802.11n Planning and Network Management

Tash Hepting & David Cohen
Trapeze Networks

enterasys® Secure Networks™

802.11n Planning and Network Management

Introduction – What is 802.11n and why is planning and management necessary?

802.11n is the next generation of wireless LAN technology which provides a dramatic increase in range and throughput over legacy 802.11a/b/g equipment. This is accomplished through multiple-input/multiple-output (MIMO) radio technologies, bonding adjacent 20 MHz wide channels together for higher bandwidth 40 MHz wide channels, and efficiency enhancements to the underlying 802.11 protocol itself. While legacy clients will experience a modest increase in range, the full impact of 802.11n isn't realized without both 802.11n capable clients and access points.

The improvements in range and throughput directly translate into a more robust wireless experience for 802.11n networks. More consistent signal levels and reductions in "dead-spots" allow voice applications to reach new levels of reliability, even in difficult environments. Higher data rates and more efficient use of the air make video and other emerging high-bandwidth applications practical, enabling the use of Wi-Fi as a primary network access method for enterprise users.

However, an 802.11n network that is not properly planned and managed can result in a tremendous waste of money and time while failing to deliver on its promises. The technology, while offering tremendous benefits, can quickly become an expensive and frustrating exercise in trial and error. Too few or misplaced access points can leave coverage holes, while too many access points, aside from being a waste of money, can result in self-interference, canceling out the benefits.

In this paper we will examine how to professionally plan, configure, and manage a Wi-Fi network that includes both 802.11n technology and legacy 802.11a/b/g technology so that the end result is an enterprise-class networking experience that delivers nonstop wireless service for all its end users. We'll describe how planning and management for 802.11n is different than for legacy Wi-Fi technologies, and we'll discuss what a network manager should expect of enterprise-class wireless network management tools.

RF Planning for an 802.11n network

Wi-Fi is rapidly becoming a fundamental access technology for the enterprise and 802.11n is a key component which will accelerate this transition. With the enterprise's increasing use of Wi-Fi, the need for a robust and reliable wireless network becomes paramount. The primary challenge for a wireless network administrator is to design a network which delivers both top performance and a level of reliability suitable for the organization's most important network applications. 802.11n can deliver the raw technology to make this a reality, but in order to properly utilize it, you need to carefully plan your deployment. A proper RF planning tool will take into consideration all of the technical aspects of 802.11n and your organization's particular needs to assist you in every stage of your wireless deployment.

Planning your 802.11n access point (AP) placement requires a sophisticated RF planning tool with an intuitive work flow. Increases in range from 802.11n's MIMO technology vary with the type of client, the frequency band the client is operating on, and the environment. How do you plan for all combinations of legacy 802.11a/b/g and 802.11n clients, in both 2.4GHz and 5GHz bands, and in different physical environments that affect the RF footprint of coverage? Taking a best guess will likely result in frustrating trial and error while testing all these combinations in a traditional site-survey is prohibitively expensive in terms of time and labor. A better approach is a tool that can predict coverage for any combination of clients, and therefore enables you to provide quality service to all clients, on all channels, tuned to your specific environment. By accurately modeling your environment, the RF obstacles within, and the types of clients, you have the ability to perform "what-if" scenarios to see how coverage and capacity can be optimized for different budget levels and different service offerings, such as data, guest access and voice. The end result is an accurate RF plan that leverages 802.11n technology as it applies to your needs and budget, without excessive cost in time, labor, or dollars.

Even after the initial plan is implemented, good RF planning tools are still useful. Without them, you would not have sufficient information to grow and adapt your network to the changing needs and applications of your users. A full lifecycle RF planning tool will allow you to fully leverage the work you've already put into your wireless network plan as well as give you a platform to grow on to upgrade or change the network over time. It will help you find the most cost-effective way to address changes in intended coverage, the number of wireless users, or adding services such as voice to your network.

Planning for pure 802.11n networks

A wireless network composed entirely of 802.11n clients and access points has a different set of planning requirements from one which will coexist with the legacy 802.11a/b/g network. Because most organizations are loathe to throw away their existing equipment, and Wi-Fi Certification of 802.11n products ensures backwards compatibility with legacy Wi-Fi gear, a pure 802.11n deployment is typically only done as a new deployment. This type of deployment typically can be categorized in one of two ways. If the organization wants to plan only for maximum coverage, but data rates are

not important, the access point density may be significantly less than that typical of legacy wireless networks and the organization can save money on the wireless infrastructure investment. If the organization wants to plan for maximum performance and throughput, then the access point density may be about the same as legacy networks but the placement of APs would likely be different. A good 802.11n-capable RF planning tool will accommodate either scenario by determining the optimal number of access points and their proper placement.

Planning for mixed 802.11 a/b/g/n networks

Many 802.11n wireless networks will be a mix of legacy and new technologies, which presents a unique planning challenge. 802.11 a/b/g uses only 20 MHz wide channels and has limited data rates and range, whereas 802.11n uses both 20 MHz wide channels and 40 MHz wide channels and has much higher data rates and longer range. Without proper planning, the legacy 802.11 a/b/g technologies can actually detract from the overall system performance improvement benefit of 802.11n by unnecessarily forcing 802.11n to downshift to lower speeds than necessary. Moreover, there are different mixed technology scenarios, each with its own challenges.

Some deployments will feature networks built entirely from 802.11n access points but with a mix of client technologies. Some may initially deploy 802.11n access points solely in high-usage or challenging RF environments, but continue to utilize the existing legacy 802.11a/b/g access points for general coverage. Other organizations may plan to migrate both their APs and clients to a pure 802.11n network eventually but will want to continue to leverage their investment in legacy 802.11 a/b/g technologies in the meantime. Each of these causes different interactions among the 802.11n access points and clients and the legacy 802.11 a/b/g access points and clients and must be professionally planned to obtain the promised benefits.

An obvious path for many organizations is to take down the old 802.11 a/b/g APs and place the new 802.11n AP's in the exact same location because the Ethernet drop is already there. However, this approach has issues too, because 802.11n's RF footprint is dramatically larger. While that's generally a positive, without proper planning to adjust power levels and channels the new access points may cause interference with each other.

In order to properly plan a mixed network, an RF planning tool must have detailed information on the legacy 802.11a/b/g infrastructure as well as the 802.11n access points, and specific details about the building and its construction materials, which can be imported from a CAD file in the better tools. It then uses that information plus guidance from the wireless network administrator on which physical areas require what level of coverage to develop the plan.

Since service is expected for both legacy and 802.11n clients, access point placement and properties will be based on both the shorter range legacy clients and new 802.11n clients. The planning tool must ensure that the access points will be placed in the optimal locations so that shorter range legacy clients can still connect to the network while longer range 802.11n clients can maintain their high data rates. This is not something that can be done via trial and error, therefore a good planning tool is absolutely required to realize the benefits of higher speed, range and coverage that 802.11n promises in the mixed environment scenario.

Special 802.11n planning considerations

"Hot Zones" – high density areas

Most deployments will have areas of high activity and usage. For example, in corporate offices, conference rooms may require higher amounts of wireless network capacity, or in university environments you may have auditoriums with hundreds of students connected to the wireless network at the same time. An RF planning tool should address this need by allowing you to identify "Hot Zones" and then planning for the higher capacity requirements specific to that area while simultaneously coordinating the RF coverage with the rest of the wireless network. These "Hot Zones" are primary candidates for upgrading to 802.11n access points, especially as the client population migrates to 802.11n, but are useful even with legacy clients.

Planning for throughput vs. planning for coverage

When planning your deployment you should consider the coverage and throughput requirements that are appropriate for the applications that will run on your network. Voice and location services demand a consistent and higher-density style of deployment, while traditional data services can work well by scaling the access point density solely according to the client density. Planning for future applications and client growth is also important, particularly for an 802.11n network that is expected to provide service for several years.

A complication created by new 802.11n access points is support for 40 MHz wide channels, which enable the fastest data rates, but also reduce the total number of channels available on the network. Another issue is the additional DFS2 channels offered in the 5 GHz band. These are an unqualified positive, but not all 802.11n gear supports them. With DFS2, up to 21 channels will be available at the original 20 MHz width, and up to 9 at the new 40 MHz width. Therefore, the number of channels actually available for your use will vary with the capabilities of the client devices as well as the regulatory certification of the access points. In certain cases you may have only 9 20 MHz channels or 4 20 MHz channels available for use, especially if the access point uses older generation 802.11n chipsets that are not DFS2 compliant.

In the 2.4 GHz band, there are only three 20 MHz wide channels and only one 40 MHz wide channel available. Most legacy clients and some new 802.11n clients operate only in 2.4 GHz, so this too must be factored into the RF plan. Legacy clients can operate in the same band as 802.11n clients, but will only be able to connect at 20 MHz channel widths and at lower speeds which lowers system throughput for all clients. Furthermore, there is a system tradeoff between the higher throughput available from a 40 MHz channel and the benefit of having additional 20 MHz channels available to plan with.

In cases where there is a significant majority of legacy clients in the population, or an extremely dense access point deployment with a concentration of clients, it may be preferable to use 20 MHz channels to improve the overall efficiency of the network. As the ratio of 802.11n to legacy clients improves, as well as compatibility with the newly available 5 GHz DFS2 channels, 40 MHz channels become a better choice. A full life-cycle RF planning tool will help you plan and configure your wireless network for the best balance of throughput and coverage, without having to know such technical details and will allow you to update the configuration on your network as technologies evolve.

Good RF planning tools offer built in templates to plan for your choice of maximum throughput or maximum compatibility for legacy clients. By selecting your preference, all the technical settings are automatically applied, such as whether 20 MHz or 40 MHz channels will be used, whether the optional short guard interval should be turned on, and whether legacy clients will be allowed to join the network. The best RF planning tools can accommodate both maximum throughput and maximum compatibility by setting up the 2.4 GHz band for compatibility with legacy 802.11 b/g clients while preserving the 5 GHz band for best throughput servicing 802.11n capable clients only. This is proving to be a very popular deployment method.

Configuring Services on your Wi-Fi Network

After planning is complete, a good management tool will guide you though the configuration process. Configuring allows you to create various services on the same network. The primary service is typically the WPA2/ 802.1X highly secured corporate data service for full time employees, but you may want to configure other services, such as a Voice over Wi-Fi service, a guest access service, and in some cases a location-based service to track the location of physical assets in real time. A good management tool will allow you to easily and intuitively create all these services on the same network with the same physical infrastructure of WLAN controllers and access points.

While configuring services is a key element in the management of any Wi-Fi network, there are certain services that are unique to 802.11n. As mentioned above, special high traffic 802.11n "Hot Zones" can be set up in areas where network traffic is often most congested, for example, for an auditorium or conference room where many people typically congregate. This is a useful way to benefit from the high capacity of 802.11n while still utilizing your existing 802.11 a/b/g infrastructure for other services. Another example is a video distribution service over 802.11n, which typically cannot be supported on the legacy Wi-Fi technologies of 802.11 a/b/g.

Built in voice support can be valuable to organizations that are deploying voice services on their Wi-Fi network now or may do so within the next few years. The better management tools have voice services built in so that technically confusing decisions for voice such as whether WMM or WMM-PS should be turned on or not need not be exposed to the network manager. Some tools include built in support for the most popular voice over Wi-Fi handsets such as SpectraLink, Vocera, Avaya, etc., further easing the deployment.

Regardless of the speed of the Wi-Fi technology, a good management tool will enforce common policies across the network so that a user that is authenticated at a certain security level with related authorization attributes will find that same level of authorized access regardless of where the user roams in the network. For example, you would not want to have a user authenticated for normal corporate data services on one side of the building – limited to email, Web browsing, and Intranet – suddenly have access to sensitive human resource or finance records on the other side of the building.

Larger organizations may also find valuable the ability to configure different services in different locations. For example, IT may want to configure primary 802.11a/b/g corporate data service secured by WPA security in all locations, while simultaneously piloting a new 802.11n corporate data service secured by WPA2 security in just one geographical site, or one building.

An often overlooked aspect of configuration is the ability to handle multiple IT managers who are working on configuring different services. Sometimes different IT users will also use different configuration methods as the same network management tool may allow configuration via the software application GUI, web-based configuration, and even command line interface (CLI) configuration. A good management tool will allow multiple users and multiple interfaces and synchronize them all in the configuration phase.

Deploying Services on your Wi-Fi Network

Configuring alone isn't useful if you don't deploy what you've configured. Yet many Wi-Fi network management applications simply treat deployment as just the next click after configuring – the "go" button. But there are important details to deployment that a good management application will address. Perhaps the most important is ensuring that the deployment is "atomic", meaning that the entire wireless infrastructure has been configured properly all at once to reflect the desired settings from the configuration phase. Consider a large deployment with 50 WLAN controllers and 2,000 Access Points. Imagine the IT headache if after deployment, most but not all of the controllers and only some of the Access Points were properly configured. IT would have to manually check each device to ensure it had the new operational image and proper settings. What good is a centrally managed network in this case? This is why a good management tool's deployment function checks and ensures that every device of the Wi-Fi infrastructure has been properly configured to match the settings intended. If it can't verify this, it rolls back each device to its original settings until the deployment can be verified.

Good deployment tools allow the network manager to schedule flexible deployments, which can be useful when managing large, multi-site networks across the country or the globe. For example, an IT manager may want to deploy voice services at the San Jose, CA headquarters site first without deploying voice in the London and Paris sites. Having the flexibility to deploy on certain equipment types but not others can sometimes be valuable. For example, a network may have physically installed all the access points necessary for the intended upgrade to 802.11n, but for now may want to deploy voice and guest access services using only legacy 802.11 a/b/g access points. IT can then go back later and turn on the 802.11n APs when they are ready.

Deployment tools can also assist in keeping the wireless network running properly by ensuring that each infrastructure device is running the most current software image available (often called firmware). A sophisticated management tool can link to the infrastructure vendor's support Web page, check for firmware upgrades, and download and install them automatically. Some will enable a "perched" upgrade option, where all the firmware upgrades are downloaded and ready to be installed, but then check with the IT manager for approval before actually deploying the upgrade. In the event that an upgrade was accidental or had unintended effects, a good tool will allow rollback to the previous stable state.

Monitoring the Network

Once deployed, the network should be up and running. Some wireless network management applications are obsolete at this point, but the better tools continue to offer valuable services to IT managers. Monitoring is a key function after deployment. IT will want to know that all the equipment is still up and running, or if there is a problem, what it is so it can be addressed. A good management tool will monitor the up/down status of all the access points, all the WLAN controllers, and all related devices such as Wireless Intrusion Detections Systems (WIDS) sensors, Location Appliances and other specialty equipment in the Wi-Fi infrastructure. It should provide a clear view of component availability of the various elements of the entire wireless infrastructure. This is particularly important with a new technology like 802.11n in its formative stages. The tool can show status of the network as a whole, or zero in on sections of it, such as a geographical site or single floor of a building.

Some tools can monitor client status with details that provide network administrators valuable insight into the mix of client device types on the network and when and why client failures occur. This gives network administrators an advantage in providing reliable service and quick resolution to their end users. Monitoring should be real time for the most accurate picture possible, but also be able to provide historical data and trends. Sophisticated monitoring applications periodically run audits for serious conditions like missing or incorrectly-configured equipment and services. If a problem is found, an alarm or notification is generated automatically.

In addition to monitoring the state of the physical wireless infrastructure, the network management tool can monitor wireless network traffic and provide both high level aggregate views as well as detailed device-by-device or client-by-client network traffic patterns. This can be useful for spotting a problem area or may provide input for future planning of the network. For example, if the IT manager sees that Zone C of the building regularly has a much higher volume of traffic than other zones, the IT manager may want to deploy more access points in that area, or deploy an 802.11n high capacity Hot Zone.

The better management applications provide a lot of information at a single glance while also enabling the IT manager to drill down into detail. They can allow the IT manager to determine the up/down status of each device on the wireless infrastructure, see client traffic by type of technology, view historical traffic patterns over different time periods, and view a summary of alarms generated by the system. Some tools prioritize alarms for the IT manager into useful categories such as informational, medium, high and severe. They can also give the IT manager the ability to customize the alarm categories, and prioritize the alarms based on the needs of the organization.

Reporting

In addition to real time monitoring, historical reporting can be useful for record keeping and for spotting long term trends on the network. The better management applications include a wide range of predefined reports, including equipment inventory, client session summary, rogue device summary, controller configuration, and equipment installation. Reports can be run on customizable criteria and can be generated on the spot or according to pre-defined schedules. Some applications offer the ability to have the reports sent to the IT manager by email or make them accessible via secure Internet connections.

A work order report can be generated by some applications which can be a useful output from the planning phase. The work order can list the specific brands, models, and types of equipment needed for the desired deployment. The work order can be given to the vendor or to the organization's IT partner such as a system integrator or value-added reseller so that the right equipment is ordered and installed.

Scaling the Network

By definition, centralized management implies that the organization has a relatively large network, certainly larger than a few access points that may be found in a home or small business. Yet many management applications were simply not designed for the large deployments of 2,000, 5,000, or even more access points that are becoming increasingly common today. The better management applications allow you to scale and grow your network smoothly, whether you started small but have grown rapidly or whether you installed a large network from the beginning. They will be just as useful to you whether you are managing a single site or managing hundreds of sites across the globe, and they will scale with you without compromising the critical management features.

Compliance and Auditing

A wireless network management application isn't typically thought of as a tool to help ensure legal compliance, obtain industry certifications, or comply with auditing requirements. Yet the better management tools have extensive historical record keeping capabilities which can provide the organization with much needed records to comply with various governmental and industry requirements. Some examples of these include Sarbanes-Oxley for all US corporations, Payment Card Industry (PCI) for the retail industry, Health Insurance Portability and Accountability Act (HIPAA) for the medical industry, Federal Information Processing Standards (FIPS) for government agencies,Technology Integration Center (TIC) for the US Army, or simply the detailed

auditing requirements of organizations in sensitive areas such as banking and financial services. Having extensive auditing and historical record keeping capabilities built in to the wireless network management application can save the organization a tremendous amount of time, expense, and headache as it strives to comply with these various requirements.

Integration into Other Applications

As good as any stand-alone Wi-Fi network management application may be, some organizations have standardized on classic wired network management applications such as Hewlett Packard's OpenView, IBM's Tivoli, or Computer Associates' Unicenter®. A good wireless network management application supports this by shipping with an extensive set of application programming interfaces (APIs) that allow developers and system integrators to weave the specialized functionality of the wireless network management application into the organization's existing management tools. The API's should enable the flow of all relevant data from the wireless network management application such as device status, data traffic trends, service state, alarms, client session details, and key report elements. However, in many real world implementations, even when integrated into the organization's existing wired network management tools, the wireless network management application is still utilized. For example, some organizations may use HP OpenView to monitor the entire wired and wireless network (thought the APIs) from one screen but for detailed troubleshooting on the wireless network, the wireless management application is still utilized. As such, one reinforces the other.

Implementation

A final but often overlooked consideration is how the organization will implement the wireless network management tool. Often, such tools are sold as server software. While useful, this requires the organization to purchase or dedicate a computer server for this purpose and ensure the server has the proper, compatible operating system and patches, a large enough hard drive, and a powerful enough microprocessor to run the server fast enough to be useful under the load of a busy network. Then when the organization grows, these severs sometimes have to be upgraded and reconfigured to manage the growing network. Some companies offer the option of a dedicated hardware appliance that is built, dedicated, and pre-configured to the wireless network management task. While typically more expensive at face value than server software, these costs are often recouped when considering the server and related hardware expenses, license costs of the operating system where applicable, and the IT time to do all the configuration.

Conclusion

802.11n is a promising technology and a major technical breakthrough for Wi-Fi networking. Its significant increases in data rates, throughput, and range will permanently change the way Wi-Fi networking is done in the workplace. However, it is also a complex technology that introduces a set of issues whether it is deployed in a brand new environment or as a migration from an existing legacy 802.11a/b/g network. If not properly planned, configured, and managed, 802.11n can quickly turn into a dissatisfying waste of an organization's time and resources while failing to achieve the promised benefits. To avoid this and fully realize the benefits of a seamless, robust, always-on wireless network, a fully featured sophisticated wireless network management tool is essential.

Enterasys Networks RoamAbout Switch Manager (RASM) Advantage

The primary purpose of this paper has been to discuss the key requirements and best practices of a sophisticated enterprise-class Wi-Fi network planning and management tool, especially as an organization considers deploying 802.11n. At Enterasys Networks, we have strived to develop and deliver the best wireless network management tools available. Our network management tool, RASM - (RoamAbout Switch Manager), has won its share of industry awards, but more importantly has helped thousands of organizations to better manage their wireless networks every day. We invite you to learn more about RASM and what it can do for your organization. Please visit us at www.enterasys.com for more information.

Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082, or +1-978-684-1000 and visit us on the Web at enterasys.com

Thought Leadership
Patented Innovation

06/08

enterasys® Secure Networks™

Delivering on our promises. On-time. On-budget.