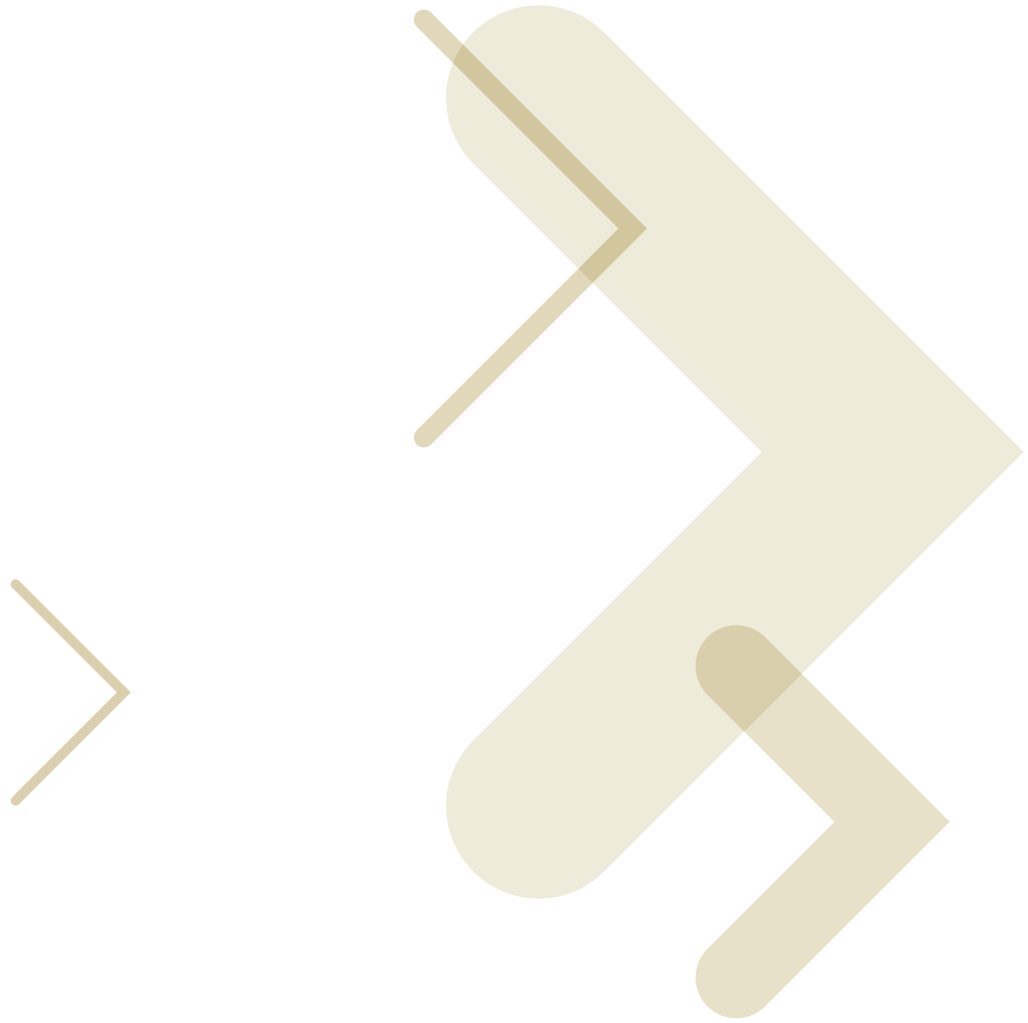
WHITE PAPER

Control your network: Comprehensive management for demanding wireless networks



Executive Summary

There are four basic components essential to wireless network management: planning, security, monitoring and analysis, and management of both network and client devices. However, until recently, administrators have had to either address each component individually, or use an "off-the-rack" management solution – often not even designed for wireless networks.

Motorola's suite of RF Management tools changes that with flexibility to suit the needs of various distributed wireless networks. Mobility Software Platform (MSP) RF Management Edition, LANPlanner, RF Management Software and Wireless Intrusion Protection System (Wireless IPS), used together or independently, can be used to tailor a network management system to the needs of a specific network and the enterprise it serves. Even more powerful when used together, this suite of network management tools share data, as well as a single command console, which is key in an integrated network management system.

Network management overview

Network management is a critical component of any IT organization's responsibilities. Network security, performance and, in many cases, compliance is of paramount importance in maximizing productivity and remaining competitive in today's business environments. While any given organization may have its own specific requirements for network management, there are four basic components involved in managing any network:

- Network Planning: determining optimal network set-up and planning for growth based on the environment(s) in which a network will be deployed and the requirements of the applications that will use it
- Network Security: Keeping data and applications out of the hands of unauthorized users, and in many cases, ensuring standards compliance
- Network Analysis: Monitoring and reporting of key performance indicators in a network to give an overall view of network health, to document standards compliance, and to aid in troubleshooting of any issues
- Device Management: Monitoring, updating or shutting down devices on the network, or components of the network itself

Many IT groups use a different tool for each of these tasks, and often those tools don't work together. This requires the use of several different network interfaces, and can also require the re-keying of data that exists in one system into another, which can be both slow and prone to error. This also means that an administrator can only see one aspect of the network at a time — in fragments — there is no holistic view of overall system health.

Of course, there are products packaged as complete management solutions, which incorporate all of these functions into a single tool. These can be useful when all components are required, but what if you only need three of the four components? Or two? And does each of the components that you will use meet your needs? In network management one size does not fit all.

Another vital part of network management is obviously the network administrator. It is important to take into account where the administrator is physically located in relation to the network components, and how proximity will impact his or her ability to perform network management duties. Is the network in a single site? Is it a distributed network that needs regional policies applied? Or perhaps it's a very large, distributed network serving tens of thousands of connected devices—all of which need to be managed from a single location, such as a NOC.

Clearly, the larger and more complicated the network, the more critical each of the four pieces of network management – planning, security, analysis, and device management – becomes.

WLAN planning

Determining what equipment a wireless enterprise network will require is already a complex task. One must consider how many connected devices will be supported and over what range, what applications will be used and by how many users, which of those applications will be bandwidth-intensive, and which, if any, applications' or users' network traffic should be prioritized. But to properly plan a wireless network, one must also consider the environment. Are there structures likely to cause interference? Are there areas that don't require coverage? Are there specific locations where high bandwidth is more likely to be required?

Does a network administrator also need to be an RF expert to create a robust and reliable wireless network?

In fact, because network planning can be so complicated, it is often done by one group and then handed off to another for implementation. So, how can one be sure that the network that was planned is the one that was implemented?

Fortunately, with the right tools, a company doesn't need an in-house RF expert, and one can easily compare the planned network to the implemented network, even if they were created by two different groups.

One such tool is LANPlanner, from Motorola. Available as a stand-alone tool or as part of Motorola's RF Management Suite, it allows a user to import a site map and input information such

Special Considerations for Managing Wireless Networks

Although they share standard elements and mechanisms, wired and wireless networks have significant differences. In addition to the conventional wired network, wireless networks have the following unique characteristics:

- Secondary hierarchy (association) – The wireless network environment is hierarchical, with mobile units attached or associated to a given access point
- Roaming – Dynamic cell connection or roaming between access points.
- Persistence of mobile units (MU) – Hand-held terminals are turned on and off frequently throughout the day, making it difficult to monitor these devices.

SNMP agents – Hand-held terminals typically run DOS and have limited memory and processor speed resources, making it difficult to provide SNMP agents for these devices. As a result, many MUs do not have SNMP agents.

as coverage needs, application requirements and physical barriers. A site design is created from which the infrastructure can be installed. Once the wireless LAN infrastructure is installed, Motorola's Site Scanner can be used to validate that the wireless coverage meets the expectations of the site design. Alternatively, an administrator may use Site Validation to import a site directly from LAN Planner, and use the real time heat map feature to validate coverage. After validation, the site plan can then be imported into Motorola's RF Management Software, eliminating the need to re-enter the data and allowing the administrator to start managing the network immediately, without further software configuration.

WLAN security

Security for a wireless network is especially important, since it is virtually impossible to "see" a wireless security breach. Additionally, depending upon the type of enterprise the network is serving, there may be certain security-related compliance standards that must be met, such as HIPAA, PCI and Sarbanes-Oxley.

An administrator should be able to locate and disable rogue APs remotely, lock down lost or stolen connected devices, provide a line of defense from wireless attacks, and perform compliance checks. All network components should be using the most powerful encryption available.

Naturally, employees must still be able to access the network, and in many cases, outsiders must be allowed some basic level of internet access without compromising network security.

Again, this delicate balancing act is easily achieved with the right tools. Motorola's enterprise WLAN switches and access points have many security features built in, such as hotspot provisioning for secure guest access, WPA/WPA2 encryption, and intrusion detection and protection with anomaly analysis, as well as detection of rogue APs and denial of service (DoS) attacks. Motorola's Wireless IPS uses locationing capabilities to detect and alert administrators to the presence of rogue APs,

and MSP RF Management Edition will allow an administrator to lock down specific client devices in case of loss or theft.

A unique feature of Wireless IPS is the ability to collect historical data on system activity, and perform forensic analysis of past events. The ability to replay events and provide proof of compliance can save a company thousands of dollars in fines should a breach occur while the system is in compliance.

WLAN monitoring and analysis

With the network up and running, and security in place, an administrator's thoughts turn to monitoring and analysis. These functions allow an administrator to keep an eye on the health of the network, to act on potential issues before they create problems, and to troubleshoot any problems that do arise. One's choice of tools for these tasks is especially important in a distributed environment, where the administrator can't simply investigate reported outages by walking to that spot and searching for a signal.

Motorola's RF Management Software shows visual representations of key performance indicators. These visual representations give administrators an intuitive view of the network health at a glance, and permit an administrator to "drill down" on anything that looks amiss. This can all be done from a central location or from an administrator's mobile device. As with Wireless IPS, locationing capabilities give RF Management Software an extra edge, showing administrators not only that there is an issue, but where that issue is.

Managing devices in a WLAN

The ability to remotely manage and keep track of individual elements or groups of devices in an enterprise wireless network is important for many reasons. If a network device is non-compliant or acting strangely, it can be shut down or updated remotely. New patches and policies can quickly and easily be applied to select or all devices, and by using configuration back-ups and compliance monitoring, the system can alert the administrator of any compliance issues as they occur. Through Motorola's use of locationing, if a high-value or sensitive mobile client device moves beyond a certain point, it can be automatically disabled.

These tasks, and others, can be managed through Motorola's MSP RF Management Edition.

Putting it all together: Motorola's RF management suite

Clearly, network planning, network security, network monitoring and analysis, and network device management are all critical pieces of network management. However, until recently, network administrators had only two choices in managing wireless networks: use different stand-alone tools for each function, even though they may not share data or a common interface; or use a "one-size-fits-all" network management system.

Recognizing this, Motorola now offers administrators more flexible solutions. Available individually, or as part of Motorola's RF Management Suite, Motorola offers four management tools that can share data, and can all be accessed through a single console.

- MSP RF Mangament Edition is at the heart of the Network Management Suite, providing the interface to all the tools, as well as day-to-day management of all network devices from the NOC level down to the client level.

Factors to consider when evaluating a wireless network management system

- What do you need – performance management, fault management, configuration management or all-in-one?
- Where will the administrator be? Local? Remote? Both?
- Do you need reporting? Do you need a to access a wealth of network information?
- Describe the environment:
  - Distributed?
  - Lots of interference?
  - How many MUs will be supported?
  - What applications will be supported?
- How mobile is your enterprise? Mobility beyond the building has additional security implications not handled by most "vanilla" network management systems.
- Is the ability to provide proof of compliance to industry regulation important?

- LANPlanner is the RF-expert-in-a-box that helps administrators plan a network perfectly suited to an enterprise's technology needs, physical environment and potential growth.
- RF Management Software is an intuitive, graphical representation of the implemented network at every location. Used in conjunction with data imported from LAN Planner, it allows users to see if the network has been implemented as planned. It provides a holistic view of network health, and is an invaluable troubleshooting tool, as it tracks key performance indicators and allows administrators to follow the path of anything that looks suspicious.
- Wireless IPS, uses locationing to provide additional protection from rogue devices

This solution offers the flexibility of choosing only the tools one needs, while providing the continuity of shared data and common interface previously only available through "complete" solutions. The inclusion of location-based features makes the Motorola Network Management Suite particularly robust.

Choosing the right Motorola network management tools for an enterprise

So, how does an administrator determine which Motorola tools he/she needs for a given enterprise network?

The data presented thus far should give network administrators something to think about when considering whether their own network's needs are currently being met in terms of planning, security, monitoring and analysis, and device management. The corresponding Motorola products have also been briefly described.

While this document should be a good starting point for anyone interested in network management, each network is different, so it is important to work with a Motorola partner or representative to determine the best solution for a given wireless network implementation.

Motorola solutions: Services and support for Wi-Fi infrastructure management

Motorola's Enterprise Mobility Services provide comprehensive support and technical expertise for designing, deploying and maintaining successful mobility solutions. With a full suite of products — from wireless switches, access points and wireless handheld devices to the management software suite— Motorola's diverse service offerings enhance enterprise business operations, providing you with value and uptime throughout the entire lifecycle of your end-to-end mobility solution.

Motorola Enterprise Mobility Services also provide access to the richest technical expertise for mobility solutions. Motorola is equipped to deliver the level of repair service that is required for your mission-critical solutions.

Summary

Managing a wireless enterprise network can be complicated – unless you have the right tools. Motorola's network management tools provide robust network planning, security, monitoring and analysis, and device management. By itself, each tool – MSP RF Management Edition, LANPlanner, RF Management Software and Wireless IPS – will aid in achieving and maintaining an enterprise-class wireless network. However, these components are greater than the sum of their parts when used together in Motorola's RF Management Suite to seamlessly provide complete wireless network management.

For more information, contact Motorola at +1.800.722.6234 or +1.631.738.2400, or visit us on the web at: www.motorola.com/enterpriseWLAN or contact your local Motorola sales representative.

MOTOROLA

motorola.com