer switches, you may see a reduction in distribution layer switches too. Since access layer switches connect to distribution layer switches, fewer access layer switches means fewer distribution layer connections are needed. If you are able to reduce the number of distribution switches, you will also reduce your capital and operational expenses relating to those switches.

Strategy #3 – Reducing Current Network Administration Operating Expenses

Every switch on the network needs to be installed, monitored, maintained, and upgraded. By decreasing the number of switches, you are also decreasing the number of administrative hours needed to support that switch. If an administrator spends as little as two hours per month planning, supporting, maintaining, updating, and monitoring each switch, decommissioning as few as four switches would result in an additional day available each month to perform other tasks. With more users moved to the wireless network, the number of adds/moves/changes performed on an annual basis also decreases.

Strategy #4 – Reducing Electrical Utility Costs

The cost of running and cooling networking equipment varies based on the number of devices and the local price of energy. Although the cost to power and cool each device is less significant than the costs of purchasing and maintaining the device, it must still be factored into the operating expense budget. A typical 48-port switch consumes about 143 Watts/hr and generates about 609 BTUs/hr. At an average cost of US\$0.10 per kilowatt-hour for electricity, each switch costs about US\$282 per year to operate. Therefore, every switch that is removed from service will result in annual operating expense savings of US\$282—more in high energy-cost areas.

Strategy #5 – Improving Productivity Through Mobility

In their *Wireless LAN 2009* report, the Aberdeen Group reported that workforce productivity was second only to information access in terms of the impact of wireless LANs on best-in-class organizations. Users no longer have to search for enabled Ethernet jacks, meetings can occur almost anywhere without regard to the availability of wired ports, and workgroup collaboration can happen spontaneously and enterprise-wide. New usage behavior and more efficient work flow are possible in a work environment that fosters mobility instead of tethering users to a wired connection.

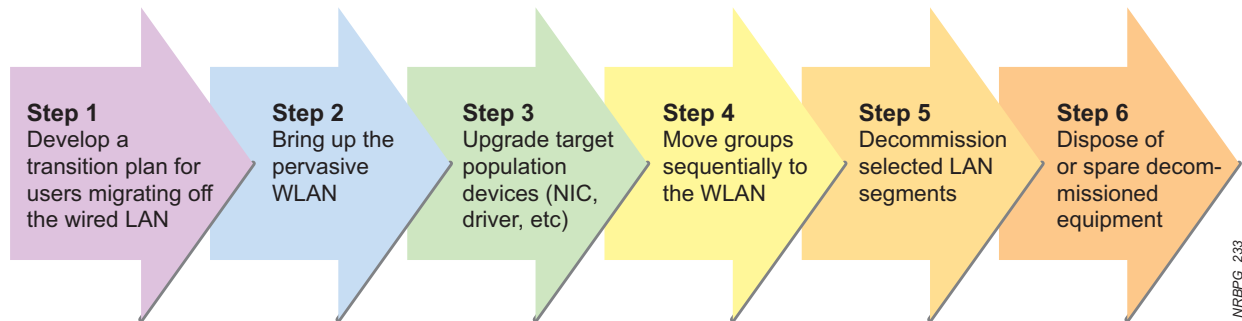
Selecting the Optimal Strategy

There is no single best strategy for justifying a network rightsizing project. Each company has unique issues, concerns, and criteria associated with their computing needs. Issues that are important for one company may be less so for another.

In most cases, the justification for network rightsizing is based on multiple concurrent financial benefits that broadly impact an enterprise. The returns on investment are spread across multiple organizations, compounding the importance of the investment relative to a single, narrowly focused project. Since the returns are derived from multiple sources, the lack of significant return from any one area will be mitigated by returns from other sources, derisking the overall rightsizing effort.

Step Three – Implement

After the decision to rightsize a network has been made, the next phase is to implement the project. This is a stepped process that needs to be carefully planned and managed to ensure that it has the greatest acceptance across the user community.



The implementation process consists of six steps:

- Step 1 – Develop a transition plan for users migrating off the wired LAN;
- Step 2 – Bring up the pervasive WLAN;
- Step 3 – Upgrade target population devices (NIC, driver, and so on);
- Step 4 – Move groups sequentially to the WLAN;
- Step 5 – Decommission selected LAN segments;
- Step 6 – Dispose of or spare decommissioned equipment.

When implementing a pervasive WLAN in a large organization, we recommend that the project be implemented one building or campus at a time using a repeatable plan that can be replicated throughout the organization. For more information on the Implementation phase, see [Chapter 5, “Implement” on page 47](#).

Step Four – Validate

After a network rightsizing project has been implemented, it is important to quantify the ROI to determine if the original goals have been achieved. To do so, Aruba recommends maintaining records during the first twelve months after rightsizing to calculate capital cost savings from decommissioned switches and ports, and operational cost savings from electrical and cooling costs, as well as changes in IT staff utilization.

To help quantify the productivity benefit due to employee mobility, compare the network utilization prior to and after rightsizing the network, including the number of users that were transitioned from the wired network to the wireless network, to determine if the numbers match your initial projections. If the users have accepted and are using the upgraded WLAN, then post-rightsizing WLAN traffic should be equal to our greater pre-rightsizing traffic. In most cases WLAN usage will rise due to increased network access, which drives up overall utilization and network traffic. If your IT Help Desk maintains user satisfaction scores for the network, these should be tracked before, during, and after the rightsizing is completed. [Chapter 6, “Validate” on page 49](#) provides more insight to the Validate phase.

Analyze

The first step in network rightsizing is to analyze network utilization. The five key components of this process follow below.

- Infrastructure analysis will inventory the current equipment, with a focus on the actual use of existing ports and switches to create a hard estimate of surplus network and port capacity.
- Traffic analysis will help to determine the general and specific network traffic loading presented by client devices and applications. This information is needed to determine the number of APs required to meet current and future bandwidth needs.
- Using the results of the infrastructure and traffic analyses, you will be able to plan the appropriate level of network closet consolidation.
- Using the information obtained in the previous steps, you will next plan the implementation of the 802.11n network.
- The implementation plans will become the basis for establishing return-on-investment (ROI) benefits and timeframes. These will feed into the financial models that justify the rightsizing program.

Third-party network measurement tools are required to complete the steps in this chapter. There are many network analysis tools available on the market, some of which you may already own. In this section you will learn how to perform a network rightsizing analysis using a product called Statseeker[®]. A free evaluation license of this product is available should you need it. It doesn't matter which tool you use so long as you can extract the necessary information from the network to complete the required steps.

Aruba has also created a financial analysis tool called the *Aruba Rightsizing Calculator*. We will review this tool in detail with some examples in [Chapter 7, "Sample Rightsizing Scenarios"](#) on page 51. This is an important step that provides input to the justification step that follows.

Infrastructure Analysis

The goal of the infrastructure analysis is to identify which LAN switch ports are being used and the percentage of users and ports that can move to a wireless network for primary network access. This information forms the quantitative justification for rightsizing, and feeds several of the planning tasks for the rightsizing implementation. For example, with port-level utilization data, you can tag LAN ports that will no longer be needed and determine how to retire those ports. You can use two methods to identify the unused ports: manual monitoring and software monitoring.

Manual monitoring is performed by visually inspecting the workstations, work environment, and wiring closets to determine which edge switch ports are being used. For stable office environments, manual monitoring offers an initial assessment of network use; however, it typically only provides an overview or snapshot at a specific point in time. Aruba recommends visiting each Intermediate Distribution Frame (IDF) during peak usage and recording the number of live and unused ports on each switch. This can be easily accomplished by checking the port status lights, but is more labor-intensive and does not permit trending data over time compared with automated software monitoring.

To obtain a more thorough view of the network, you will need a basic network monitoring tool to centrally monitor all of the ports on the network switches to assess port activity. In most environments, just a few hours of monitoring will yield information about the percentage of unused ports on your network. We recommend that you monitor your network for a minimum of two weeks. This will provide

better data sampling and will help avoid misidentified ports that are associated with users who are temporarily out of the office. Monitoring should also be performed during periods representative of typical usage, i.e., not during the summer months at a school campus when activity typically decreases.

For some customers, it may be best to conduct the network monitoring exercise and confirm the results with a manual inspection of the rightsized coverage area. For example, a manual inspection would highlight ports reserved for contractors in designated cubicles that would otherwise be shown as unused.

Statseeker Installation and Configuration

Aruba has tested and recommends the Statseeker software tool for network monitoring. Statseeker is a highly scalable, industrial strength, network infrastructure monitoring application. Statseeker uses SNMP and PING to unobtrusively poll and collect data from network devices. You can obtain a fully functional evaluation copy of the software upon request. Depending on the size of your network, Statseeker typically requires a computer with a 64bit Dual or Quad Core CPU, 2–8 GB RAM, 240–500 GB hard drive, and a Gigabit Ethernet adapter. Please visit the Statseeker website to determine the specific equipment requirement for your network size. If your network has more than 200,000 network interfaces, you will need to speak with Statseeker technical support to determine how best to support your deployment.

Installing Statseeker

Statseeker installation is performed from a bootable CD that will completely reformat and partition the hard drive of the computer on which it is installed. You will be prompted for typical computer and networking information, and a license key. The installation should take 10 to 15 minutes to perform. Once Statseeker is installed, all interaction with the product is done from a desktop computer using a Web browser.

Configuring Statseeker for Device Discovery

Before you can poll the network for usage information, it is necessary to spend some time configuring Statseeker. In order to monitor the network, you must first populate the Statseeker tool with all of the devices existing on your network. There are two methods for doing this:

- Discover the devices using a hosts file;
- Discover the devices by scanning a set of IP Ranges.

If you have an up-to-date list of IP addresses and hostnames, then discovering via the hosts file is the best method to use. If you do not have an up-to-date list, then you will need to discover the devices by scanning IP Ranges. It is recommended that you keep these IP address ranges as close as possible to your specific edge switch infrastructure IP addresses; do not use a very large IP range or superset that would include devices that you don't need to monitor for the network rightsizing assessment. The Statseeker server should be located on a network segment that is routable to all IP address ranges that will be scanned.

The first step toward discovering your devices is to configure the SNMP Community Strings used to query the network.

1. After you use your Web browser to connect to the Statseeker server and log in, go to the **Administration Tool** menu to configure the initial settings.
2. To add the SNMP community strings, select **SNMP Communities** and then enter the read-only SNMP community strings that have been configured on your network devices.

You want to try to keep this list short since Statseeker will try each configured community string on each device; therefore, each additional configured community string will significantly increase the device discovery time. As you configure Statseeker, beneath many of the entry windows you will see notes describing the information that you need to enter, as well as rules for entering that information and examples.



Once the community strings are entered, you need to tell Statseeker what to scan.

- To configure Statseeker with a hosts file, go to the **Administration Tool** menu and select **Hosts File**. At this point you can either enter the IP address of each host, followed by the hostname, or copy and paste a list of hosts into this window.

The host information must be entered as shown in the graphic that follows, with each line containing one entry and the IP address being followed by at least one space and then the hostname. Each device must have only one entry in the hosts file.



If a device has more than one IP address, select the single address that should be polled by Statseeker.

The screenshot shows the 'Hosts File (plain text)' configuration window. On the left is a navigation menu with categories: General, Network Discovery, Group Assignments, and Discover My Network. The 'Hosts File' option is highlighted with an orange box. The main area contains a text input field with the following text: '10.2.1.243 core-router', '10.2.1.253 border-router', '10.100.10.234 server-switch', '10.100.10.252 Port-of-Baltimore-Core2', and '10.100.10.253 Port-of-Baltimore-Core1'. Below the input field is a 'Save' button. Below the 'Save' button is a 'Then click Save' instruction with a downward arrow. At the bottom, there is an 'Example' section showing the format: '10.1.1.1 router1' and '10.1.1.4 switch1'.

Hosts File (plain text)

```
10.2.1.243 core-router
10.2.1.253 border-router
10.100.10.234 server-switch
10.100.10.252 Port-of-Baltimore-Core2
10.100.10.253 Port-of-Baltimore-Core1
```

Enter IP / Host names here

Then click Save

Save

This is a plain text file which lists IP Addresses and hostnames in the following format:

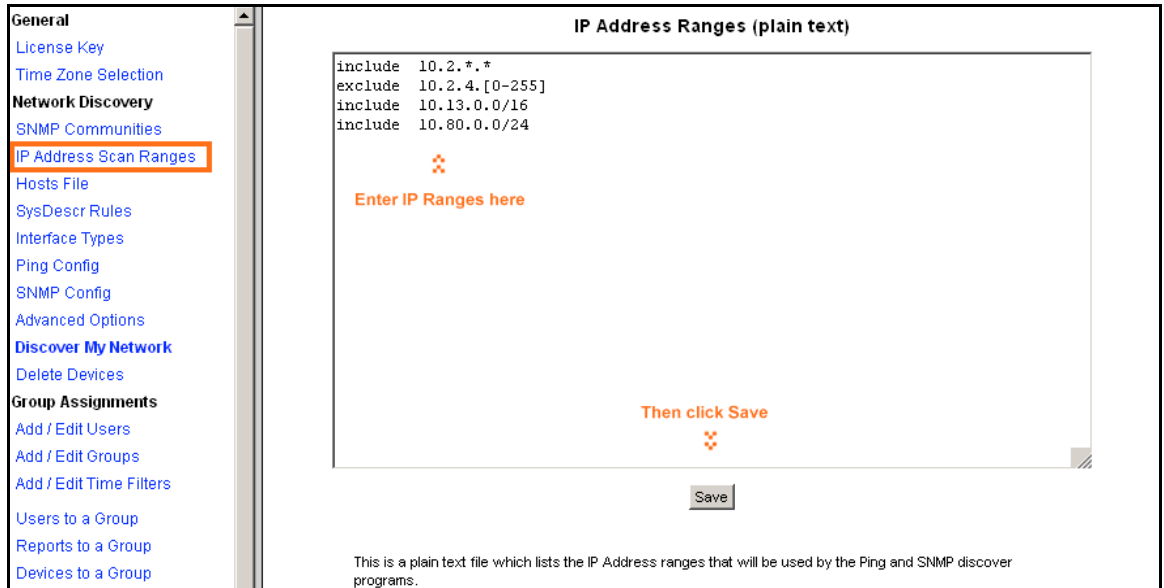
```
IPAddress {one or more spaces} hostname
```

Example

```
10.1.1.1 router1
10.1.1.4 switch1
```

4. If you are using a Discover Range to search for devices either in addition to the hosts file or instead of the hosts file, from the menu select **IP Address Scan Ranges** and enter the ranges of IP addresses you want to include or exclude.

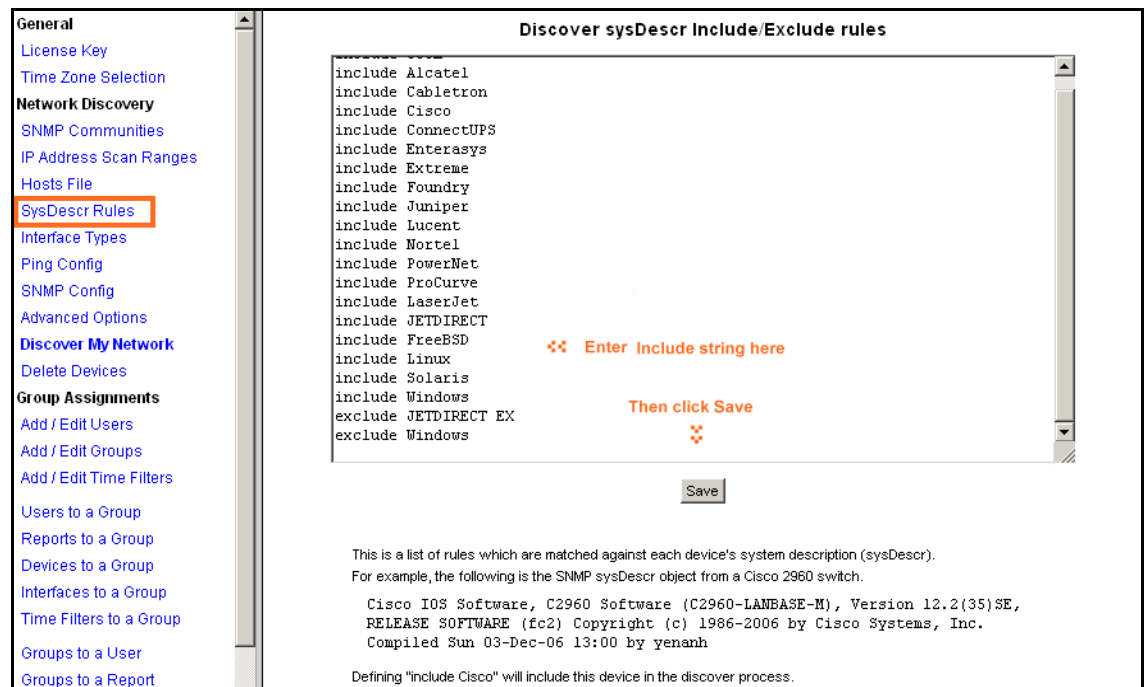
Here is an image of the Discover Ranges screen. Notice that you can include and exclude ranges to scan. Also note the different ways that you can enter the IP addresses using regular expressions, wildcards, and netmasks.



Make sure that IP ranges fall on a natural subnet boundary. Also, be careful that you do not include massively large network ranges (for example, 0.0.0.0/0) since this will require an extremely long time to perform the scan. Although not shown, lines starting with a hash (#) character will be ignored.

When scanning the network, Statseeker will specifically include and exclude devices in the configuration based on the device type. When a network device responds to the SNMP request, it includes the SNMP sysDescr object in its reply, also known as a system description. Statseeker compares the SNMP sysDescr object against a preconfigured, editable list of devices that should be included and devices that should be excluded. The list of included and excluded devices can be seen and edited in SysDescr Rules from the Administration Tool menu. The default list covers most network manufacturers, server operating systems, printers, and UPSs.

This screen capture shows a sample of rules for including and excluding devices.



5. The last configuration step that you may want to perform prior to discovering the network devices is to specify the network interface types that you want to track. This can be performed from the **Interface Types** menu.

Numerous types of interfaces exist on many different types of network devices. For the purposes of network rightsizing, you will be primarily interested in ethernetCsmacd interfaces. You can add or remove interface types from this list if you desire, though typically changes are not required.

At this point, the preliminary setup has been completed and you are ready to perform the initial scan of the network. Before you begin scanning the network, it is important to realize that Statseeker will display and list your network devices based on the SNMP information that is entered on each of them. It will be easier to *identify and group* the devices if this information was carefully entered using a consistent naming convention. If the information was entered haphazardly, then it will be more difficult to identify and locate the devices. This will be important in later steps such as network consolidation.

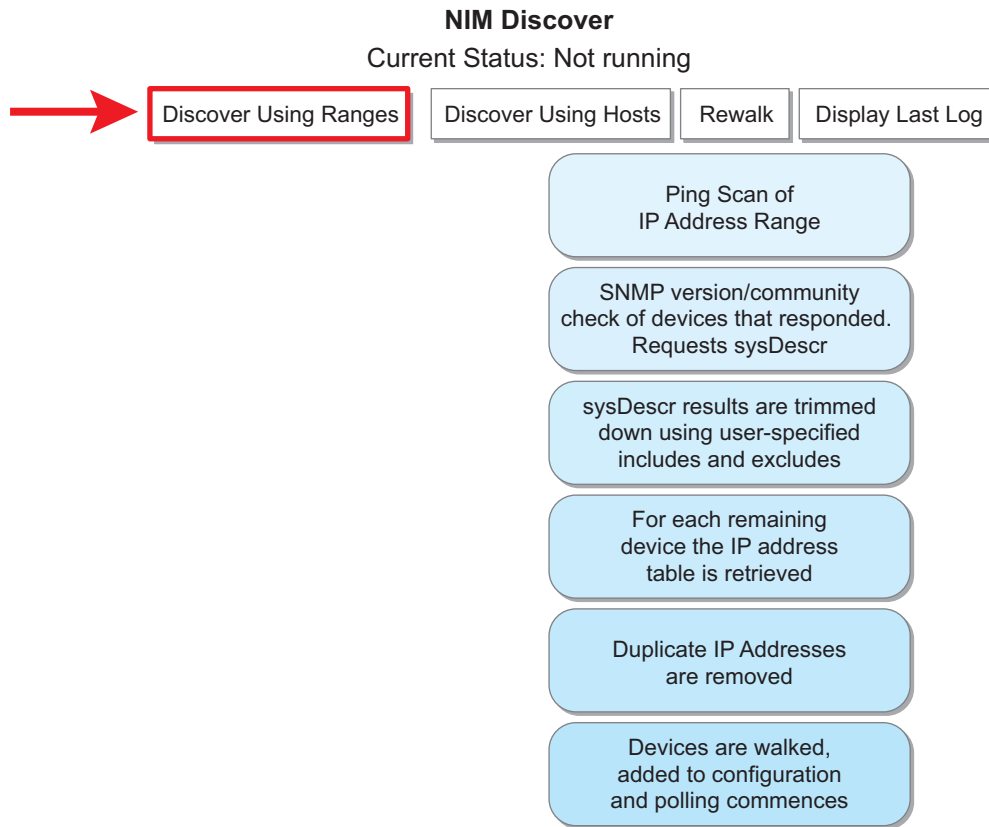
Discovering Devices on the Network

1. From the Administration Tool menu you can now select **Discover My Network** to display the Network Infrastructure Monitor (NIM) Discover options.

or

If you choose **Discover Using Ranges**, Statseeker will first perform a PING scan of the network. Then, based on the responses back from the PING scan, Statseeker will attempt to communicate with the discovered devices using each of the SNMP community strings that you entered. The sysDescr object of each identified device is checked against the SysDescr Rules to determine if the device is to be included or excluded. For the remaining devices, the ones that will be monitored in Statseeker, IP address tables are retrieved and duplicate IP addresses are removed. Statseeker now has the list of devices, but doesn't have information for the devices yet. Using SNMP, Statseeker will now SNMP-walk each device, add it to the configuration, and begin scheduled polling of the devices. The default polling interval for Statseeker is every 60 seconds.

Below is a flowchart of Statseeker's discovery process for the network using IP address ranges.



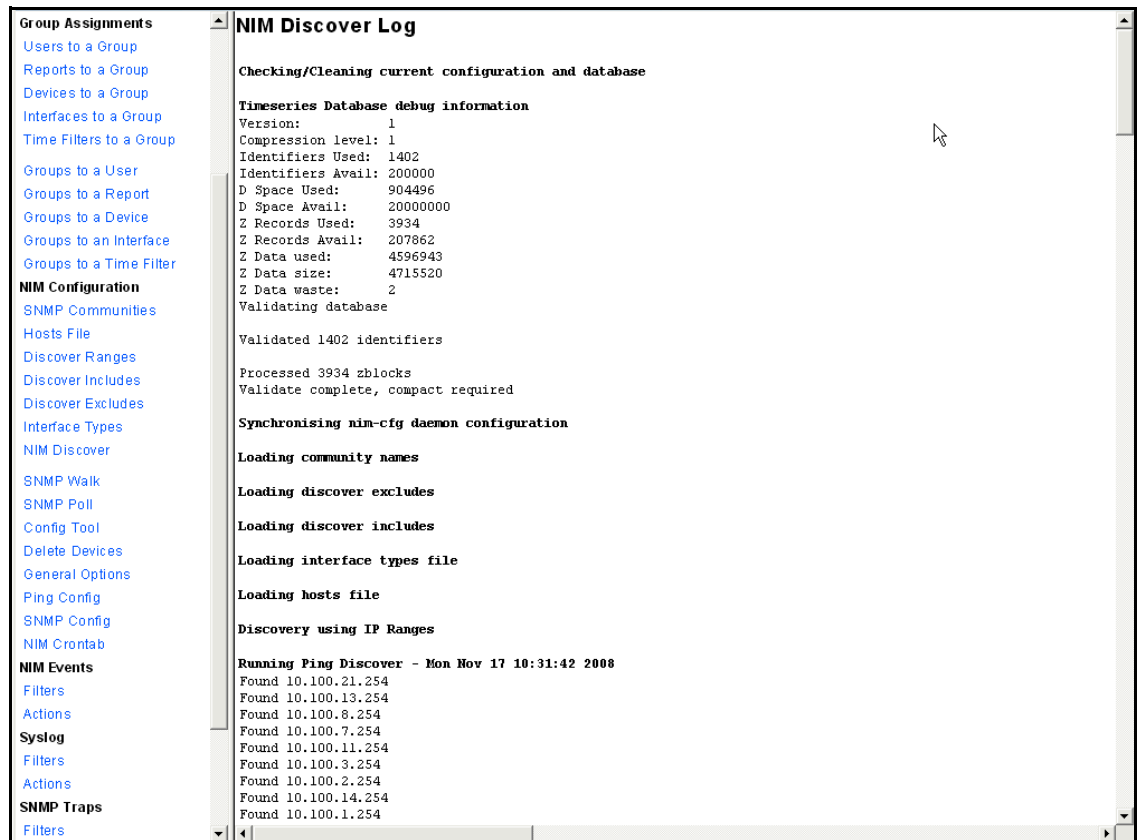
NRBPG_234

If you are discovering the devices using the hosts file, the process is identical, with the exception of the initial PING scan. Since you are providing a list of networking devices, it is not necessary to scan for them.

It should only take a few minutes for Statseeker to completely poll your network. The actual time will depend on the size of your network, though Statseeker estimates that it takes five minutes to discover a network with up to 5,000 devices and 100,000 interfaces. By default, a daily 11 A.M. process is performed to discover new devices and update the device database with any changes.

After Statseeker performs the initial discovery of the network, either by scanning the IP address ranges or by using the hosts file, review the log to determine if any scanning problems occurred.

- The Discover Log can be displayed by clicking the **Display Last Log** button, which is directly to the right of the buttons you clicked to perform either scan. The output of the discover log displays each task as it was performed, as well as a listing of the devices that were discovered and scanned using PING and SNMP. The screen capture below displays just the first portion of the log file after a Discover Using Ranges was performed. Reviewing this log will help you identify devices that are not responding to SNMP queries, often due to misconfigured community information.



```
Group Assignments
Users to a Group
Reports to a Group
Devices to a Group
Interfaces to a Group
Time Filters to a Group
Groups to a User
Groups to a Report
Groups to a Device
Groups to an Interface
Groups to a Time Filter
NIM Configuration
SNMP Communities
Hosts File
Discover Ranges
Discover Includes
Discover Excludes
Interface Types
NIM Discover
SNMP Walk
SNMP Poll
Config Tool
Delete Devices
General Options
Ping Config
SNMP Config
NIM Crontab
NIM Events
Filters
Actions
Syslog
Filters
Actions
SNMP Traps
Filters
```

NIM Discover Log

Checking/Cleaning current configuration and database

Timeseries Database debug information

Version: 1
Compression level: 1
Identifiers Used: 1402
Identifiers Avail: 200000
D Space Used: 904496
D Space Avail: 20000000
Z Records Used: 3934
Z Records Avail: 207862
Z Data used: 4596943
Z Data size: 4715520
Z Data waste: 2
Validating database

Validated 1402 identifiers

Processed 3934 zblocks
Validate complete, compact required

Synchronising nin-cfg daemon configuration

Loading community names

Loading discover excludes

Loading discover includes

Loading interface types file

Loading hosts file

Discovery using IP Ranges

Running Ping Discover - Mon Nov 17 10:31:42 2008

Found 10.100.21.254
Found 10.100.13.254
Found 10.100.8.254
Found 10.100.7.254
Found 10.100.11.254
Found 10.100.3.254
Found 10.100.2.254
Found 10.100.14.254
Found 10.100.1.254

Now that Statseeker has completed a discovery of the network, the Network Infrastructure Monitor (NIM) Console should be populated with a list of all of the devices on your network. Statseeker will scan each of these devices and interfaces every five minutes, collecting the information and making it available to be viewed through the NIM.

Port Usage and Utilization

After Statseeker or another network monitoring program is running, you need to let it collect data for a minimum of two weeks in order to isolate time-of-day or out-of-office anomalies. This also ensures that the majority of the user population is sampled. If you are using a program other than Statseeker, make sure that it is capable of tracking and displaying port utilization, in addition to being able to identify the ports that have been or have not used for a given edge device.

Once Statseeker collects sufficient data, you will next turn to data analysis. To start, check to see how many total network interfaces have been scanned, and how many show no network activity during the period. This can easily be done from the NIM Standard Console.

1. In the Report List area, under the Interfaces section, select **Usage**.

Here you will see a list of all of the Interfaces that you have discovered on your network. In the top header area, you will see the total number of interfaces, how many are used, and how many are free. The report shows all of the devices and lists each one with the interface totals for the time Statseeker has been scanning the network, up to the past 90 days. At the top of each column, you can sort the list by clicking on the up or down arrows.

Interfaces Used/Free			
Wed 14 Oct 2009, 17:23 (America/Los_Angeles)			
Report is based on last 90 days of data			
Total: 317, Used 141, Free 176			
Device	Total	Used	Free
▲ ▼	▲ ▼	▲ ▼	▲ ▼
SUP1-B	26	1	25
A2400-A	26	1	25
core4	38	15	23
warehouse-ethersphere	26	5	21
orion	26	9	17
local-beijing-02	26	14	12
SUP1-A	26	16	10
OPS2400	26	16	10
A800-A	9	1	8
voyager	26	20	6
A3600-A	4	1	3
apollo	4	1	3
A3200-A	4	1	3
A3400-A	4	1	3
shanghai-2400-01	26	24	2
viking	4	2	2
M3-A	12	10	2
A200-A	2	1	1
pathfinder	1	1	0
vpnsrvr	1	1	0

The total number of used and unused ports is valuable for quickly assessing network utilization; however, you need to collect more detail to see what specific ports and switches are unused or underutilized with respect to your edge devices. This will be the primary determinant of switch consolidation candidates. In order to do this you will want to first group your edge devices in Statseeker so that your searches are focused on only those devices.

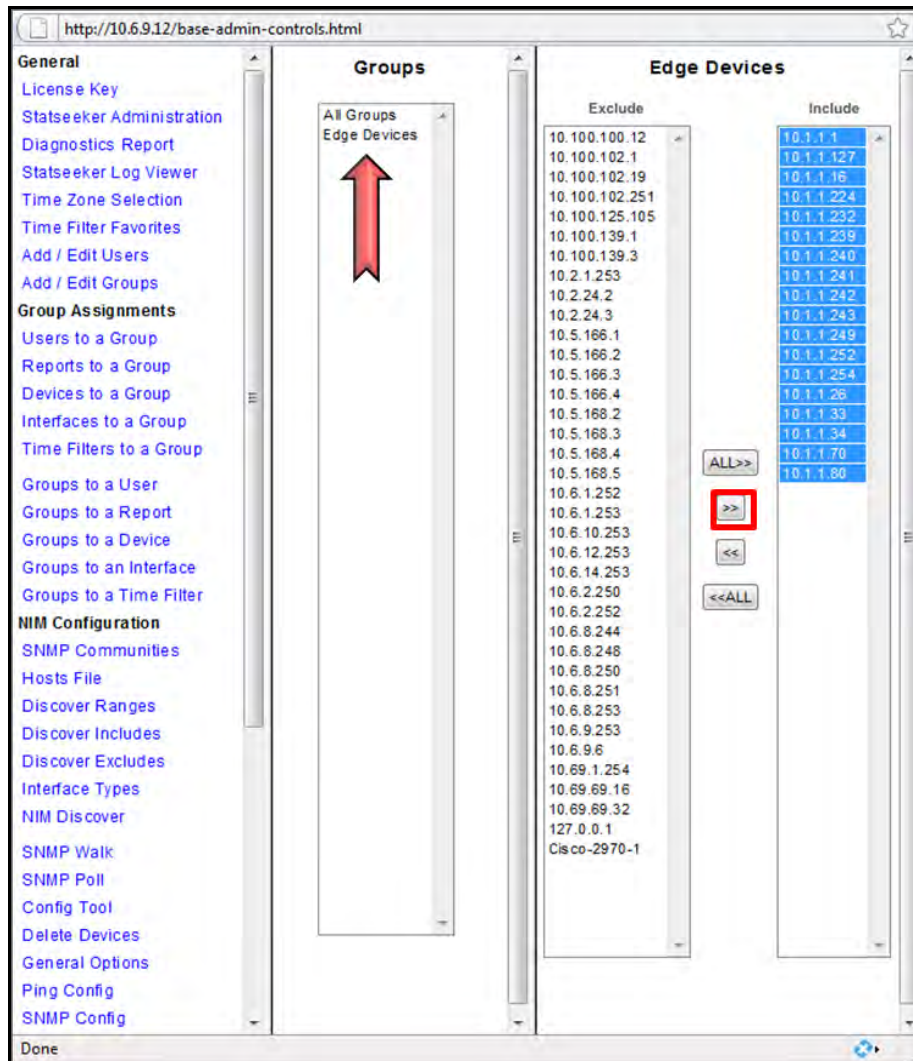
2. From the Administration Tool, under the General area, select **Add/Edit Groups**.
3. After you enter a name (such as Edge Devices – Location1) for this group, click the **Add** button.
4. Now under the Group Assignments header, select **Devices to a Group**, click the group name that you just created, and select the devices that are in the Exclude column. Use the right arrow to move them to the Include column.

Once you have put all of your edge devices into the appropriate group you can easily perform reporting solely on that group of devices.



It is strongly recommended that you group devices by location, and if possible sub-group them by closet.

This will simplify the switch consolidation step. This information will also be used as the baseline from which future cost savings will be confirmed in the Validate phase. The screen capture below shows a group named Edge Devices and a list of devices that are included in that group.



You are now ready to run a detailed report of your interfaces to identify the unused ports. You will generate this report from the NIM Advanced Console.

- Begin in the Group Filter column by selecting the group that you want to analyze, in this example the Edge Devices group. Then in the Report List area under Interfaces, select **Reporting Tool**.

In a moment the Advanced Interface Reporting Tool window appears with a listing of all of the Interfaces, as well as the Time Filter, General Options, and Graphing Options sections so that you can specify the exact parameters you want to report on. Since you want to identify unused ports, for the initial analysis the Time Filter should be left blank in order to view all of the data that has been collected.

On larger networks it may be difficult to maneuver around the menus and analyze individual ports on thousands or tens of thousands of devices. Statseeker provides the ability to copy the data file that contains the statistics used to generate the 90-day usage report mentioned in the previous section. The name of the file is `/home/statseeker/nim/tmp/interface-if-stats-90d`. This data file is a comma-separated file, which contains the following 19 fields:

- Value 1: Device Name
- Value 2: Interface Index

- Value 3: Interface Name
- Value 4: Total Number of In Byte
- Value 5: Total Number of Out Byte
- Value 6: Average In Bits per second
- Value 7: Average Out Bits per second
- Value 8: Average In Utilisation
- Value 9: Average Out Utilisation
- Value 10: Total Number of In Packets
- Value 11: Total Number of Out Packets
- Value 12: Total Number of In Errors
- Value 13: Total Number of Out Errors
- Value 14: Total Number of In Discards
- Value 15: Total Number of Out Discards
- Value 16: Percentage of In Packets that had Errors
- Value 17: Percentage of Out Packets that had Errors
- Value 18: Percentage of In Packets that were Discarded
- Value 19: Percentage of Out Packets that were Discarded



Do not modify the copy of the file on the Statseeker server.

Since the Statseeker server is running on Linux, you can log on to the server and copy this file to another computer. Once you have copied it to another computer, the file can be imported into a spreadsheet or database application, where you can more easily sort the data or search for specific criteria.

Statseeker has developed a custom rightsizing script file for Aruba in order to provide even more information than is available in the interface-if-stats-90d file. The script 90d.pl combines the output of the interface-if-stats-90d file and adds five more fields to the file:

- Value 20: ifTitle
- Value 21: ipaddress
- Value 22: sysDescr
- Value 23: sysLocation
- Value 24: sysContact

On request, Aruba can provide a copy of this script. To use it, simply copy it to the Statseeker server in /home/statseeker directory and run it as ./90d.pl.

When you copy the file to the server, make sure that the transfer mode is set to ASCII and not binary. After it is copied, you will also need to make it executable by issuing the command “chmod +x 90d.pl”.

The name of the output file will be */home/statseeker/interface-if-stats-90d-extra.csv*.

Since several of the extra fields may contain commas, the fields are quoted. The five extra fields provide additional information that should help identify and locate the switches on your network.

Traffic Analysis

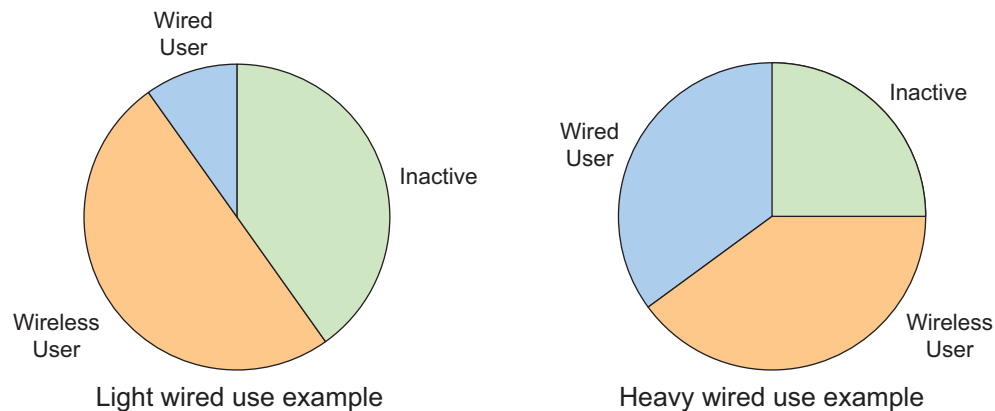
Traffic analysis helps determine which active wired users can be safely migrated to wireless as their primary least-cost access method with no loss of performance. There are two parts to Traffic Analysis: creating a list of user categories specific to your unique environment, and assigning employee populations to those groups. The step after this—Network Consolidation—will leverage this information to quantify infrastructure changes at the closet level.

User Categorization for Rightsizing

Ultimately, the rightsizing process comes down to assigning each of your current network ports to one of three groups:

- Inactive
- Active user – good candidate for rightsizing
- Active user – required wired connection

To use the Aruba Rightsizing Calculator discussed later in this chapter, you will first need to assign users into these three categories. The first group should be evident following a review of the infrastructure data gathered in the previous step. Here are some examples of how different customers may assess their user bases:



But how do you decide whether a user on an active port is a good candidate for rightsizing or requires a wired LAN connection? There are three basic methods you can use to answer the question.

- Method A – Assign by usage type or job function
- Method B – Assign by port utilization
- Method C – Assign by network traffic analysis

Generally speaking, the first two methods are the most commonly used primary classification tools. Traffic analysis is typically reserved for custom applications that are not well documented or for users whose port statistics appear borderline and hence more investigation is warranted. You should choose the method that is most comfortable for the management style of your organization and the available resources on the IT team. The good news is that no matter which method(s) you choose, the majority of wired ports will use far less network capacity than is available from your current access-layer switches.

Method A – Assign by Usage Type or Job Function

The simplest method is to identify the specific users that require wired connections by either their usage type or job function. This should be straightforward for the IT staff because they already understand the types of applications in use.

Every organization has groups of users with similar network needs. The network demands of the applications used by these groups are fairly constant. By analyzing network traffic, either individually

or by groups of users, you can determine the demands imposed on the network by different applications. Groups such as laptop users, Internet and email users, Web application users, and office-productivity application users are all likely candidates to be moved from wired to wireless networks.

Laptop users deserve special attention. As stated in [Chapter 1 on page 7](#), laptop usage is growing fast as a percentage of total users. Network utilization by laptop applications tends to be low, making laptops connected to wired ports excellent prospects for migration to 802.11n networks. And network rightsizing is the vehicle that will pay for it because freeing wired ports also frees funds that can be diverted to the 802.11n deployment.

By contrast, some groups are better served by remaining on a wired LAN connection by virtue of the network access requirements. These groups include heavy computation or visualization software users, thick client users with heavy data base access, and software developers.

Another way to define candidates for migration is to look at a user's job function. Typical job functions with minimal network access requirements that are excellent candidates to migrate to wireless as their primary connection include:

- Managerial employees in most company departments
- Salespersons
- Clerical and administrative assistants

Job functions that are less likely to be moved from wired to wireless because of their heavy network utilization or time-sensitive application requirements include:

- Graphic artists
- Video editors
- CAD/CAM designers
- Data base developers

Most of this analysis has centered on data-only users. Some IT departments will be open to migrating voice users to VoWi-Fi handsets and decommissioning the associated wired switch ports, while others will not be so receptive. The same is true for IPTV applications. The bias of the IT staff will significantly impact the percentage of users that can migrated to wireless and the network architecture required to support high density voice and video clients. The considerations need to be factored in during the evaluation stage.

Regardless of the approach taken, the Usage Type or Job Function method, you need to be able to identify the ports to which users are connected to so that unused or soon-to-be-unused ports can be decommissioned after the rightsizing transition.

Method B – Assign by Port Utilization

An alternate method of assessing ports is to leverage the network port utilization data described above and then apply across-the-board filters in Statseeker (or alternate software tool) to identify groups whose network usage falls below a targeted threshold.

A single 802.11n radio can support at least 25, and in some cases more than 50, client devices depending on usage patterns. Aruba has measured aggregate application-layer per-radio throughput of 170Mbps or more with this number of clients. By simply dividing 170 by 25, we arrive at a reasonable threshold target of 6.8Mbps per user. To run a detailed report in Statseeker that identifies all the ports that fall below this level of use, follow these steps:

1. From the Statseeker Advanced Console screen, highlight the appropriate devices from the Device Filter list. All devices that have been added to Statseeker for monitoring should be listed here. In the Report List column on the far left of the screen, click the **Reporting Tool** selection under the Interfaces heading.

2. After the Advanced Interface Reporting Tool screen opens, the Interfaces column should be pre-populated with all the interfaces from the devices selected in the previous step. Select all the interfaces in the list, or select specific interfaces for which the report should be run.
3. In the Time Filter section on the right of the page, choose a time range to run the report against. You have the option of choosing a common pre-defined range from the **Favorites** drop-down list, or you can specify a custom time frame in the Range section.
4. Next, move to the General Options section in the middle of the screen. In the Report Type drop-down menu, select **BitsPerSecond**. For the Database Type, select **Total**. The Interval section defaults to one minute, but can be extended as high as one day.
5. Click the **Report** button at the bottom of the page to generate your report.
6. The Interfaces Reporting Tool output shows the transmit and receive bits-per-second totals, in one minute intervals, for the devices/interfaces selected in previous steps.

Interfaces Reporting Tool - BitsPerSecond			
Wed 14 Oct 2009, 20:25 (America/Los_Angeles)			
Mon Sep 14 00:00 2009 to Wed Oct 14 20:25 2009			
Device	Interface	Rx Bps	Tx Bps
▲ ▼	▲ ▼	▲ ▼	▲ ▼
shanghai-2400-01	fe1/0	150.3M	247.8M
shanghai-2400-01	fe1/1	5.7G	5.4G
shanghai-2400-01	fe1/10	172.8M	2.5G
shanghai-2400-01	fe1/11	404.8M	1.8G
shanghai-2400-01	fe1/12	28.7M	62.8M
shanghai-2400-01	fe1/13	196.0M	56.8M
shanghai-2400-01	fe1/14	79.8M	70.1M
shanghai-2400-01	fe1/15	124.8M	52.3M
shanghai-2400-01	fe1/16	89.5M	67.7M
shanghai-2400-01	fe1/17	851.3M	4.4G
shanghai-2400-01	fe1/18	422.5M	4.6G
shanghai-2400-01	fe1/19	30.9M	56.0M
shanghai-2400-01	fe1/2	24.3M	144.6M
shanghai-2400-01	fe1/20	33.5M	59.1M
shanghai-2400-01	fe1/21	11.3G	1.0G
shanghai-2400-01	fe1/22	5.5G	1.9G
shanghai-2400-01	fe1/23	4.0G	7.6G
shanghai-2400-01	fe1/3	128.0K	2.3M
shanghai-2400-01	fe1/4	79.5M	69.2M
shanghai-2400-01	fe1/5	13.3M	50.8M
shanghai-2400-01	fe1/6	24.5M	62.1M
shanghai-2400-01	fe1/7	164.7M	55.1M
shanghai-2400-01	fe1/8	84.1M	73.8M
shanghai-2400-01	fe1/9	16.3M	292.2M
shanghai-2400-01	gig1/24	0	0
shanghai-2400-01	gig1/25	0	0
orion	FE 1/0	196.4M	131.0M
orion	FE 1/1	160.8M	95.5M
orion	FE 1/10	0	0
orion	FE 1/11	0	0
orion	FE 1/12	0	0
orion	FE 1/13	0	0
orion	FE 1/14	0	0
orion	FE 1/15	0	0
orion	FE 1/16	0	0

You will now need to sort the data (or export them to a spreadsheet program) to determine which ports are between a given data utilization range.

Network activity is not consistent and uniform throughout the day, week, month, or even the year. As a result, it is important to factor in changing client demands over time when using the port utilization method. Within every organization, trends will show variability in client usage during certain times of the day, days of the week, and seasons of the year. It is important to recognize these trends and plan the design of your network accordingly. As mentioned earlier, it is essential to monitor the network for a minimum of two weeks and ideally at least four weeks to take usage variability into account. Depending on the type of organization, the time of year chosen for the assessment is also critical. For instance, universities should be evaluated when classes are in session, and retailers should be monitored during the fourth calendar quarter when business is at its peak for the year.

Method C – Assign by Network Traffic Analysis

It may be desirable to complete a network traffic study for specific user populations, especially when there are custom applications whose load characteristics are not well documented. Traffic studies are also useful for deciding whether borderline cases are better served over a wireless or wired network.

Using packet analysis software, you can determine what type of traffic is being sent across the network, how much traffic is being sent, and how long it takes to send that data. By selecting a few typical users and then analyzing their traffic, these data can be used to estimate the load presented by a group or type of applications, and the resources necessary to support them.

Network Consolidation

The transition of wired users to the wireless network provides an opportunity to decommission unused wired ports. How best to consolidate the wired network and decommission the unneeded ports and switches will vary between organizations. Before you consolidate the network connections, check the VLAN and network configurations on the switches, ensuring that the users that are migrated are connected to the correct ports and VLANs, and that the necessary VLANs are trunked and properly tagged.

Closet Layout

The design of your network and your closet layout will affect the consolidation of ports and switches on your network. After transitioning users from the wired network to the wireless LAN, cost savings will be tied to decommissioning unneeded ports, consolidating the ports that are needed onto a smaller number of switches, and removing the switches that no longer have active network connections. This process works best if your IDF closets are centralized and contain many switches. If you transition 40% of your wired users to the wireless LAN, and your IDF contains 10 switches, then you will be able to decommission four of the 10 switches in that closet. However, if each of your closets contains only two or three switches, there may be insufficient unused ports to permit a switch to be decommissioned. For IP voice devices that are to remain wired, these devices could be aggregated onto a common switch or switches, or distributed across remaining switches if desired.

During the planning process, you need to identify and document the layout of your wiring closets to determine how they will be affected by rightsizing your network.

Stacked Switches

Consolidating networks with stacked switches is straightforward: connections that are no longer needed can be disconnected from the switches, the remaining connections can be consolidated onto other switches, and unused switches can be removed from the rack. It is recommended that the oldest switches be removed first, and this may require moving new switches from one closet to another to replace older switches that have been taken out of service. Unused switches can either be scrapped (recycled) or used as spares. Be sure to discontinue any maintenance contracts on unused access switches, or even discontinue contracts for actively used switches and rely instead on using the extra switches as spares.

Blade Switches

Network consolidation with blade switches begins in the same way as with stacked switches. Connections that are no longer needed should be removed from the switches, and the remaining connections consolidated among the remaining blades. The port density of these switches and chassis—and their locations—will determine how equipment should be decommissioned. If there are multiple chassis within one closet, blade consolidation may permit the removal of one or more entire chassis. At a minimum, unused blades can be removed — decreasing power and cooling requirements — and used as spares.

802.11n Implementation Plan

There are three primary 802.11n wireless LAN installation scenarios. Greenfield installation¹ is the most flexible scenario as there is no legacy infrastructure with which to contend. Aruba's RF planning tool can be used to estimate the placement of access points. Once the APs have been installed, Adaptive Radio Management (ARM) will fine tune AP and client operation to dynamically optimize performance, maximize coverage, and minimize the effects of interference.

The second scenario entails upgrading an existing 802.11a/b/g network to 802.11n. In an upgrade installation, the existing APs are removed and replaced with new high-throughput 802.11n APs either network-wide or in specific areas that require higher throughput or capacity. Aruba's AP 12x and AP 105 families of access points can be cabled to the network using standard 10/100/1000 Ethernet cables and support either 802.1af PoE or PoE+, allowing you to reuse existing cabling and PoE infrastructure. Aruba's RF planning tool should be used to determine the optimal AP count and placement.

Regardless of which scenario you choose to implement, having an understanding of some key Wi-Fi fundamentals will aid in the design of a rightsized wireless LAN.

Capacity Planning

The design of a rightsized wireless LAN should be based upon network capacity, coverage, and utilization. The goal of a capacity-based, or “dense”², design is to ensure the universal availability of a minimum data rate throughout the installed area, for every device and for every application. APs can support a finite number of clients simultaneously at a given data rate, and therefore dense designs need to take into account the number and types of clients in the coverage area, as well as the bandwidth and quality of service demands of applications and protocols that will be running. Doing so will ensure that the rightsized network can handle the needs of your users and applications.

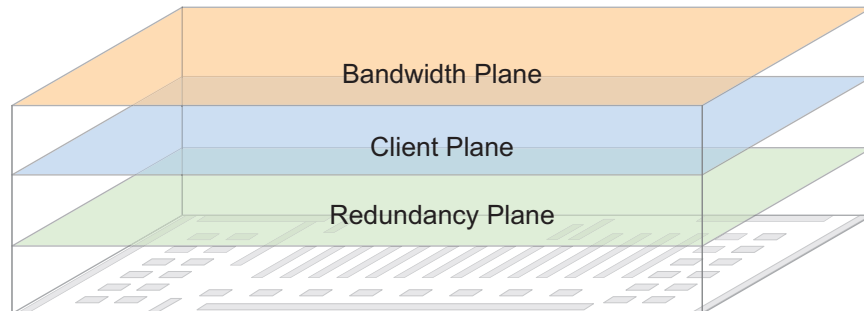
The wireless LAN controller manages service levels for three types of RF-related variables on a continuous basis for all of the APs in a given three-dimensional area:

1. Managing bandwidth to meet a uniform minimum data rate or SNR target
2. Managing clients to hold peak device loads below a per-AP or per-SSID target maximum
3. Managing redundancy to ensure uninterrupted minimum RF signal coverage

While all three of these factors are interrelated, the AP density required to maintain each one within expected tolerances is unique. The number of APs needed to achieve a target bandwidth can be higher or lower than the number of APs needed to serve a particular population of users. The greater of these two numbers then needs to be increased by an overlap factor to assure redundancy. For each wireless coverage zone, there is a minimum density of APs that allows all three service levels to be successfully met by a wireless controller

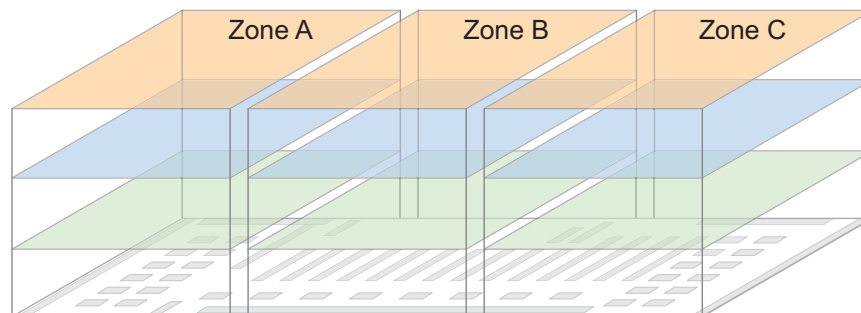
-
1. This is not to be confused with “802.11n Greenfield Mode,” which is not supported today by most WLAN infrastructure.
 2. A “dense” deployment uses a microcell architecture to cover an area using overlapping APs at relatively low transmit power. This design strategy enables Adaptive Radio Management (ARM) to detect and close coverage holes in the event of an AP failure by increasing power on neighboring APs. Smaller cells also help facilitate proper load balancing of voice over WLAN callers.

Bandwidth, client, and redundancy density may be thought of as logical RF planes or layers that are managed by the WLAN controller in real time, using a single physical pool of thin APs for a given coverage area. This concept is depicted in the figure below. Each of the three planes requires a minimum AP density to achieve a target service level. Using this conceptual approach provides the wireless engineer with a clear way to describe and compute these densities. RF planes may also interact with one another, such as when increased client demand reduces overall bandwidth, or when a failed AP temporarily reduces client capacity in that area.



NRBPG_125

A coverage zone can be an entire facility, or a single facility may be subdivided into multiple zones to accommodate different requirements in each one, as seen in the following graphic. Whether you are designing for one zone or many zones, you still need to be concerned with providing enough coverage density for each of the RF planes.



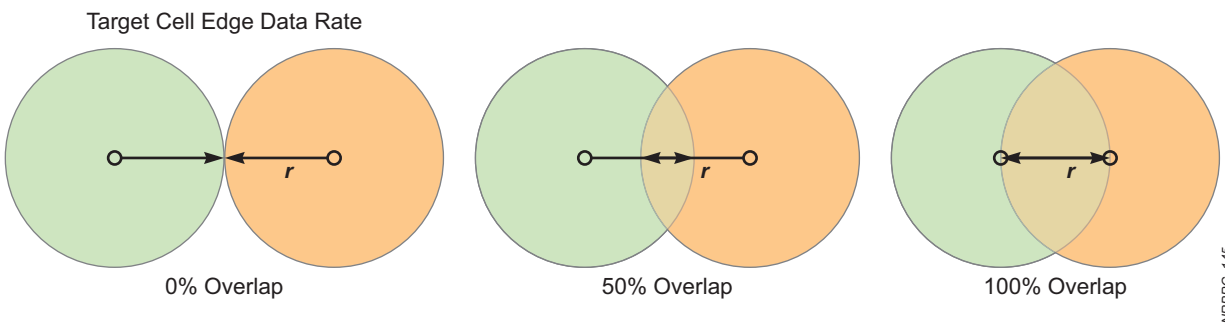
NRBPG_126

The bandwidth plane is engineered so that a targeted minimum data rate is available throughout the coverage zone. The Aruba WLAN controller dynamically adjusts RF settings to provide the minimum data rate with the available installed APs. To achieve this objective, controllers must select the optimal channel and power settings for each AP and radio on an ongoing basis as ambient RF conditions change. For dual-radio APs, the controller does this for both 2.4 GHz and 5 GHz frequency bands, ensuring that the maximum designed capacity of each band is available at all times. To create roughly equal physical cell sizes for the two radios, the WLAN controller reduces the transmit power of the 2.4 GHz radio by 6dB (roughly 75%). This compensates for the decreased coverage area that typically exists with a 5 GHz network due to greater free space path loss caused by the higher 5 GHz frequencies.

The goal of the client plane is to maintain an acceptable client density level. Client capacity is generally expressed as a maximum number of client devices per AP per radio. Each access point is capable of providing a finite level of throughput. If too many clients connect to one AP, it may not be able to handle the load that the clients are requesting. Aruba WLAN controllers can perform load balancing to spread client density peaks across multiple APs and even across multiple RF frequency bands or channels. In an Aruba WLAN, all of the APs that service each coverage zone work together as a system to maximize the performance of the client devices. For planning purposes, wireless designers generally assume that the targeted minimum data rate is distributed uniformly throughout each cell.

The goal of the RF redundancy plane for a coverage zone is to provide a specific level of cell coverage and overlap. The Aruba RF Planning tool defines “overlap” as a percentage of coverage. It is measured

as the percentage of the RF coverage area. 0% coverage overlap¹, as seen in the graphic below, will fail to meet the minimum data rate target in the event of an AP failure. A coverage area with 100% coverage overlap will maintain the minimum target data rate even if an AP fails. Coverage overlap of greater than 0% is necessary for smooth roaming. Aruba recommends a minimum of 25% coverage overlap, even if no RF redundancy is desired.



In addition to providing a specific level of cell coverage, RF Redundancy also refers to the ability of a wireless LAN to continue to provide service throughout a target area in the event of an AP failure, temporary obstruction of the RF signal, or presence of narrowband interference. Aruba also uniquely can adjust to high overlap conditions and turn AP radios into Air Monitors until more coverage is needed, then revert back to APs.

Customers purchase WLAN controllers with the expectation that they will automatically balance and enforce each of the bandwidth, client, and redundancy density objectives simultaneously without administrative intervention. Each controller must have enough APs to work within the coverage area to successfully achieve the goals set by the wireless designer. Therefore, the proper AP density for a thin AP deployment is determined by computing the bandwidth, client, and redundancy density for a given coverage zone and selecting the larger of the three values. This process is repeated for multi-zone deployments. Aruba offers planning tools such as RF Plan and AirWave VisualRF that will allow you to design and manage your network based on your specific requirements.

Aruba RF Plan

Now that you are familiar with some of the key parameters and concepts needed to design an 802.11n wireless LAN, you will learn how these parameters are used when designing a network using the Aruba RF Planning Tool. The first step is to go to the Download Software section of the Aruba support site to ensure that you have the latest version of the RF Planning Tool. You should also download the *RF Plan: Installation and User Guide*, which describes in detail how to install and use the RF Planning Tool. Study the guide to familiarize yourself with the RF Planning Tool before designing your network.

In this section we will review the RF Planning Tool's AP Modeling settings, which encompass the bandwidth, client, and redundancy planes used to determine the required number of access points. The AP Modeling settings allow you to change the radio properties, total users, users per AP, and overlap factor, and see how these variables affect the total number of required APs. The steps below will take you through the initial configuration to a point where you can see and modify the AP Modeling settings.

1. After you have downloaded and installed the Aruba RF Planning Tool, begin the planning process by selecting **Aruba RF Plan** from the **Windows** menu.

When the RF Planning Tool loads, you are presented with a blank white window split vertically into two sections. The smaller section on the left will list your campuses, buildings, and floors as you create them, and the section on the right will display the object that you currently have selected.

You begin planning a network by first creating or adding a campus.

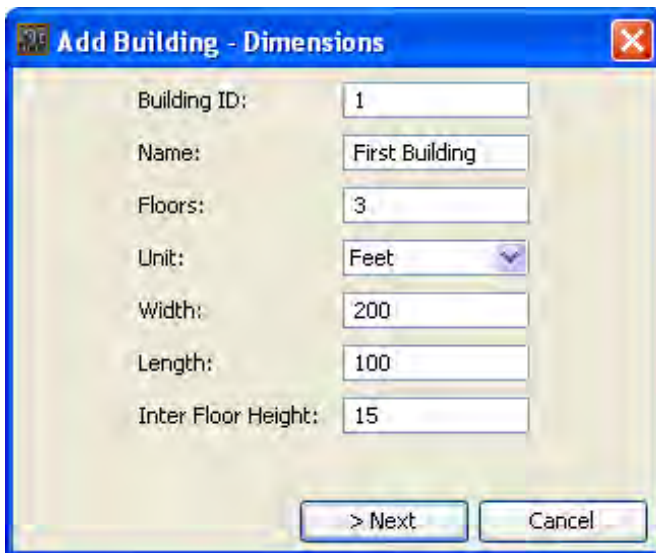
1. Aruba's RF Plan uses a 100–200% scale rather than a 0–100% overlap scale as described in this section.

- From the menu select **File** → **New** → **Campus** → **Add Campus**, and the **Add Campus** dialog box below appears. Name your campus and select the country where it is located, and then click **Ok** to continue.



After you have added a campus, you need to add a building to the campus.

- This is easily performed by right-clicking on the campus and selecting **Add Building**, then filling out the initial dialog box with the building name, number of floors, and appropriate building dimension information. The Add Building - Dimensions window is shown below. This is the first of three very important screens for creating the wireless design for a building.
- After entering the dimension information, click the **>Next** button and the AP Modeling window displays.



The AP Modeling window, as seen below, has many fields and buttons that can be set to help design your rightsized wireless LAN.

- When designing your rightsized network, you will most likely want to choose the **Capacity** option for the design criteria. This will allow you to more granularly choose the settings and options that will be used as the foundation of your network.
- After you have selected the design criteria, the next settings that need to be made are the selection of the Radio Type and the AP Type. For the **Radio Type** you can choosing to deploy
 - GHz 802.11n with support for 802.11b/g (802.11g+n)
 - GHz 802.11n with support for 802.11a (802.11a+n)
 - Or, both 2.4 GHz and 5 GHz 802.11n with support for 802.11a/b/g (802.11a/b/g+n).

Since in an enterprise environment there is little advantage in operating 802.11n only in the 2.4 GHz, the decision typically is a choice between 802.11a+n or 802.11a/b/g+n. Most companies have legacy clients that operate at 2.4 GHz. 802.11a/b/g+n supports both those legacy devices as well as newer

devices that operate in the preferred 5 GHz band, and from which the greatest benefit will be derived in a rightsized network.

7. In the **AP Type** selection box, choose the type of AP that you intend to install.

Add Building - AP Modeling

Design Criteria

Coverage Capacity Custom

Radio Type: 802.11a|b|g + n Total Users: 5

AP Type: 125 Users Per AP: 5

Overlap Factor: 100% (Low) Overlap Factor Custom Value: 100

Number of APs: 1

5 GHz Radio Properties

802.11a Desired Rate: 6

802.11n (HT) Support

802.11n Desired Rate: 65

Use 40 MHz Channel Spacing

2.4 GHz Radio Properties

802.11b|g Desired Rate: 18

802.11n (HT) Support

802.11n Desired Rate: 65

Use 40 MHz Channel Spacing

No. of Required APs: 3

No. of APs to Support Total Users: 1

No. of APs to Meet Desired Rate: 3

< Previous > Next Cancel

8. You are now at a point where making changes to the RF Planning Tool will affect the bandwidth, client, and redundancy planes. Complete the fields in the dialog box in the following sequence:
 - a. In the Design Criteria section, select **Capacity**.
 - b. When you selected the radio type, 802.11n support was automatically enabled or disabled depending on your selection.
 - c. Making changes to the 5 GHz Radio Properties or the 2.4 GHz Radio Properties sections of the window will affect the number of access points necessary to provide the specified bandwidth requirements.
 - d. You must specify two fields related to the bandwidth plane. The first option is whether you want to use 40 MHz channel spacing, also known as channel bonding. Due to the limited number of channels available in the 2.4 GHz frequency band, it is recommended that you only enable 40 MHz channel spacing in the 5 GHz frequency band.

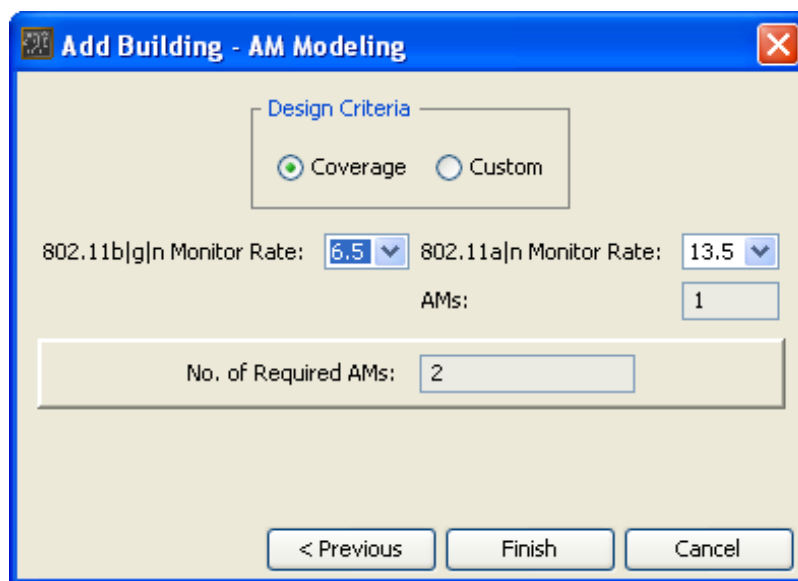
The second option is to choose your desired minimum uniform data rate. Depending on some of the other choices you have made so far, the data rate can be a value ranging from 6.5 Mbps up to 300 Mbps. As this number rises, the number of devices and data throughput that can be supported rise, too. In order to support the higher data rates and smaller cell sizes, the network will require that access points be deployed. As you adjust the data rate in the RF Planning Tool, please note that the No. of APs to Meet Desired Rate: value also changes to indicate the number of APs needed to support the specified bandwidth.

Using the bandwidth plane information, the RF Plan utility calculates two fields that in turn define the capacity of the client plane. These two fields are Total Users and Users Per AP. The RF Planning Tool takes the total users and divides it by the users per AP value to calculate the number of APs that are needed. As you adjusted values in the procedure above, you will have noticed that the No. of APs to Support Total Users: value also changes to reflect the number of APs needed to support the specified number of clients. The RF Planning Tool assumes an evenly distributed density of users throughout the building. Later in this document you will learn how ARM can automatically help to distribute users among different access points when user density temporarily increases due to events such as meetings or presentations.

The redundancy plane is modified by making changes to a single setting, the Overlap Factor. The overlap factor defines the coverage of the access points. A value of 100% means that the wireless network will provide coverage to 100% of the facility with essentially *no overlap* between access points. Aruba recommends an overlap factor of at least 125% to allow the network to provide coverage in areas where the RF signal may experience more attenuation. A value of 150% or greater will provide for better redundancy if an AP fails or is disconnected. As you adjust this value, notice that the number of required APs is adjusted relative to the percentage that you enter in this field. You will enter the number of APs predicted by the tool into the Aruba Rightsizing Calculator discussed later in this chapter.

9. After you have configured the AP modeling parameters, click the **>Next** button to move to the Add Building – AM Modeling window.

The AM Modeling window, as shown here, has very few options to set. Air Monitors are used for wireless intrusion detection, wireless intrusion prevention, and location tracking. In order to perform these and other services, air monitors only need to listen to and monitor 802.11 management frames. By default, 802.11 management frames are transmitted at the lowest supported data rate, and the RF Planning Tool automatically sets the air monitors to this same data rate.



The goal of this section was to explain how the RF Planning Tool parameters can address the three different logical RF planes of bandwidth, client, and redundancy. As mentioned earlier in this section, you should review the *RF Planning Tool: Installation and User Guide* so that you are comfortable with using it to design your rightsized network.

Financial Analysis

The culmination of a successful network rightsizing analysis is a quantitative model of the net cost savings that you can expect to achieve from the project. When analyzing the financial impact of a potential rightsizing initiative, it is important to compare the current and projected capital expenses and operating expenses of your existing networking environment against the projected capital expenses and operating expenses after rightsizing. We recommend that you compare the projected costs for a period of at least three years to understand best how the project will affect your capital and operating expenses.

Aruba has a financial model spreadsheet, the Rightsizing Calculator, that can assist you with performing this financial analysis. Later in this section we will describe the Rightsizing Calculator and some of the key variables that need to be entered to perform the financial analysis. The spreadsheet allows you to input capital and operating expense variables based on your specific environment. The spreadsheet uses your variables and assumptions to automatically calculate the return on investment that you can expect from rightsizing, as well as how many months it will take to pay for the project. Whether you use the Aruba spreadsheet or create your own, there are many different expenses that need to be considered. These expenses are discussed in the sections below.

Building Your Own Financial Model

To better understand the Rightsizing Calculator, let's first review the various types of financial models that must be created in order to arrive at the multi-year Total Cost of Ownership savings from network rightsizing.

Creating Financial Models for Future Capital Expenses

To create a financial model for determining future capital expenses in a Greenfield scenario, you will need to compare the cost of installing cabling and switches to support a traditional wired network design versus the cost of cabling and switches to support a rightsized network. Almost certainly the capital expense savings will outweigh operating expense savings in the near term.

If you are rightsizing an existing network, you will instead need to determine how many current wired ports and switches can be eliminated. Operating expenses will drop as soon as the equipment is removed from service, and future capital expenses will drop because there will be less equipment to purchase during subsequent refreshes. In this case, operating expense savings will typically outweigh near-term capital expense savings.

Creating Financial Models for Future Operating Expenses

There are more variables to consider when building a financial model to calculate projected operational expenses. To begin with, you will need to assess yearly maintenance contract costs for both existing switches and switches required for the rightsized network. You will also need to calculate projected electrical and cooling costs for both the wired network and the rightsized network. Two operating expenses that vary considerably across companies are the cost of adds, moves, and changes to the wired network, and the administrative expense of maintaining and updating equipment. Both categories of expenses will drop in a rightsized network, but the savings will vary based on building construction, the rate of office churn, and the policies regarding maintenance and upkeep.

Projecting Capital Expenses and Operational Expenses for a Pervasive WLAN

The installation of a rightsized network will require the purchase, deployment, maintenance, and operation of a pervasive WLAN. These costs offset the capital and operating savings identified above, and include the purchase and maintenance of Aruba 802.11n access points, controllers, remote access equipment, and network management tools or cloud-based SaaS. In addition to calculating the capital expense of the wireless equipment, you will also need to factor in the additional switches and ports, if any, required to support the wireless LAN and the electrical and cooling costs of the wireless gear.

Computing Rightsizing Savings

After building the financial models listed above, you can easily create a summary model that calculates costs of both the steady-state and rightsized scenarios, taking care to add in the cost of the new pervasive WLAN. In most cases, the savings obtained from rightsizing greatly exceeds the cost of the new 802.11n infrastructure. For example, the California State University System was able to pay for their entire 802.11n upgrade with savings obtained from rightsizing from the legacy wired network. The Rightsizing Calculator integrates the five financial models into a single spreadsheet, allowing you to determine the projected yearly savings and how many months it will take to pay for the pervasive WLAN.

Using the Aruba Return on Investment Calculator

The ROI calculator is an Excel workbook that consists of four integrated spreadsheets:

- *About The Tool* describes the calculator, the theory of operation, and the design principles used to create it;
- *Input & Summary Results* is the main input page and displays a summary of the results;
- *Detailed Results* shows more granular results from the detailed calculations that are derived from inputs on the *Input & Summary Results* page;
- *Editable Defaults* contains a list of default values are used to perform the analysis.



To obtain a copy of Aruba's ROI calculator, email dl-rightsizing@arubanetworks.com.

Once the data are entered, the calculator will estimate the total three-year cost savings from network rightsizing.

The grey cells on the *Input & Summary Results* page contain information about the organization and must be adjusted for each organization. The grey cells on the *Editable Defaults* page contain typical values that apply to most organizations and can be modified as needed to explore other scenarios.

As with most analytical tools, the accuracy of the calculator depends on the data and assumptions that are used in the formulas. [Appendix B, "Key 802.11n Technologies that Enable Rightsizing" on page 61](#) contains a worksheet with fields specific to your organization as well as five key editable defaults that you can modify based on your organization's switching equipment, purchasing, and policy.

The section below will first define the key data required by the *Existing Enterprise Network Environment* section of the calculator.

Existing Enterprise Network Environment Values Section (Input & Summary Results Sheet)

Total # of network Users is the number of network users in your organization. This value is one of the key values used when determining the scope of your network access layer needs and examining options for shifting devices from wired to wireless access.

Size of existing facilities (in square feet) is the total square footage of all facilities. This value is used for estimating the number of access points that will be needed for the pervasive wireless LAN. In North America, the average office building has 200 to 300 square feet per employee.

% of existing facility space with existing wireless coverage (802.11abg) is an estimate of the square footage of all existing areas with 802.11abg wireless coverage. The calculator generates two pervasive wireless LAN investment and ROI values, one based on installing an Aruba 802.11n network throughout every facility and another based on covering only those areas without existing 802.11abg coverage.

Additional % of existing facility space that will be covered by 802.11abg (planned growth) is an estimate of the square footage of all existing area that you currently have planned and budgeted for 802.11 access points. Budgeted money can be applied to offset some of the outlays required for the pervasive wireless LAN.

Average number of adds/moves/changes per year, per employee is an estimate of the number of times each year that the IT department must make a change to the wired network for each employee or network user. This number includes adds/moves/changes due to new hires being added to the network, current employees moving to new offices, and the removal of terminated employees from the network.

% of these moves in which the employee is moved to a new or refurbished space (requiring new cable pulls) is an estimate of the percentage of the adds/moves/changes that will require new cable pulls for each of the next three years. If this number is expected to vary by year, then the cell will direct you to separately enter values for each of the years.

Current average # of ports per user (including common areas, conference rooms, printers, etc.) is the total number of ports for the organization divided by the number of users in the organization. The easiest way to determine the total number of ports is to count and total all of the ports in the wiring closets using a network monitoring tool or a visual count.

% of users capable of shifting to wireless-only for data access is an estimate of the percentage of users whose network data jacks and switch ports can be decommissioned. This value often corresponds closely to the percentage of laptop computers in the organization.

Questions About Typical Costs Section (Editable Defaults Sheet)

The *Editable Defaults* sheet has many variables that you can modify based on your organization. Below are five key variables that you may want or need to modify.

Average cost per switch is the average discounted cost for a 48-port blade or switch. This value is used in the calculations when estimating maintenance costs and when determining the potential savings of decommissioning a blade or switch without needing to replace it.

Average discount off list price for switches (%) is the estimated discount rate that you receive when purchasing blades or switches. Since maintenance fees are typically based on a percentage of the list price of a blade or switch, this value is used with the Average cost per switch to determine the list price of the blade or switch and subsequent maintenance fees.

Average annual maintenance fee for switches (%) is the percentage of list price that you pay for maintaining your switching equipment.

Replacement schedule of switches (for example, 4, 5, or 6 years) defines how often you perform a closet refresh, retiring old switches and replacing them with new ones.

Average cost per cable pull is the estimated cost incurred every time you install another Ethernet cable and jack.

Justify

To the extent that rightsizing may entail near-term investment to obtain longer-term savings, or may significantly change a projected capital expense plan in exchange for changing user behavior across the organization, your executive management will require justification for the project. Justification is the business basis to proceed with the project, and must explain why time, resources, and money should be invested in, and what benefits that will be derived from, the rightsizing project. Justification also includes a corresponding ROI time horizon.

This section reviews some of the key benefits and reasons for rightsizing a network. The cost estimates in this section are calculated from Aruba's ROI calculator. More information about the ROI calculator and actual case studies can be found in [Chapter 7, "Sample Rightsizing Scenarios"](#) on page 51.

Reducing Future Access-Layer Capital Expenses and Maintenance Fees

It is important to remember that every user who is transitioned from the wired network to the wireless LAN represents a potential cost savings at the access-layer. At least one 48-port access-switch or blade can be taken out of service – or not purchased in the case of a Greenfield deployment - every time 48 users are transitioned to the wireless LAN; even more switches can be decommissioned if there are multiple Ethernet drops per user. If you are rightsizing an existing network, then the capital savings will be realized during the next network refresh because fewer switches will be required - thousands of dollars in savings will accrue for each switch that does not need to be installed or replaced.

In all cases, maintenance fees will be reduced with each switch that is taken out of service. An access-switch service contract is typically priced at 15% of the price of the switch, making the annual cost of maintenance about US\$1,343. Pull a switch out of service and these savings drop directly to the bottom line.

Reducing Future Distribution-Layer Capital Expenses and Maintenance Fees

In addition to the savings achieved by decommissioning access-layer switches, there are similar savings to be had by decommissioning distribution-layer switches. The number of distribution layer ports needed is based on the number of access-layer switches. If enough access-layer switches are removed from service, then one distribution-layer switch can be decommissioned as well. To avoid a single point failure, it is not uncommon to connect one access-layer switch to two different distribution layer switches for redundancy. In these cases, decommissioning one access-layer switch will actually free up two distribution-layer ports, doubling the savings.

If rightsizing allows you to decommission a distribution-layer switch, the savings will be spread across roughly the same categories as would be the case for an access-layer switch: capital, maintenance, power, cooling, and IT support costs. The actual costs will be greater. Since the cost to purchase and support a distribution-layer switch are higher, the actual dollar savings will be greater than for an access-layer switch.

Reducing Current Network Administration Operating Expenses

There are considerable operating costs associated with the adds/moves/changes made on a wired network. To calculate these costs, you first need to estimate the average number of times each year that an employee or user changes locations. This number should include employees that you plan to hire and let go. If each employee moves once per year, and it takes an average of 24 minutes to modify the network accordingly, then at a cost of US\$86 per hour, each change to the wired network will cost the company an average of US\$34 per year. When multiplied times the total number of changes, the numbers add up quickly.

Once a user has transitioned to the wireless LAN, the cost of changes drops nearly to zero. Network and security information will transition with the user regardless of which access point is used to connect to the network.

Add/move/change costs vary widely between organizations. Be sure to check the defaults in the Rightsizing Calculator tool to ensure that they align with the cost structure of your company.

Reducing Electrical Utility Costs

The electrical costs used in the access-layer section of the calculator assume that each switch consumes 143 Watts per hour. The typical switch generates an estimated 609 BTUs of heat, and using an average electricity price of US\$0.10 per kilowatt hour, the estimated annual cost to run and cool a switch is US\$282.

Improving Employee Productivity Through Mobility

Mobility enhances productivity by making it possible to work anywhere, at any time. Increased productivity resulting from the deployment of a wireless LAN can be estimated by comparing network traffic before and after network rightsizing. If the same number of users generate increased network traffic on the wireless LAN, or if new workflows or work processes can be accomplished on the wireless LAN that were previously not possible, then productivity can be said to have increased. Quantifying the benefits to the user may be easier than assessing the resulting savings, but at least the statistics about usage and application inform you about which users to track.

Summarizing Cumulative Cost Savings

The access-layer cost reductions discussed so far have related directly to the cost of purchasing the switches and maintenance contracts, and powering and cooling the switches. Another operational expense that needs to be considered is the planning, installation, configuration, maintenance, updating, and monitoring involved with running the switch. With an estimated cost of US\$86 per hour for an IT Network Engineer, and an estimate of 25 support hours per year, each access-layer switch costs US\$2,150 per year to manage.

If your organization's policy is to replace access-layer switches every five years, then at an estimated cost of US\$5,375 per switch (US\$1,075 per year), yearly maintenance contract costs of US\$1,343, yearly power costs of US\$282, and IT support costs of US\$2,150 per year, each switch that is decommissioned will generate a savings of US\$4,850 per year. This does not consider the additional costs of the wiring closet, computer rack, UPS, and other items that consume time and money.

Case Studies of Successful Justifications

In the following case studies, you will learn how three very different organizations benefited from network rightsizing.

- *California State University* saved almost US\$30 million while expanding networking capabilities to more than 490,000 students, faculty members, and staff.
- *KPMG* designed its new 2,800-person headquarters near Amsterdam using wireless LAN as the primary means for network access. In so doing, the company reduced capital costs by more than US\$2,000,000, and pocketed estimated recurring savings of US\$760,000.
- *Aruba* rightsized its own wired network and is projected to save more than US\$1,200,000 over three years.

The California State University

California State University (CSU) includes 23 university campuses and supports more than 490,000 students, faculty members, and staff. As with many organizations, as technology changes and matures, CSU must periodically update and refresh its networking equipment. Updating the network and providing one 10/100 Ethernet connection to each and every user, as well as providing adequate capacity for the classrooms, libraries, labs, common areas, and retail centers, would be an extremely complicated and cost prohibitive task.

While planning the network refresh, the Technology Infrastructure Services (TIS) group began to measure network and port usage so that it could make more informed spending decisions. During this analysis, it found that more than half of the wired network ports had passed no packets during the previous six months. With half of the wired jacks being unused, CSU decided to explore a different approach to its planned network refresh. The TIS staff created a database with every telecommunication room in CSU, the number of ports in each room, and the number of those ports that were actively used. A formula was developed to use this information to determine the refresh requirements of each campus and closet, and to decommission unused equipment.

Consolidating the equipment in the wiring closets would lower equipment, maintenance costs, electrical, and cooling costs. Still the need existed to provide network access to all users. For this, CSU decided to install Aruba's 802.11n wireless LANs. CSU recognized a net savings of approximately US\$30 million by reducing the scale of its planned wired network refresh, and it used some of the savings to purchase and deploy Aruba's wireless LANs across all campuses.

Centralized controllers provide policy enforcement firewalling, mesh, wireless intrusion prevention, and secure remote access points. 802.11n provides seamless network access throughout each campus. Prior to the upgrade, university faculty and staff were the primary users of the wired network. That is no longer the case, and the students are now the primary network users. Some campuses have seen a nearly fivefold increase in network usage following the installation of pervasive 802.11n networks.

KPMG

While designing a new 2,800-person headquarters near Amsterdam, KPMG's IT group calculated that its traditional port-based wired network capacity planning approach would have required 18,000 cable pulls, more than 55 chassis, and 260 switches. The initial cost was expected to exceed US\$6,000,000, with recurring ownership costs into the millions annually. Upon further investigation, KPMG found that its end user network requirements could be met by either Fast Ethernet or an Aruba 802.11n wireless LAN. It also found that enterprise-class wired switches cost about four times as much as 802.11n access points, yet support about the same number of devices in real-world deployments. Additionally, wired network installation costs are much higher than wireless. The issue was that some users preferred to use a wired Ethernet connection.

KPMG compromised by installing a hybrid access layer with 50% fewer ports, cables, chassis, and switches, and at the same time pervasively deployed an 802.11n wireless LAN from Aruba. By shifting

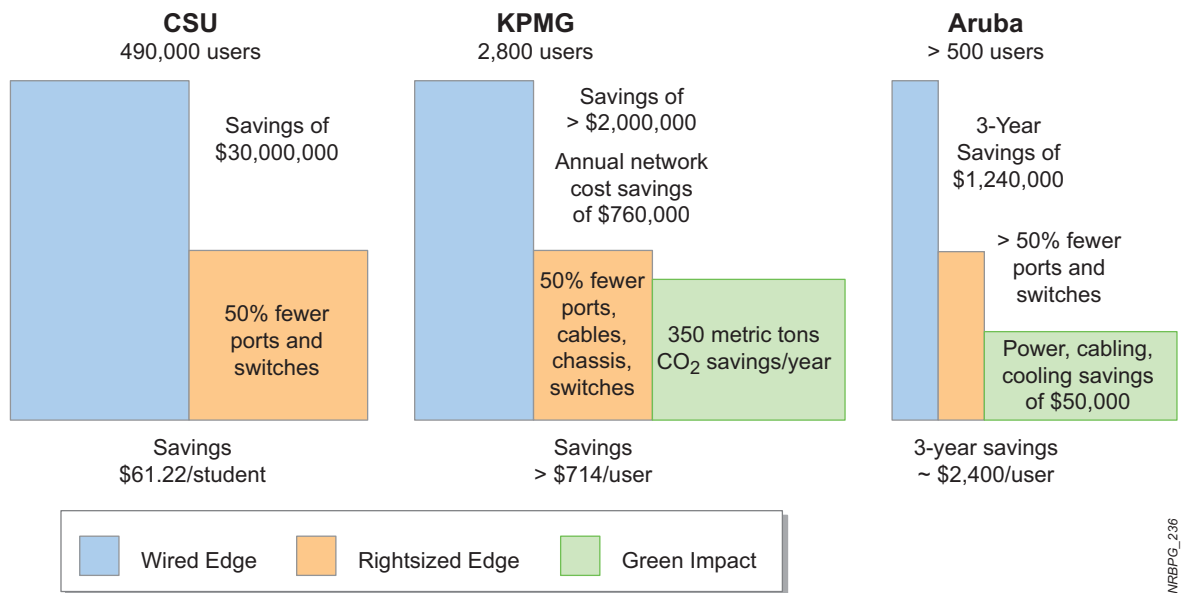
many of the users to the wireless network, KPMG reduced the capital costs of its new headquarters by more than US\$2,000,000. It also reduced recurring networking costs by more than US\$760,000 per year, with greater savings expected as more users migrate to the wireless LAN.

Aruba Networks

As a firm believer in both wireless and green IT, Aruba's IT department rightsized on its internal enterprise network by replacing much of the wired infrastructure with 802.11n. Following an analysis of the network, it was determined that more than 90% of the 500+ employees could best be served by an 802.11n wireless LAN. VPN clients and secure tokens were replaced with Aruba's secure Remote Access Point (RAP) technology, a secure plug-and-play AP that extends the corporate network to remote sites.

The process not only lowered expenses, but also increased employee productivity and reduced the company's resource footprint. Through rightsizing, Aruba's IT department was able to transition from 26 switches with 1,200 ports down to 12 switches with 525 ports. Decommissioning the switches and ports yielded estimated three-year savings of US\$398,000 – roughly one-third of the overall US\$1,240,000 savings. US\$200,000 was saved in reduced IT support costs. Reduced power, cabling, and cooling costs saved another US\$50,000. The increased use of the VoWi-Fi infrastructure allows employees to connect to the corporate network (whether at an Aruba office or through a RAP) and call any other employee or office in the world on the internal network at no cost.

Comparitive studies of Wired Edge vs. Rightsized Edge



NRBPG_236

Implement

This section walks you through the major steps involved with implementing a rightsized network. In addition to deploying the 802.11n WLAN, you may need to update and/or configure client devices and software prior to transitioning them to the WLAN. Users will be migrated to the WLAN in groups. After confirming that users have been transitioned to the WLAN, unneeded wired infrastructure can be decommissioned and either redeployed, added to a spares pool, or recycled.

Step 1 – Develop a Transition Plan for Migrating Users to the WLAN

Using the list of user populations that was created in the Analyze phase, inform and educate users who will be transitioning to the WLAN about the dates and service interruptions, if any, they will experience. New WLAN users should be shown how to use the wireless network and the benefits they will obtain. Dates need to be set defining when the transition will begin and when the unneeded wired connections will be disconnected and removed. IT staff needs to be available to assist users throughout the transition should they have problems updating their computers or connecting to the wireless LAN. The smoother the transition, the quicker users will embrace the new technology.

Step 2 – Bring Up the Pervasive WLAN

The next step is the installation of the wireless infrastructure. The master controller needs to be configured and the local controllers added to the master. Access points and air monitors need to be configured and installed. You can install the wireless LAN throughout the entire organization and then begin transitioning users, or you can roll out one area at a time. Since you are implementing a pervasive WLAN, buildings should not be deployed with only partial coverage. For this reason, it is recommended that the WLAN be implemented at least one building at a time.

A pilot building should be chosen and meet the following criteria:

- Close proximity to the organization's IT staff
- Cooperative management and users with past experience participating in trials
- An environment that will benefit greatly from the addition of a pervasive WLAN

The access points and air monitors should be powered by PoE. Aruba's family AP 12x 802.11n Access Points can connect to 802.3af and PoE+ power sources. Since 802.11n APs are capable of handling more data than the earlier 802.11a/b/g APs, the new 802.11n APs should be connected to gigabit Ethernet switches. You can either use mid-span PoE with gigabit Ethernet or PoE-capable gigabit Ethernet edge switches to provide power for these APs.

Step 3 – Upgrade Target Population Devices (NICs, drivers)

Depending on your organization, you may have strict control over the user's equipment and configuration or, as is the case with universities, you may have very little control over the user's equipment. With the installation of the WLAN, it may be necessary to upgrade and/or configure the client computers to connect to the wireless network. 802.1X/EAP is typically used to provide secure access to the WLAN for the enterprise, and it uses client software known as a "supplicant" to provide authentication and encryption. An 802.1X/EAP supplicant is integrated into most popular operating

systems, however, the firmware, drivers, and on rare occasions, the NIC in older wireless devices may need to be upgraded to enable a WLAN connection.

Step 4 – Move Groups Sequentially to WLAN

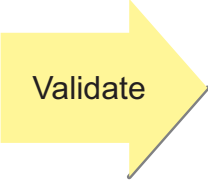
Just as it is easier to deploy a pervasive WLAN one building or area at a time, so, too, is it easier to transition groups of users to the WLAN. Earlier, you identified the different user populations that will be migrated to the WLAN. Plan a transition strategy that allows the IT team to meet with each of the affected groups. This can be done one building or campus or floor at a time. User groups will need configuration parameters and settings for WLAN connectivity. Transition windows should be scheduled and closely monitored. Using Aruba WLAN controllers and AirWave monitoring tools, you can track which groups have successfully migrated to the WLAN and then monitor their usage. Conversely, you can use the same tools to identify connection problems and clients.

Step 5 – Decommission Selected LAN Segments

After you have successfully transitioned users from the wired to the wireless network, the next step is to consolidate and decommission equipment that is no longer needed. Unneeded wired ports should be disconnected from the layer two switches, and the remaining wired connections should be consolidated. You should check your switch configurations prior to moving any cables since you may need to reconfigure the remaining switches to support the wired VLANs that are still in use.

Step 6 – Dispose of Decommissioned Equipment Properly

Once you have removed unneeded equipment from the network, you can spare, sell, or recycle them. For Greenfield deployments, there will of course be no equipment to discard. For closet refreshes, Aruba recommends that you remove the oldest switches first and either use them for spares, recycle them, or sell them to generate cash.


 Validate

The best way to validate a rightsizing project is to compare the financial models and justification predications with observed results. Cost savings will be easy to verify to the extent that you constructed complete capital and operational expense savings models in the Analyze phase.

Validation Against Justification

During the Justification phase, you planned and calculated how many users could be migrated to the wireless LAN and how many ports and switches you would be able to decommission. Using the Aruba Operating System and AirWave suite monitor screens, you can identify how many users are connected to the wireless LAN. If Statseeker is still installed, you can also identify the number of switches and ports that are connected to the network. Comparing these numbers to your initial snapshot and Justification stage data will show the percentage of users that migrated to the wireless LAN and the number of ports that were decommissioned. If the observed numbers are equal to or higher than the projected numbers, then the project satisfied the justification criteria.

How to Confirm/Prove that the Projected Return on Investment was Achieved

In order to confirm that the expected return on investment was achieved, compare the current costs associated with the network with the costs prior to rightsizing. You'll want to review post-rightsizing maintenance fees, electricity and gas expenses, IT labor expenses, and IT time cards and help desk tickets showing labor allocated to adds/moves/changes. Comparing pre- and post-rightsizing actuals can help to show if the ROI was achieved.

The following chart lists suggested metrics for comparing network costs prior to and after rightsizing your company's network.

Three Months and Six Months

1. Validate and measure the actual hardware operational expense reduction for monthly charges (power, cooling, and so on)
2. Validate management and administrative operational expense reduction (this requires some kind of baseline)
3. Measure the number of network cases going to the Help Desk before and after the transition (to show that transition has been problem-free)
4. Show network customer satisfaction surveys and/or Help Desk trouble tickets related to the network before and after, if the Help Desk tracks this kind of information
5. Measure overall network utilization
6. Validate and measure the reduction in the number of switch ports, while overall bandwidth usage stays the same or begins to climb
7. Quantify the proceeds of asset sales from decommissioned equipment

Twelve Months

1. Total the previous 12-month capital expenditures avoided
2. Total the impact on coming 12–24 month budgeting cycle
3. Total the 12-month maintenance avoided (NOTE: Difficult to track on a monthly basis)
4. Total the impact on coming 12–24 month cycle
5. Quantify the “mobility” productivity benefit of users being wireless.

To assist you with your network rightsizing analysis and using the ROI calculator, this section describes three different rightsizing scenarios, the values that each organization would enter on the worksheet and in the template, the expected return on their investment, and simple “what if” comparisons based on minor changes to the enterprise template information in the calculator.

Scenario 1 – 500-Employee Publishing Company

The organization is a publishing company with 500 employees. The company has been in business at the same location for many years, occupying five floors of a downtown building with 125,000 total square feet of office space. Until now the company has not installed any wireless networking. The computer environment is heavily based on desktop publishing and graphics, with limited laptop use; however, there has been a trend towards using laptop computers over the past couple of years, especially by the salespeople, managers, and office staff. The cabling throughout the organization is lean, providing Ethernet connections for personal computers, telephones, conference rooms, and printers. Their wiring closets contain 1250 switch ports, which are supported by 35 access-layer switches, with each switch having 48 ports.

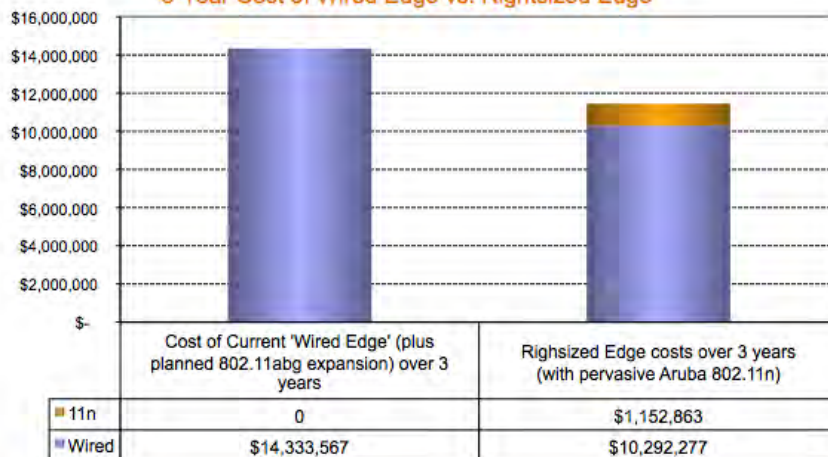
The New 'Rightsized Edge'

Number of switch ports decommissioned after Rightsizing:	8,000
Number of switches decommissioned after Rightsizing:	166
Annual reduction in 'Wired Edge' costs through Rightsizing	\$1,347,096

3-Year Cost Assessment

Reduction in 'Wired Edge' Costs (3 years)	\$4,041,289
Elimination of planned 802.11abg expansion (not required after Rightsizing)	\$341,285
Estimated cost of 802.11n expansion and operating costs (3 years)	(\$1,152,863)
Total 3-year cost savings through Rightsizing	\$3,229,712

3-Year Cost of Wired Edge vs. Rightsized Edge

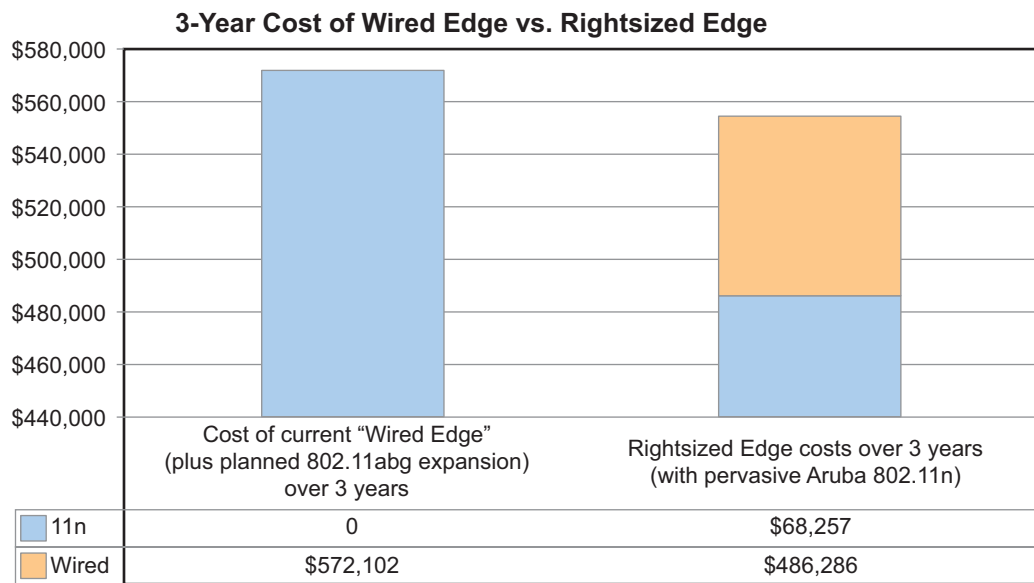


Year-1 Budget reduction (or increase) from pervasive 11n	\$659,969
Metric tons of CO2 emissions eliminated by move to WLAN	913.68

From the company profile above, the information for the ROI worksheet can be completed and then transferred into the calculator to perform the analysis. This scenario uses conservative values, including 0.5 adds/moves/changes per year per employee, of which none will require additional cabling.

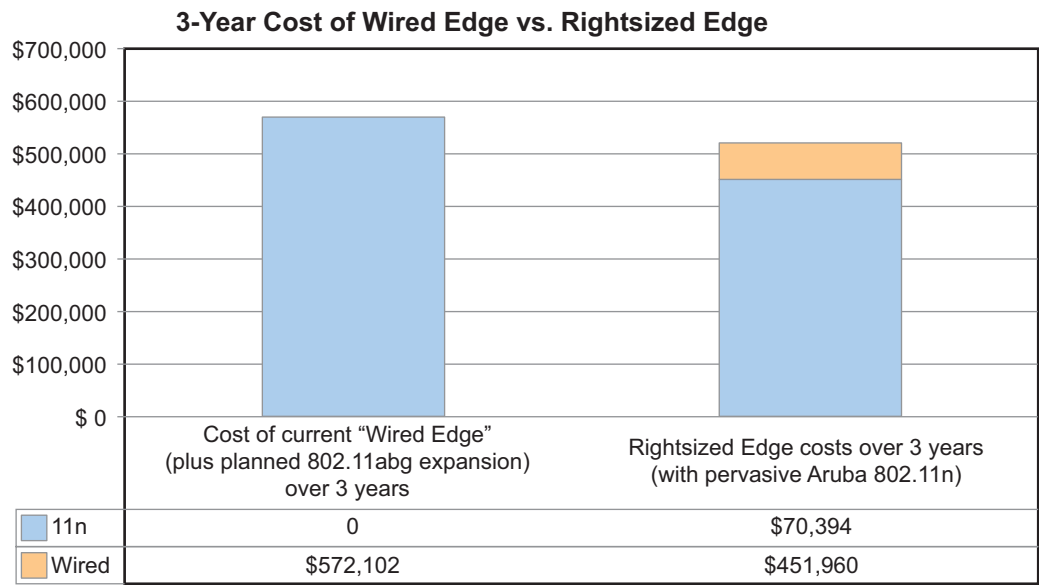
500	Total # of network users
125,000	Size of existing facilities (in square feet)
0	% of existing facility space with existing wireless coverage (802.11abg)
0	Additional % of existing facility space that will be covered by 802.11abg (planned growth)
.5	Average number adds/moves/changes per year per employee
0	% of these moves in which the employee is moved to a new or refurbished space (requiring new cable pulls)
2.5	Current average # of ports per user (including common areas, conference rooms, printers, etc)
25	% of users capable of shifting to wireless-only for data access

Based on the information entered, the publishing company is currently incurring US\$190,701 in capital and operating expenses to support its wired network. By switching 25% of the users from Ethernet to the WLAN, a total of 188 switch ports and three switches can be decommissioned, generating an annual savings of US\$28,605 and a three-year return of US\$85,815. In this environment, the installation of a rightsized Aruba 802.11n network will have a three-year cost of US\$68,257. The publishing company would realize a three-year net savings of US\$17,558 by installing a pervasive 802.11n network. In addition to the cost benefit and the enhanced capabilities, an estimated 27 tons of CO₂ emissions will be removed from the environment by transitioning to the rightsized network. The figure below summarizes the results of these calculations.



NRBPG_237

The Aruba Rightsizing Calculator can perform “what if” comparisons. This scenario is based on 25% of the users switching from a wired network to a WLAN. What type of savings could the organization realize if 35% of the users were migrated to the WLAN? By simply changing the “% of users capable of shifting to wireless-only for data access” field to 35%, we see that the three-year savings will almost triple to a total of US\$49,747, and the estimated total decrease of CO₂ emissions will rise to almost 43 metric tons, as summarized in the figure below.



NRBPG_238

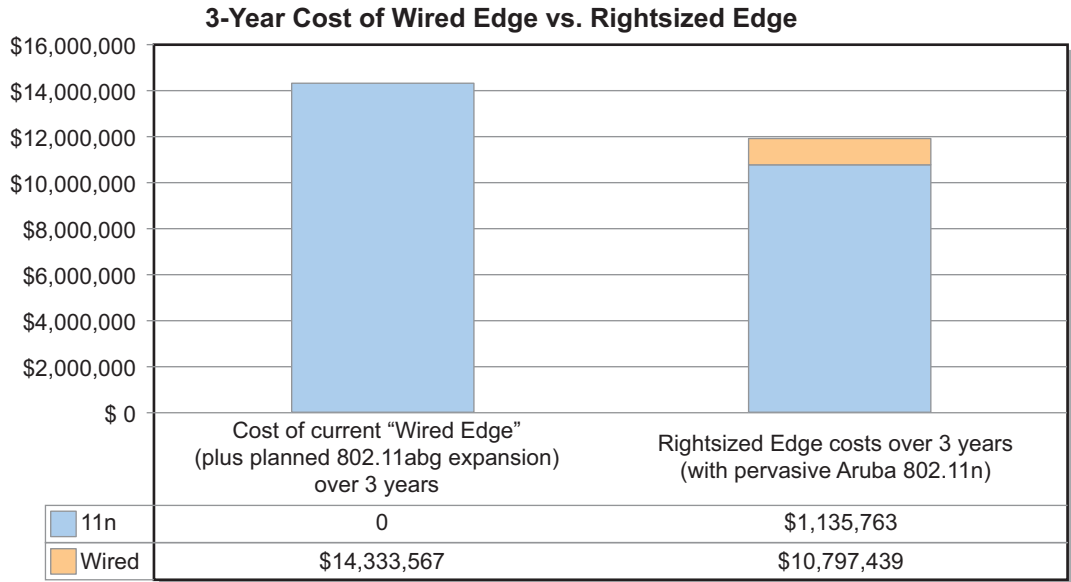
Scenario 2 – Investment Bank with 8,000 Employees

The organization is an investment firm with 8,000 employees. The company occupies 2,000,000 square feet of space in a building near the city. The company has WLANs covering about 20% of the building installed on some of the floors. This year it has budgeted to expand the wireless network covering about another 10% of the building. The computers are a mix of desktops and laptops. Most of the offices are double-occupancy, and the conference and meeting rooms include multiple Ethernet jacks. The majority of the laptop users are salespeople, marketing staff, and executives. The wiring closets contain 28,000 switch ports, and are supported by 603 access-layer switches, each with 48 ports.

Using the company profile above, the ROI worksheet can be completed and then transferred to the calculator for analysis. This scenario is more typical than the first example because it has moderate staff turnover and periodic installation of new cables and jacks.

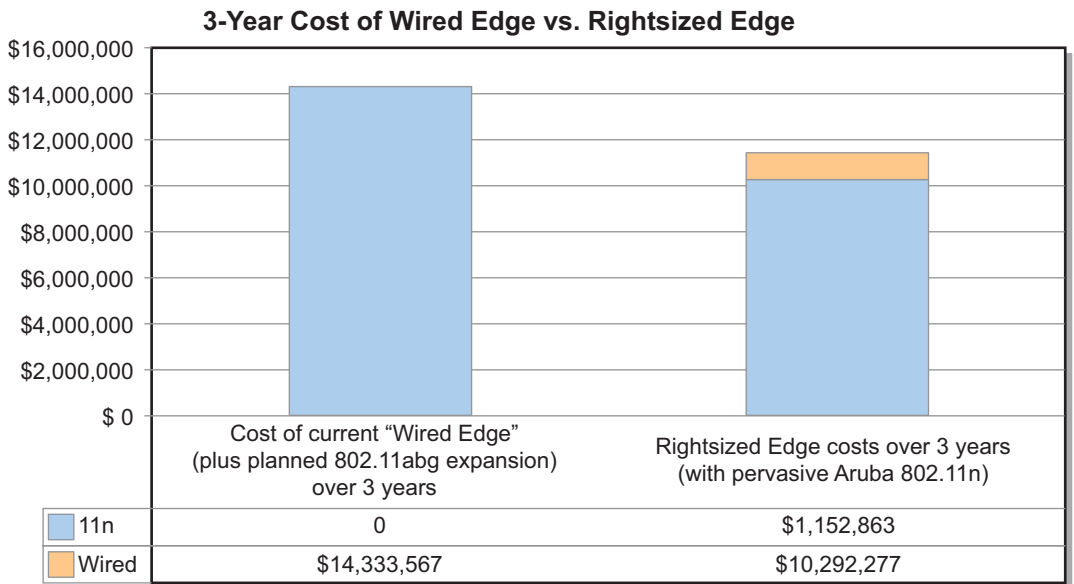
8000	Total # of network users
2,000,000	Size of existing facilities (in square feet)
20	% of existing facility space with existing wireless coverage (802.11abg)
10	Additional % of existing facility space that will be covered by 802.11abg (planned growth)
1	Average number adds/moves/changes per year per employee
15	% of these moves in which the employee is moved to a new or refurbished space (requiring new cable pulls)
3.5	Current average # of ports per user (including common areas, conference rooms, printers, etc)
35	% of users capable of shifting to wireless-only for data access

Based on the information entered, the investment company is currently incurring US\$4,714,838 in capital and operating expenses to support its wired network. By switching 35% of the users from Ethernet to WLAN, a total of 7,000 switch ports and 145 switches can be decommissioned, generating an annual savings of US\$1,178,709 and a three-year return of US\$3,536,128. In this environment, the installation of a rightsized Aruba 802.11n network will have a three-year cost of US\$1,135,763. So, the investment company would realize a three-year savings of US\$2,741,650 by installing a pervasive 802.11n network. In addition to the cost benefit and the enhanced capabilities, an estimated 784 tons of CO₂ emissions will be removed from the environment by transitioning to a rightsized network. The figure below summarizes the results of these calculations.



NRBPG_239

This scenario is based on 35% of the users switching from a wired network to a WLAN. What type of savings could the organization realize if it could move 40% of the users to the wireless network? By simply changing the "% of users capable of shifting to wireless-only for data access" field to 40%, we see that the three-year savings will increase by US\$488,062, to a total of US\$3,229,712, and the estimated total decrease of CO₂ emissions will be about 913 metric tons, as shown in the figure below.



NRBPG_240

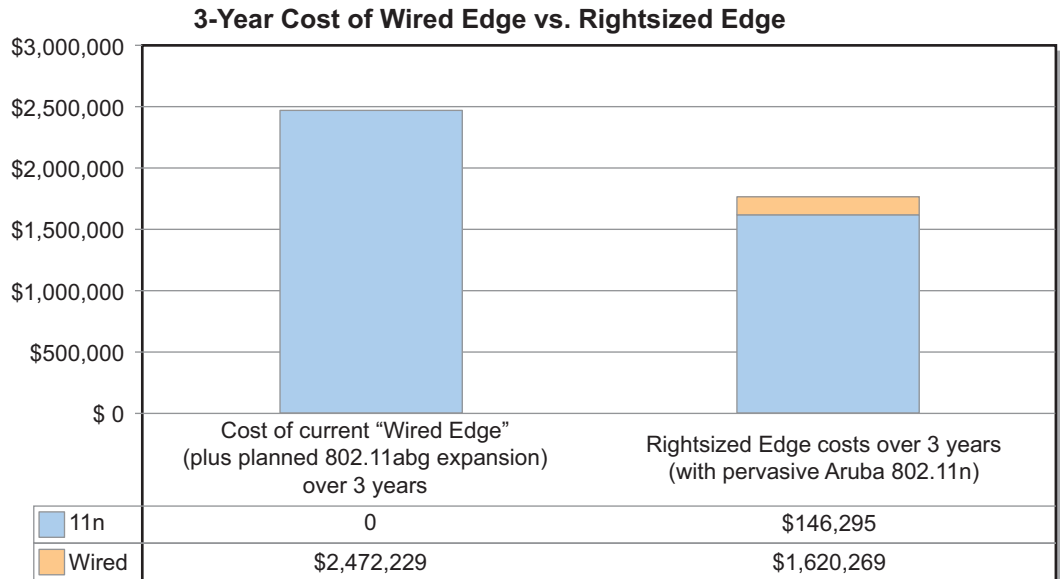
Scenario 3 – Technology Company with 1,000 Employees

A large technology company is planning a major closet refresh. The organization has 1,000 employees and 70% of them are using laptop computers. 250,000 total square feet of office space is spread across multiple locations: the corporate headquarters occupies 200,000 square feet while the remaining 50,000 square feet is divided among three locations in other parts of the state. Two years ago, the company installed wireless networks covering about 20% of the headquarters facility, primarily the conference rooms and public areas. This year it budgeted to add wireless to the three off-site locations to reduce the costs of installing new Ethernet cables and jacks. When the company originally moved into its offices, it installed extra data cabling to accommodate future expansion. A total of 4,500 ports are terminated at 108 48-port switches in the wiring closets. With the installation of a pervasive wireless LAN, the company plans to transition 45% of its users, more than half of which are laptop users, from the wired network to the wireless LAN.

Using the company profile above, the ROI worksheet can be completed and then transferred to the calculator for analysis.

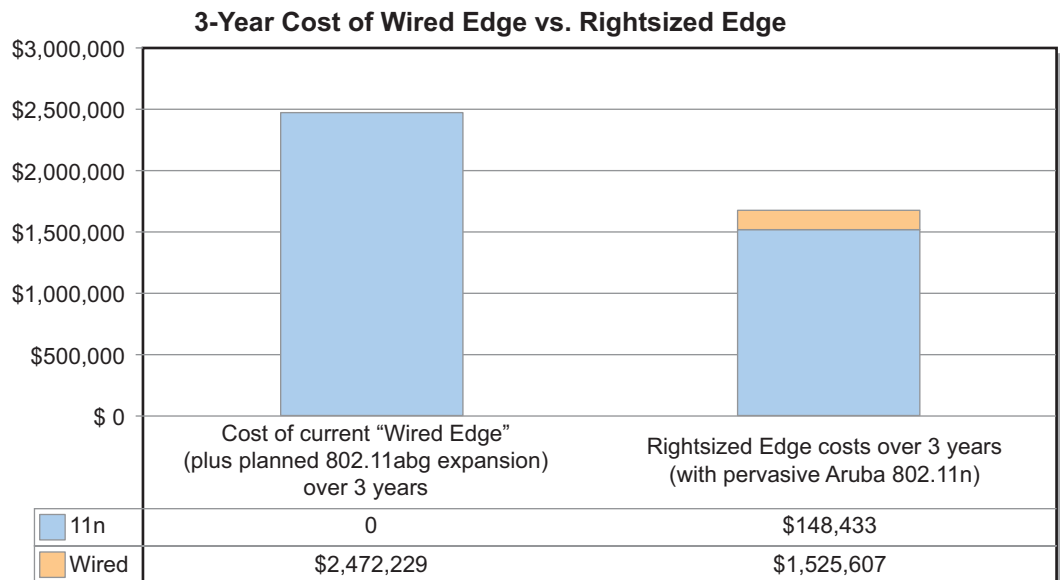
1000	Total # of network users
250,000	Size of existing facilities (in square feet)
20	% of existing facility space with existing wireless coverage (802.11abg)
20	Additional % of existing facility space that will be covered by 802.11abg (planned growth)
1	Average number adds/moves/changes per year per employee
15	% of these moves in which the employee is moved to a new or refurbished space (requiring new cable pulls)
4.5	Current average # of ports per user (including common areas, conference rooms, printers, etc)
45	% of users capable of shifting to wireless-only for data access

Based on the information entered, this technology company is incurring US\$811,390 in capital and operating expenses to support its wired network. By switching 45% of the users from wired to WLAN, a total of 1,575 switch ports and 32 switches can be decommissioned, generating an annual savings of US\$283,987 and a three-year return of US\$851,960. In this environment, the installation of a rightsized Aruba 802.11n network will have a three-year cost of US\$146,295. So, the technology company would realize a three-year savings of US\$781,780 by installing the pervasive 802.11n network. In addition to the cost benefit and the enhanced capabilities, an estimated 193 tons of CO₂ emissions will be removed from the environment by transitioning to a rightsized network. The figure below summarizes the results of these calculations.



NRBPG_241

This scenario is based on 45% of the users switching from a wired network to a wireless network. What type of savings could the organization realize if 50% of the users were migrated to the WLAN? By simply changing the “% of users capable of shifting to wireless-only for data access” field to 50%, we see that the three-year savings will increase by US\$92,525, to a total of US\$874,305, and the estimated total amount of CO₂ emissions eliminated will exceed 216 metric tons, as shown in the figure below.



NRBPG_242

Network rightsizing is a capacity planning and cost reduction strategy. The strategy defines how to assess wired network infrastructure, both in term of expenses and user needs, with an eye towards eliminating inefficiencies and waste. The strategy also defines how to assess the value of migrating to 802.11n edge access in light of the growing demand by users for increased mobility. A methodology for collecting, tabulating, and evaluating the wired and wireless options was described, and a calculator for tabulating results was presented. Finally some example scenarios were played through to show the final steps of the overall evaluation process.

Organizations have increasingly migrated toward using laptop computers, mobile handheld computers, smart phones, and other mobile clients. The tide has turned in favor of Wi-Fi, and there is no going back to a predominantly wired world. The open question is when will you reap the benefits of this fundamental transformation in networking – sooner or later?

Today many mobile users are underserved and less productive than they might otherwise be because the wired edge is overbuilt at the expense of the wireless edge. Many closet switches are under-utilized, equipment that could be retired from service remains under service contracts, and energy-consuming infrastructure that could be shut down remains on-line. Budgets are being consumed, heat generated, CO2 emitted – all needlessly. Network rightsizing addresses these issues, ensuring that you pay for what you need today and will need in the future. It is, quite simply, one of the most practical steps you can take to enhance user efficiency and prevent wastage of money, energy, and time.

Ongoing Analysis

Since network usage and user requirements are constantly changing, you will need to periodically analyze the network to ensure that it's still delivering the performance that users need. You may also need to address areas where network utilization exceeds available capacity. Rightsizing is not a one-time task, but rather a different way of implementing and operating a networking environment. After the installation of a pervasive wireless LAN, other users may start migrating to the wireless LAN for the convenience and flexibility that it offers. You need to monitor the network to ensure that when they do so, there is adequate capacity to handle the increased load.

Infrastructure Analysis

After the rightsized network has been deployed, monitor the network to determine if there are additional ports that can be decommissioned in the future. As users become more comfortable with the wireless LAN, additional wired users may transition to using the WLAN as their primary or sole connection to the network. If sufficient users migrate to the WLAN, you will be able to decommission additional switches, further reducing capital and operational expenses.

Network Utilization

With greater access to the network available through the WLAN, usage patterns may change. How and where the network is accessed may change. Laptop users will be more likely to bring their computers with them when attending meetings or visiting colleagues. It is important to monitor the network to track changes in utilization and ensure that adequate bandwidth is available in the right locations.

Traffic Analysis

You should also monitor the types of traffic that are traversing the network. It is likely that changes in usage patterns include changes in the type of traffic traversing the network. Instant messaging, voice, video, and peer-to-peer application use could climb. Analyzing traffic patterns will help you more effectively plan and maintain the network.

Existing Enterprise Network Environment

_____	Total # of network users
_____	Size of existing facilities (in square feet)
_____	% of existing facility space with existing wireless coverage (802.11abg)
_____	Additional % of existing facility space that will be covered by 802.11abg (planned growth)
_____	Average number adds/moves/changes per year, per employee
_____	% of these moves in which the employee is moved to a new or refurbished space (requiring new cable pulls)
_____	Current average # of ports per user (including common areas, conference rooms, printers, etc)
_____	% of users capable of shifting to wireless-only for data access

Questions About Typical Costs

_____	Average cost per switch
_____	Average discount off list price for switches (%)
_____	Average annual maintenance fee for switches (%)
_____	Replacement schedule of switches (for example, four, five, or six years)
_____	Average cost per cable pull

In [Other Key Enabling Technologies for Rightsizing on page 11](#), you learned about some of the key enabling technologies in 802.11n that make rightsizing possible. These technologies fall into four categories: reliability, manageability, security, and scalability. In this appendix, you will learn more about these technologies and relevant configuration settings.

Reliability

Network reliability is essential in business-critical infrastructure like a wireless LAN. If the WLAN doesn't meet user expectations, then it will be removed and the rightsizing effort will be for naught. ARM technology provides the reliability needed for the WLAN to deliver wire-like performance.

ARM¹

Wireless LANs need to adapt to the dynamic surroundings in which they operate. ARM technology monitors the network and adapts to changes in clients, applications, and the RF environment. ARM includes many unique features, and this section will explain those features that are particularly important to network rightsizing.

ARM Config

ARM manages the configuration of access points, including initial setup and adjustment of the AP's channel and RF power. If an AP stops working for any reason – component failure, damage, loss of power, loss of data - the Aruba controller will automatically adjust settings on nearby APs in an attempt to fix the resulting coverage hole. This dynamic adjustment capability reduces or eliminates the need to perform a formal site survey since ARM will cause the network to adapt to the environment.

Each AP will periodically scan the RF channels and provide the RF information to the controller. The controller uses these samples to properly adjust the channel and power level of each AP. In most environments, this off-channel scanning period is so small as to be unnoticeable. However, at certain times, such as during voice over Wi-Fi (VoWi-Fi) transmissions or periods of heavy load, even this short period of scanning can affect the wireless connection. To prevent problems from occurring, ARM can be configured to be aware of the application environment and automatically disable scanning when certain conditions occur. For example, voice-aware settings can prevent an AP from scanning when it is transporting VoWi-Fi packets, load-aware settings can prevent an AP from scanning during periods of high traffic load, and mode-aware settings can even dynamically convert access points to air monitors to mitigate co-channel interference if ARM detects high-coverage overlap.

1. For more information about Aruba's innovative ARM technology, please see the whitepaper on Aruba's website: http://www.arubanetworks.com/pdf/technology/whitepapers/wp_ARM_EnterpriseWLAN.pdf.

All application-aware ARM parameters can be customized to address the specific needs of any wireless environment. These settings can also be configured globally across the entire wireless network, or they can be customized to address conditions that exist in specific locations or areas of the wireless network. The screen capture below (from the menu: Configuration > All Profiles > RF Management > Adaptive Radio Management (ARM) Profile > default) shows the ARM profile screen in which these settings can be enabled, disabled, or customized to meet your specific needs.

Profile Details			
Adaptive Radio Management (ARM) profile > default			
		<input type="button" value="Show Reference"/> <input type="button" value="Save As"/> <input type="button" value="Reset"/>	
Assignment	single-band	Allowed bands for 40MHz channels	a-only
Client Aware	<input checked="" type="checkbox"/>	Max Tx EIRP	127
Min Tx EIRP	9	Multi Band Scan	<input checked="" type="checkbox"/>
Rogue AP Aware	<input type="checkbox"/>	Scan Interval	10 sec
Active Scan	<input type="checkbox"/>	Scanning	<input checked="" type="checkbox"/>
Scan Time	110 msec	VoIP Aware Scan	<input type="checkbox"/>
Power Save Aware Scan	<input checked="" type="checkbox"/>	Ideal Coverage Index	10
Acceptable Coverage Index	4	Free Channel Index	25
Backoff Time	240 sec	Error Rate Threshold	50 %
Error Rate Wait Time	30 sec	Noise Threshold	75 -dBm
Noise Wait Time	120 sec	Minimum Scan Time	8
Load aware Scan Threshold	1250000 Bps	Mode Aware Arm	<input type="checkbox"/>

Band Steering

Many wireless client devices are capable of both 2.4 GHz and 5 GHz communications. Most are configured to automatically choose either band based on received-signal parameters such as signal and noise levels. Allowing the client device to connect to either band provides greater flexibility when connecting between different networks. When a client device connects to a network, it typically chooses to connect to the AP with the strongest signal, regardless of the band.

Band steering allows the controller to move clients from the 2.4 GHz to the 5 GHz network when possible. Using client fingerprinting techniques, the controller can encourage 5 GHz-capable clients to transition from the 2.4 GHz network to the 5 GHz network by “hiding” the 2.4 GHz APs from the specific client devices. Doing so encourages the client to roam to a 5 GHz AP. Since there are only three non-overlapping channels in the 2.4 GHz band, it is very beneficial to move 5 GHz-capable clients to the 5 GHz band where there are as many as 23 (20 MHz) channels or 11 (40 MHz) channels available. By decreasing the number of devices on the 2.4 GHz band and transitioning them to the 5 GHz band, band steering can reduce overcrowding in the 2.4 GHz band and improve overall network throughput on both bands. Band Steering can be enabled in the Configuration > All Profiles > Wireless LAN > Virtual AP menu.

Spectrum Load Balancing

Similar to the way in which ARM encourages clients to transition from one band to another, spectrum load balancing encourages clients to transition from busy channels to channels that are not as busy. With spectrum load balancing, APs that are busy will respond to client association requests with an error code, encouraging the clients to connect to a different AP. The controller analyzes groups of APs and client density to determine the intelligent distribution of clients across the available spectrum. Spectrum load balancing can be configured globally across the entire wireless network, or it can be customized to address conditions that exist in specific locations or areas of the wireless network. Spectrum Load Balancing can be enabled in either of the radio profile sections under the Configuration > All Profiles > RF Management menu.

Traffic Shaping for Airtime Fairness

Traffic shaping for airtime fairness ensures that clients with different capabilities and data rates are given equal time on the channel. In a typical mixed-mode environment, devices that transmit at slower data rates take longer to transmit the same amount of data as their faster counterparts. Airtime allocation can provide three different levels of airtime fairness and is configured under the Configuration > All Profiles > QOS > Traffic Management Profile menu in a field labeled Station Shaping Policy. If Station Shaping Policy is configured to default-access, the standard 802.11 access control methods will allocate bandwidth to the different clients. If Station Shaping Policy is configured to fair-access, the Aruba controller will allocate the same airtime to clients regardless of their client capabilities. If Station Shaping Policy is configured to preferred-access, the Aruba controller will give higher priority to faster clients (802.11n > 802.11a/g > 802.11b) while ensuring all clients do receive access.

Airtime fairness will be enforced by an access point regardless of the number of service set identifiers (SSID) that the access point is supporting. The controller keeps track of all basic service set identifiers (BSSIDs) on a physical radio, and allocates to each client according to the setting that is selected. QoS frames will be given higher priority, and 802.1X frames will not be shaped.

Multicast Traffic Optimization

Aruba supports technology for optimizing multicast traffic when sending video broadcasts over the wireless LAN. When Internet Group Management Protocol (IGMP) Snooping is enabled, the Aruba controller keeps track of client multicast stream subscriptions and forwards the multicast stream only to access points with client subscriptions, limiting the unnecessary flooding of the multicast stream to all access points.

Multicast rate optimization optimizes multicast traffic. By default, multicast traffic is transmitted at the lowest configured data rate of the AP. For 2.4 GHz networks this is typically 1 Mbps, and for 5 GHz networks this is typically 6 Mbps. Even if all clients are connected to the access point at higher data rates, by default, the AP will transmit the multicast at the lowest data rate. To prevent this from occurring, the Aruba controller will determine the slowest active single-stream unicast rate and transmit multicast at that rate. Doing so minimizes the amount of airtime used by the multicast stream, and provides additional capacity for other wireless communications.

Adjacent and Co-Channel Interference

When multiple access points are installed near each other, they can cause co-channel interference (CCI) or adjacent channel interference (ACI), regardless of whether they are part of the same or different networks. CCI occurs when multiple APs and/or clients on the same channel can hear each other. Network communications are still possible in the presence of CCI albeit with delays. As a result of 802.11 CSMA/CA access control, when a wireless device hears another device transmitting it must wait before it can transmit. Any transmission between an AP and a client on one network can cause another AP and client to hold off communications in the belief that the medium is busy. ACI is caused when multiple APs and/or clients on nearby overlapping channels can hear each other. Even though the devices are on different channels, it is possible for their signals to interfere with the other devices. This phenomenon is mostly likely to happen in the 2.4 GHz frequency band.

Enable ARM to minimize or prevent the effects of CCI or ACI. Doing so enables the Aruba controller to dynamically set the channel and power on the access points. Another setting, Mode Aware ARM, allows the Aruba controller to dynamically convert an access point temporarily to an air monitor when the controller determines that there is too much co-channel overlap.

Receive (Rx) Sensitivity Tuning Based Channel Reuse is yet a third ARM feature that can improve performance in the presence of CCI or ACI. In dense deployments, it is possible for APs to hear other APs on the same or nearby channel. Prior to transmitting data, an access point checks to see if the wireless medium is being used. This is known as a clear channel assessment (CCA). If Rx sensitivity tuning is set to Static Mode, the CCA is adjusted according to the transmission power level of the AP. So

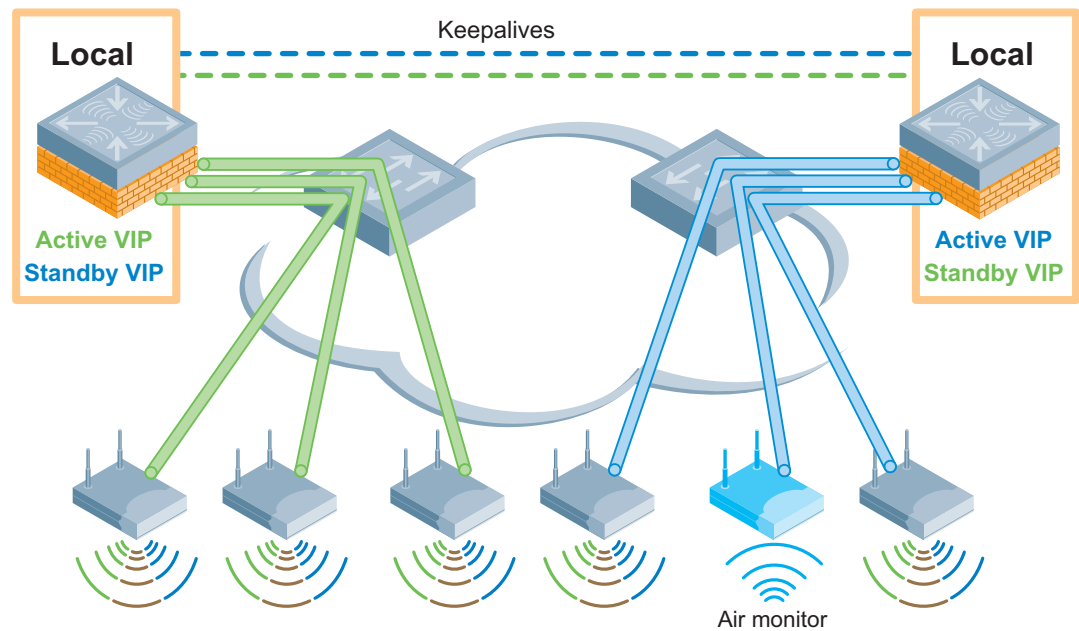
the transmit power of the AP decreases as the CCA threshold increases and vice versa. If Rx sensitivity tuning is set to Dynamic Mode, the controller adjusts the CCA threshold to accommodate transmissions between the AP and its most distant associated client.

Redundancy

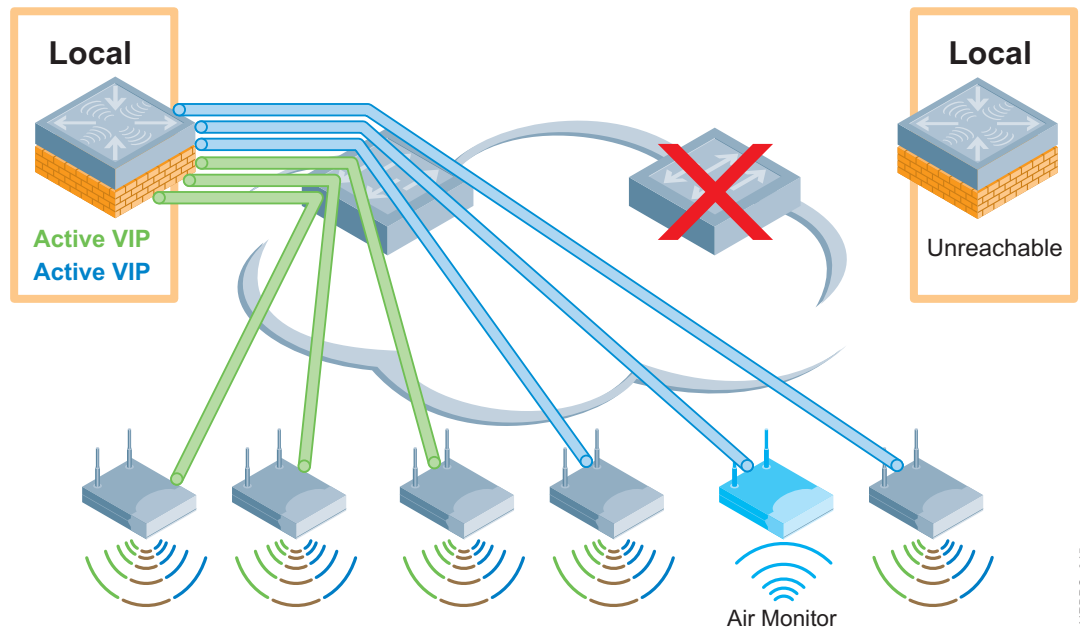
Redundancy helps keep the WLAN working in the event of a single point of failure. We've already discussed how ARM adapts the network to the loss of an AP. Using a technology known as Virtual Router Redundancy Protocol (VRRP), Aruba also provides controller failover to a backup unit in the event of failure or damage.

An Aruba wireless network typically consists of a Master controller and at least one or more Local controllers. Network configuration is performed on the Master and pushed out to the Locals. The Master is also responsible for user troubleshooting, RF planning, ARM decisions, wireless intrusion detection, and location services. Without Master Redundancy, if the Master becomes unreachable, the network will continue to operate as expected, but without the ability to perform operations such as configuration, heat map analysis, intrusion detection and prevention, or location services. If Master Redundancy is deployed, management layer redundancy is provided via dual Master controllers configured in an Active-Standby configuration. Only one Master is active at any one time, periodically synchronizing its configuration and databases with the Standby Master.

Local controllers provide the logical termination for access points and air monitors. If a local controller becomes unreachable, the APs that are logically connected to the Local controller will no longer be able to provide wireless services to the clients. Local controllers can be configured in an Active-Active configuration. Each controller is configured as an Active controller with the other controller configured as its Standby controller. The controllers need to be configured to support a maximum of 50% of their capable load. If either controller fails or becomes unreachable, the APs connected to the unreachable controller will fail over to one of the standby Local controllers, increasing its load to 100%. This first illustration, displayed below, shows two Local controllers, each supporting three access points or air monitors. Each controller is in the active role supporting its connected devices, while acting as a standby for the other controller.



The illustration below shows that when the controller on the right becomes unavailable, the access points and air monitors connected to it will fail over to the standby local controller. Each controller must have sufficient processing power and licenses to support all of the APs that need to be handled during normal and failover operation.



Manageability

Proactively managing your wireless network, effectively troubleshooting the network when problems arise, and continuously monitoring the network are all important activities. In addition to the Aruba Operating System that manages the controllers, the AirWave Wireless Management Suite (AWMS) provides tools and resources to proactively monitor the network and react to problems when they arise.

Aruba Operating System

In addition to its ability to configure the wireless network, the Aruba Operating System provides both a graphical user interface and a command line interface for accessing network status and controller log files. Through either interface, you can look at statistics and logs showing the current settings and status of the controller, access points, and air monitors. Logging information can be sent to a syslog server, and SNMP traps can be sent to an SNMP server.

The controller also has the ability to configure an access point or air monitor to remotely capture wireless packets. This feature allows a network administrator to choose any access point or air monitor on the network and configure it to forward all the wireless packets that it hears to packet analysis software running on the administrator's computer.

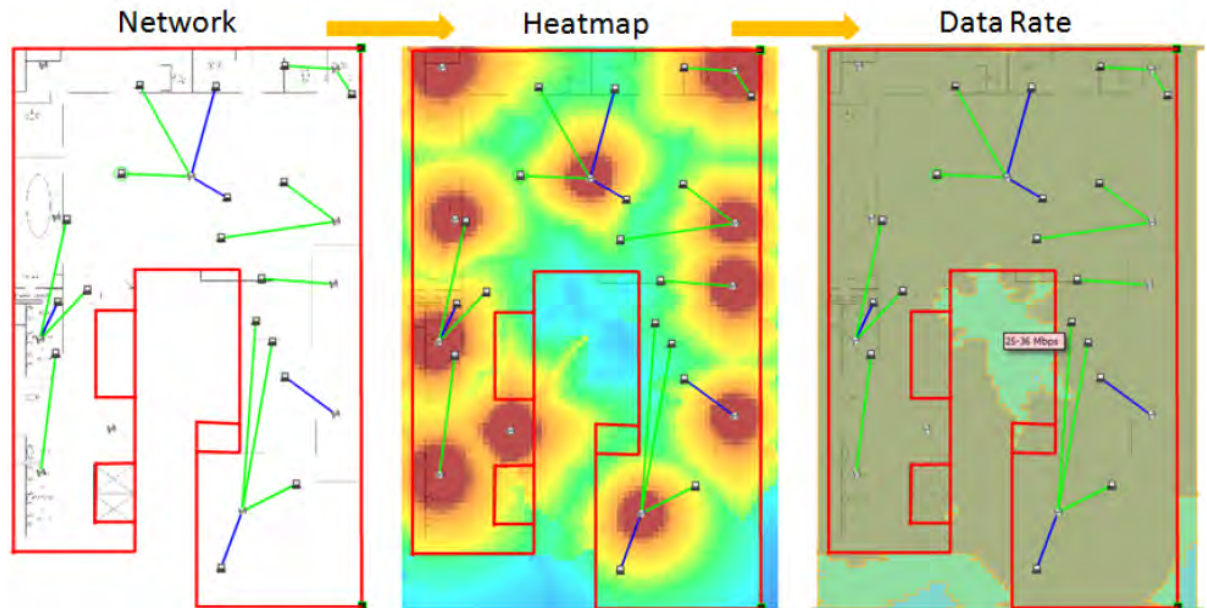
AWMS

AWMS is network management software that provides the IT staff with full visibility and control over the wireless network. AWMS is made up of three components: AirWave Management Platform (AMP); VisualRF Location and Mapping Module; and RAPIDS – Rogue AP Detection Module.

Among other features, AMP provides discovery, configuration management, device and user monitoring, reporting and diagnostics, software distribution, compliance auditing, and real-time data and trend reports for every user, device, and segment of your network. AMP can be configured with different users and levels of permission, providing customized access to resources for all levels of IT staff, from the most experienced network engineers to Level 1 Help Desk support. Access to this

information helps the IT staff better understand current conditions of the network and changes that have occurred to the network, and also give them the tools to both proactively and reactively diagnose and resolve problems.

The VisualRF Location and Mapping module calculates and displays RF coverage maps and location information for every user and wireless device connected to the network. VisualRF uses data gathered from the controller, access points, and air monitors that are installed on the network. VisualRF can be used to proactively manage the wireless LAN by providing real-time views of the network and RF environment. As seen in the graphics below, an assortment of maps can be displayed, including network maps, RF heatmaps, and channel maps, in addition to campus and building maps.



The RAPIDS software module employs a combination of wireless and wired discovery techniques to detect unauthorized rogue access points on your network. RAPIDS can automatically detect and locate unauthorized access points using data gathered from the controller, access points, and air monitors. RAPIDS provides a default set of rules to identify and classify rogue devices. These rules can be modified to fit your network security policy by adjusting or creating new rules. RAPIDS can classify devices as rogue, suspected rogue, unclassified, suspected neighbor, neighbor, suspected valid, and valid. In addition to the RAPIDS classification, RAPIDS can generate a threat level classification, quantifying the threat with a value from 1 to 10. When rogue devices are detected, RAPIDS can generate automatic, high-priority alerts that can be emailed to a specified distribution list. RAPIDS also helps to locate and identify the rogue device by using RF data from existing APs to triangulate the location of rogue devices and display them on a VisualRF map.

If you need Payment Card Industry (PCI) Data Security Standard (DSS) compliance reporting, AMP includes an in-depth compliance reporting feature that evaluates individual managed devices against several PCI requirements to validate that safeguards are working as intended. The report also summarizes any intrusions detected by the wireless intrusion protection system, as well as any detected rogue wireless access points. The screen capture below shows the output of the Daily PCI Compliance Report and includes the PCI requirement, description, and status.

Daily PCI Compliance Report for All Groups, Folders and PCI Requirements		
1/20/2009 12:00 AM to 1/21/2009 12:00 AM Generated on 1/21/2009 12:23 AM		XML (XHTML) export Email this report Print report
<p>This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2 requirements that are relevant to security in your network. PCI DSS standard requirements are available at https://www.pcisecuritystandards.org.</p> <p>Disclaimer: The PCI Compliance Report must be completed by an authorized QSA. The sole purpose of this report is to provide IT administrators with an on-demand internal audit of components which are visible to AirWave Wireless Management Suite.</p>		
Summary		
PCI Requirement ▲	Description	Status
1.1	Configuration standards for router. A device fails if it is in read-write management mode and there are mismatches between the desired configuration and the configuration on the device.	Pass
1.2.3	Install firewalls between any wireless networks and the cardholder data environment. A device passes if it can function as a stateful firewall.	Pass
2.1	Always change vendor-supplied defaults. A device fails if the usernames, passwords or SNMP credentials being used by AWMS to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults.	Pass
2.1.1	Change vendor-supplied defaults for wireless environments. A device fails if the passphrases, SSIDs or other security-related settings are on a list of forbidden values. The list includes common manufacturer defaults.	Pass
4.1.1	Use strong encryption in wireless networks. A device fails if the desired or actual configuration reflect that WEP is enabled or if associated users can connect with WEP.	Pass
11.1	Identify unauthorized wireless devices. A report will indicate a failure if there are unacknowledged rogue APs present in RAPIDS or there are no wireless rogues discovered in the last three months.	Pass
11.4	Use intrusion-detection systems and/or intrusion-prevention systems to monitor all traffic. A report will indicate a "pass" for the requirement if AWMS is monitoring devices capable of reporting IDS events. Recent IDS events will be summarized in the report.	Pass

AMP is a vendor-neutral solution supporting both current-generation products and older legacy gear from most wireless hardware providers. If you are replacing an older wireless LAN, you can use AMP to manage and control the legacy wireless devices as you transition to the new Aruba 802.11n WLAN.

Security

Since Wi-Fi uses an open medium for communications, security is a major concern of most wireless users. Aruba incorporates many layers and levels of security to protect the user, data, network, and RF spectrum. A properly installed, rightsized wireless LAN uses authentication to permit only authorized users to gain access to the network. Data encryption ensures that the user's data remain secure from client to core. The Aruba controller includes a bi-directional stateful firewall that supports identity-based security. The stateful firewall analyzes every wireless frame that arrives at the controller. With identity-based security, each user is assigned a role consisting of a set of firewall policies. Based on the user's identity and the set of rules in the firewall policies that are assigned to the user, the controller

will allow or restrict access to network resources or the Internet. The Aruba controller can also be integrated with a network admission control (NAC) server to validate client configuration prior to allowing the client access to the network.

Even with all of these levels of security built into the network, it is important to monitor the wired and wireless components so that you can identify, locate, and eradicate unauthorized attempts to connect to your network or attempts to disrupt your network. In this section you will learn about the security components that will secure your network and how to configure them.

Endpoint-to-Core Authentication and Encryption

802.1X is an IEEE standard that provides port-based access control. When integrated with Extensible Authentication Protocol (EAP), 802.1X provides a means to securely authenticate users prior to granting access to the layer 2 media, prior to the user even being assigned an IP address. EAP is actually a framework for authentication and not a specific authentication mechanism, therefore different varieties of EAP have been created over the years to provide authentication. The three most popular secure versions of EAP recommended by Aruba include:

- Protected EAP (PEAP)
- EAP with Transport Level Security (EAP-TLS)
- EAP-Tunneled Transport Layer Security (EAP-TTLS)

On the client side, PEAP requires the user to provide a username and password or to have a client-side digital certificate to authenticate the client. PEAP uses a digital certificate on the network side to authenticate the network to which the user is connecting. This provides mutual authentication, certifying that the client is a valid user and that the client is connecting to a valid network. PEAP is very popular and is supported by most client operating systems either directly or through third-party software.

EAP-TLS is an IETF open standard and is defined in RFC 5216. EAP-TLS differs from PEAP in that it requires a certificate on both the client and network side of the connection. Like PEAP, EAP-TLS provides mutual authentication, certifying that the client is a valid user and that the client is connecting to a valid network. EAP-TLS is also popular and supported by most client operating systems either directly or through third-party software.

EAP-TTLS requires the user to provide a username and password, token, or have a client-side digital certificate to authenticate the client. EAP-TTLS uses a digital certificate on the network side to authenticate the network to which the user is connecting. As with PEAP and EAP-TLS, this provides mutual authentication. EAP-TTLS is widely supported across client platforms; however, it is not natively supported by Windows, and PCs require the installation of third-party software.

When configuring the wireless LAN for 802.1X authentication, you also need to determine the type of encryption to use. Advanced Encryption Standard (AES) is considered the state-of-the-art encryption for wireless networks. The 802.11i amendment, which is now part of the 802.11 standard, incorporates AES. The Wi-Fi Alliance's WPA2 certification implements the mandatory components of 802.11i, but not all devices are yet capable of supporting WPA2 and AES.

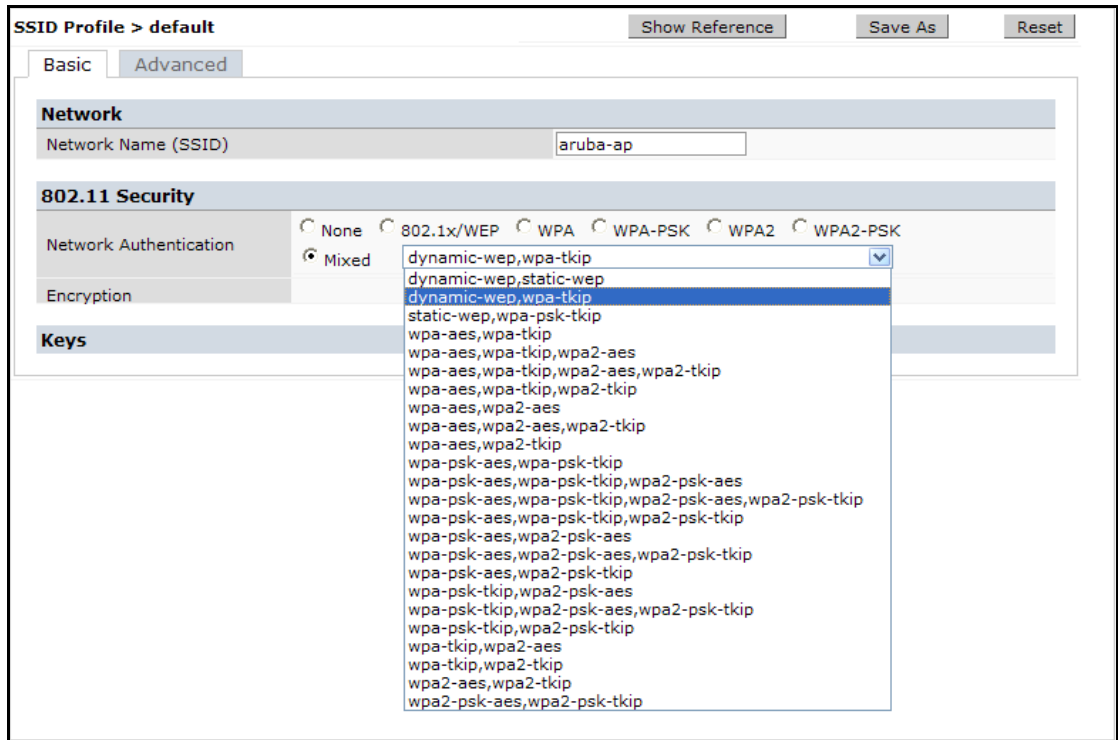
Temporal Key Integrity Protocol (TKIP) is another popular encryption technique that was designed by the IEEE and the Wi-Fi Alliance as an interim solution to replace WEP. The Wi-Fi Alliance's WPA certification was introduced as an interim solution until 802.11i was ratified. WPA implemented much of the 802.11i standard and included TKIP for encryption because, at the time of its introduction, TKIP could be implemented on most existing wireless devices through firmware upgrades. Because it is supported on most wireless adapters, and because of the delay in ratification of 802.11i, over the years TKIP has become extremely popular. In 2008, however, a flaw was discovered in TKIP that could allow an attacker to inject forged packets onto the network. The attack method requires one minute to compromise a byte of data, so setting the TKIP rotation value to an interval of 120 seconds should

prevent an attacker from making significant gains. You can enable this setting on the Master controller using the command line interface by typing in the following commands:

```
enable
configure terminal
aaa authentication dot1x
multicast-keyrotation
unicast-keyrotation
timer mkey-rotation-period 120
timer ukey-rotation-period 120
```

Be aware that not all clients support key rotation (notably some mobile computers, scanners, and VOIP handsets), so you will need to test these changes in your environment. Also note that once a crack or flaw is found in a security protocol, further compromise is likely.

Aruba recommends transitioning to AES as soon as possible. When you do upgrade to AES, you need to block clients from falling back to using TKIP by using one or more of the following configuration modes: wpa-psk-aes, wpa-aes, wpa2-psk-aes, and wpa2-aes. The screen capture below shows an SSID profile in which these configurations can be selected individually - or in groups using Mixed mode.



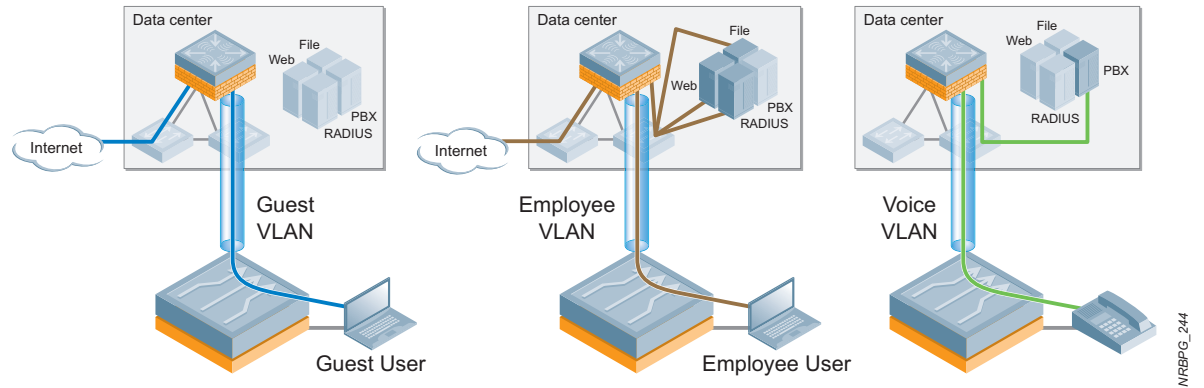
Identity-Based Security

Whenever a user or device connects to an Aruba wireless LAN a “role” is assigned. A role is a set of firewall rules that extend certain rights and privileges on the network. Typical roles include employee, guest, and voice. Often, users will be assigned to the employee role if they log on using an authenticated and encrypted method such as an 802.1X/EAP. Someone with the employee role will likely be allowed access to the internal network as well as access to the Internet. The controller is able to assign specific roles based on a user’s individual identity when he or she logs onto the network.

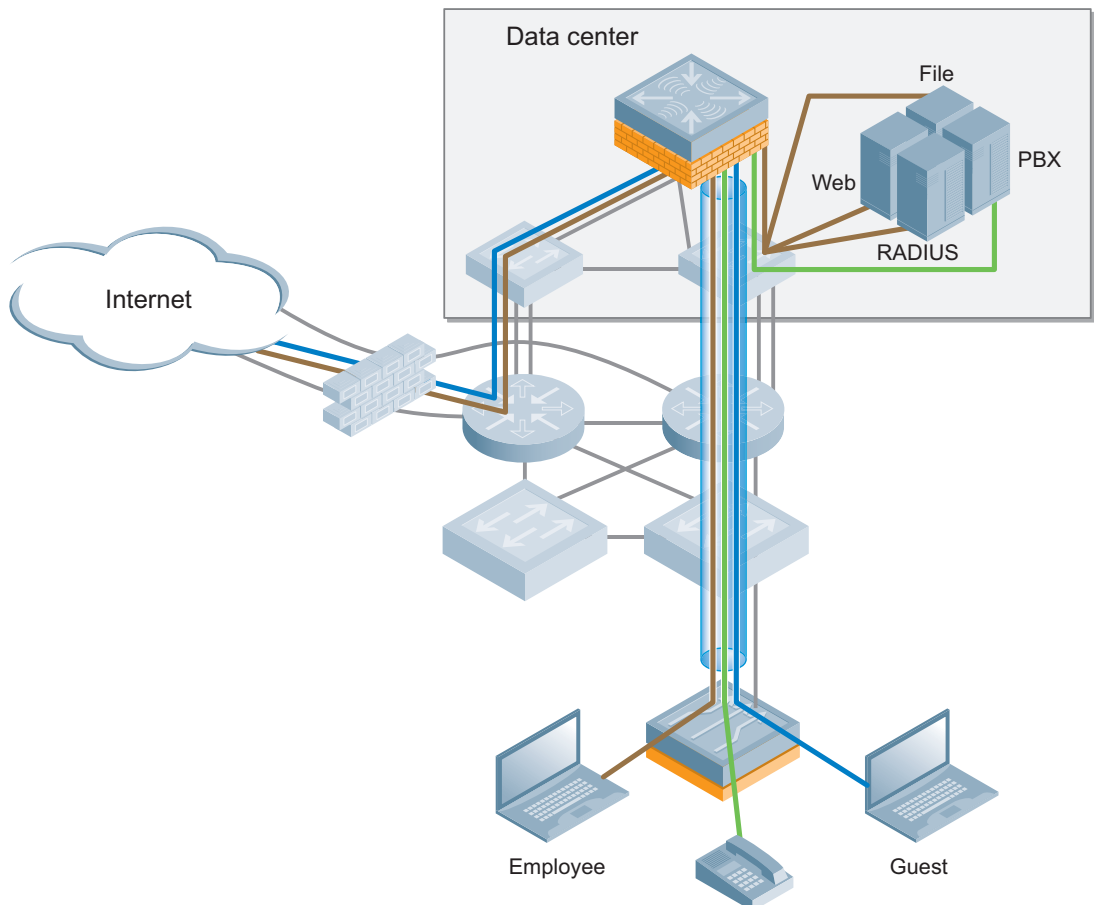
You can configure the controller so that other users who connect using less secure methods, such as captive portal, will be assigned a guest role. Since these users have connected to the network using a less secure method, they will typically be restricted from the internal network and only be allowed access to the Internet.

If you use Wi-Fi enabled handset devices, such as voice over Wi-Fi telephones, you can assign them to a separate device-oriented role such as voice. This role only allows the devices to communicate with the PBX server and function as phones.

The drawing below illustrates the capabilities of each of these roles, and shows the data paths of each associated VLAN. The left drawing shows data on the Guest VLAN that can only travel to the Internet. The middle drawing shows data on the Employee VLAN that can travel to the File, Web, or RADIUS servers, as well as the Internet. The drawing on the right shows phone traffic that can only travel to the PBX server.



The drawing below shows the network with all three VLANs and the paths down which the traffic on each of the corresponding VLANs can travel.



Network Admission Control

Large corporate and educational networks often deploy network admission control (NAC) systems for identity-based policy control, health-based assessment, and network-based protection. Identity-based policy control assesses the user role, device, location, time, and application. Identity-based policy control allows policies to follow users throughout the network, based on the user's identity. Health-based assessment validates the health of a client when it connects to the network. Health-based assessment can check if clients are running updated versions of the operating system and other applications, such as anti-virus software. If a client does not meet the minimal health standards, NAC can be configured to implement automatic remediation of the client, automatically installing the missing components. If NAC is not configured for automatic remediation, clients are typically allowed only enough access to the network to allow remediation to be performed manually. Health-based assessment is not only performed when the client connects to the network, but also on an ongoing basis. Network-based protection uses Aruba's built-in firewall to enforce policies and either blacklist or quarantine clients, based on identity policy controls or failure to pass the health validation check.

The Extended Services Interface (ESI) module provides software APIs and other methods for integration with external devices such as virus bulk scanners, syslog from any device, RADIUS RFC3576 Change of Authorization (CoA) and Disconnect Messages (DM). It also integrates with external captive portals to enable solutions such as credit card billing for captive portal users.

Aruba controllers can be integrated with Cisco's Network Admission Control, Juniper's Unified Access Control (UAC), and Microsoft Network Access Protection (NAP) for wired NAC enforcement.

Wireless Intrusion Protection

Securing a wired or wireless network is not just about protection, but also monitoring the network to identify, locate, and eradicate unauthorized attempts to connect to or disrupt the network. A wireless network should not be installed without a Wireless Intrusion Protection (WIPs) system. No matter how secure your network appears to be, users often connect devices that provide unsecured access to an otherwise secure network. These devices include rogue access points, laptops acting as bridges, misconfigured laptops, and Ad-Hoc networks. Users are often unaware when they are enabling a potential security breach. For these reasons, it is important that the network monitor itself for potential security violations.

You should also to monitor your network for attempts to illegally access or disrupt network operations. Denial of service, packet flooding, forged packets, man-in-the-middle attempts, and encryption cracking are all intentional, active attacks that can disrupt the network. Wireless intrusion protection should be used to constantly monitor and block these types of attacks.

Your Aruba controller working in conjunction with RAPIDS, a component of AWMS, and air monitors can perform many of these tasks. An air monitor can scan all of the 2.4 GHz and 5 GHz frequencies, whereas an access point can only scan the channels that are supported by the local regulatory domain. As an example, in the United States, an air monitor is allowed to scan the 2.4 GHz channels 1 through 14, whereas an access point is only allowed to scan the 2.4 GHz channels 1 through 11. Since it is not uncommon for an attacker to hide an access point by using one of the channels that are outside the regulatory domain, air monitors can provide additional network security.

Scalability

It is important to design your wireless LAN to support both your current and future networking needs. The network needs to be able to easily support additional access points and high-speed clients that could be added in the future.

Performance

Aruba controllers can support as many as 2,048 APs and are designed to handle high sustained throughout levels. Multiple Aruba controllers can be configured in a Master/Local architecture if more than one controller is required. The first controller is configured as the master and each of the additional controllers are configured as locals. The installation of additional controllers typically occurs when it is necessary to support additional APs. Configuration and management of the network is performed on the master controller, and changes to the master are automatically pushed to the local controllers.

All of the Aruba controllers use the same operating system software, so you can add any controller model to your network as needed.

Overlay Architecture

Another scalability benefit of the Aruba wireless LAN is its overlay architecture design. Controllers and access points can be installed on the existing wired network. The devices communicate with each other over the backhaul Ethernet network without requiring a redesign of the existing infrastructure. As long as the underlying network can provide bridging or routing of IP packets between the Aruba devices, the WLAN will work properly.

L2/L3 Mobility Design Considerations

One of the primary objectives of a WLAN is to provide seamless client roaming. This can be accomplished by configuring the network for either layer 2 (L2) or layer 3 (L3) roaming.

L2 roaming maintains application connectivity within the roaming domain as long as its layer 3 network address (IP address) does not change. In an L2 design, the client maintains its IP address as it roams across APs or controllers. The client is always assigned an address from the same IP subnet irrespective of the controller or AP to which it associates. A general rule of thumb is to limit the number of devices per subnet to 253, however, this number can vary depending on the protocol used and the amount of broadcast or multicast traffic the protocol generates.

L3 roaming sees the user handoffs from an AP on one subnet to an AP on another subnet. In a typical environment, when the user connects to the new network, the client obtains a different IP address on the new network. Aruba's layer 3 mobility utilizes the Mobile IP protocol standard (RFC 3344, "IP Mobility Support for IPv4"), which allows the client to roam to the new AP and maintain its active IP address, even though it is roaming to a different subnet. The Aruba controllers perform the tasks required to enable clients to roam within the mobility domain. This solution does not require software be installed on the client devices.

The chart below compares Layer 2 and Layer 3 roaming.

Layer 2	Layer 3
Easy to configure	Planning required before configuration is implemented
Provides fast roaming times	Works with VLAN pooling
Works well with VLAN pooling	Controllers within mobility domain don't need to share same subnet
All wireless MAC addresses are stored in every controller bridge table	Controllers do not need to be L2 connected to each other
Controllers within VLAN mobility domain must share same subnets	L3 session state is synched between controllers
Controllers within VLAN mobility domain need to be L2 connected	IGMP does not work when client has roamed
L3 session state is not synched between controllers	

Contacting Aruba Networks

Web Site Support	
Main Site	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Software Licensing Site	https://licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
• Americas and APAC	support@arubanetworks.com
• EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Telephone Support	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
• United States	+1-800-WI-FI-LAN (800-943-4526)
• Universal Free Phone Service Numbers (UIFN):	
■ Australia	Reach: 11 800 494 34526
■ United States	1 800 9434526 1 650 3856589
■ Canada	1 800 9434526 1 650 3856589
■ United Kingdom	BT: 0 825 494 34526 MCL: 0 825 494 34526
■ Japan	IDC: 10 810 494 34526 * Select fixed phones IDC: 0061 010 812 494 34526 * Any fixed, mobile & payphone KDD: 10 813 494 34526 * Select fixed phones JT: 10 815 494 34526 * Select fixed phones JT: 0041 010 816 494 34526 * Any fixed, mobile & payphone
■ Korea	DACOM: 2 819 494 34526 KT: 1 820 494 34526 ONSE: 8 821 494 34526
■ Singapore	Singapore Telecom: 1 822 494 34526
■ Taiwan (U)	CHT-I: 0 824 494 34526
■ Belgium	Belgacom: 0 827 494 34526

Telephone Support

■ Israel	Bezeq: 14 807 494 34526 Barack ITC: 13 808 494 34526
■ Ireland	EIRCOM: 0 806 494 34526
■ Hong Kong	HKTI: 1 805 494 34526
■ Germany	Deutsche Telekom: 0 804 494 34526
■ France	France Telecom: 0 803 494 34526
■ China (P)	China Telecom South: 0 801 494 34526 China Netcom Group: 0 802 494 34526
■ Saudi Arabia	800 8445708
■ UAE	800 04416077
■ Egypt	2510-0200 8885177267 * within Cairo 02-2510-0200 8885177267 * outside Cairo
■ India	91 044 66768150