

NETGEAR®

The Benefits of Wireless LAN Controller in Small and Mid-sized Business Networks

4500 Great America Parkway
Santa Clara, CA 95054 USA
1-888-NETGEAR (638-4327)
E-mail: info@NETGEAR.com
www.NETGEAR.com

The Evolving SMB

To understand the function of a wireless LAN (WLAN) controller in an SMB network, it helps to understand the history of evolution of wireless LANs in the SMB.

Small and mid-sized businesses since the early 90's have wholly embraced wireless access for their networks for a number of reasons. Initially offered as a convenience to provide access to the network, the wireless LAN today has become an integral part of the business not only boosting employee productivity but also becoming a viable alternative to wired (Ethernet-based) access to the network. As the number of clients using the wireless infrastructure continues to increase, including devices such as Skype/Wi-Fi phones and PDA's, so do the requirements for continuous wireless coverage, wireless network uptime, centralized management and monitoring. Wireless networks today have transitioned from being offered as a convenience in the early 90's to becoming a necessity for any SMB today.

Traditional WLAN deployments in a large part today, consist of access points operating as separate and independent nodes that are autonomously configured. Also called "fat" access points these access points on the network are managed, operated and configured independently. Over a period of time as organizations grow, hire new employees, or move to different buildings or floors, the ability to manage the overall wireless infrastructure presents new requirements and challenges. Some of the challenges and how they are handled today in autonomous (fat) access points are highlighted in the table below:

Requirement	Description	Traditional Autonomous (Fat Access Point Solution)
Management and Monitoring	Cost-effectively manage, monitor and deploy the wireless network	Implement scripts or SNMP solution to configure WLAN management and individually configure each access point and monitor through the centralized management station
Upgrade Costs	Time to deploy additional access points and push new images to existing access points	Deploy a centralized network management station or use scripts. The cost is extra as it requires third party software.
Guest Access	Ability to provide customers, vendors and partners with controlled access to the network while keeping the network secure	Implement special VLAN (Guest) across each access point and trunk them across the network. Not user friendly and cumbersome to manage
RF Planning	Understand how to deploy a wireless network and include tools that advise you on how to deploy a wireless network based upon the structure of the floor or building	Use a third party planning tool that costs extra.
Voice over WLAN	Cost-effective, real-time voice services using the existing wireless infrastructure	Partial implementation is available today with limited support for fast-roaming and voice-protocol support
Load Balancing	Auto balance clients load between access points	Individual access points advertise load, but load is not automatically spread across access points.
Fast, Secure Roaming	Seamless client roaming within networks and VLANs	Add an access point that supports bridging and repeating to facilitate roaming
Continuous Wireless Coverage	Immediate dynamic adaptation of the wireless environment	Traditionally not available in fat access points.
Rogue AP Detection	Ability to detect rogue access points and unauthorized access	You can use rogue access point detection on the access point however that affects overall performance of the access point itself.

As SMBs grow in size three critical issues need to be addressed:

1. Lower the cost of deployment
2. Ease of management
3. Security

Enter Wireless LAN Switching

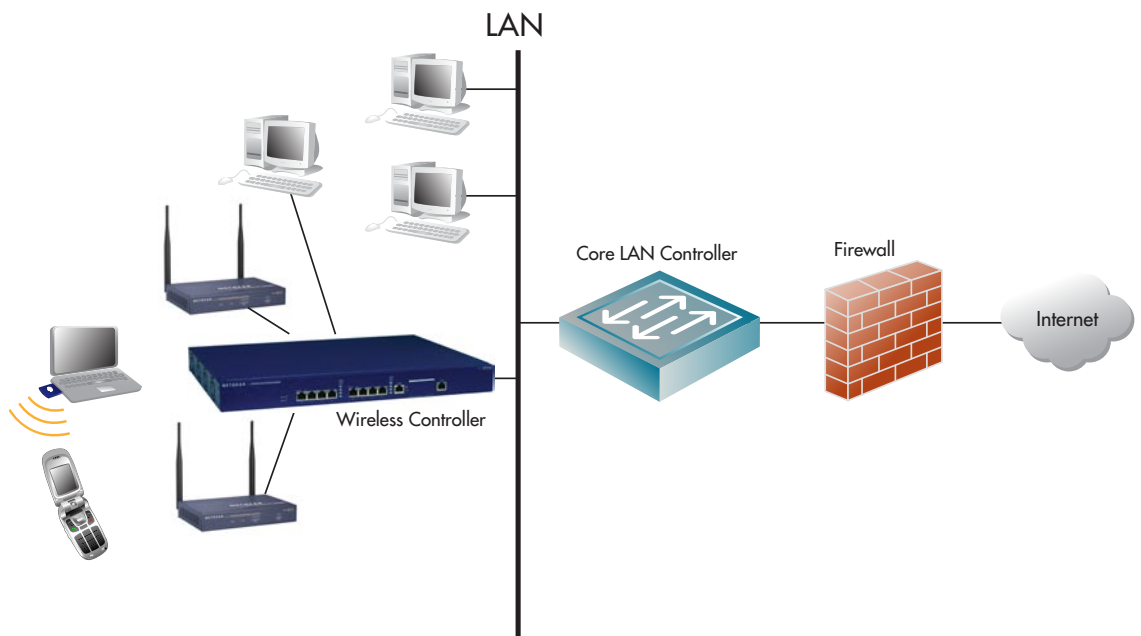
A WLAN controller is a centralized device in the network, usually located at the data center, to which all the wireless APs on the network are directly or indirectly connected. By virtue of its centralized location and intelligence, the WLAN controller is completely aware of the WLAN environment. It provides all essential services to lower the cost of deployment, simplify management, and provide multiple layers of security.

Lowering the cost of deployment

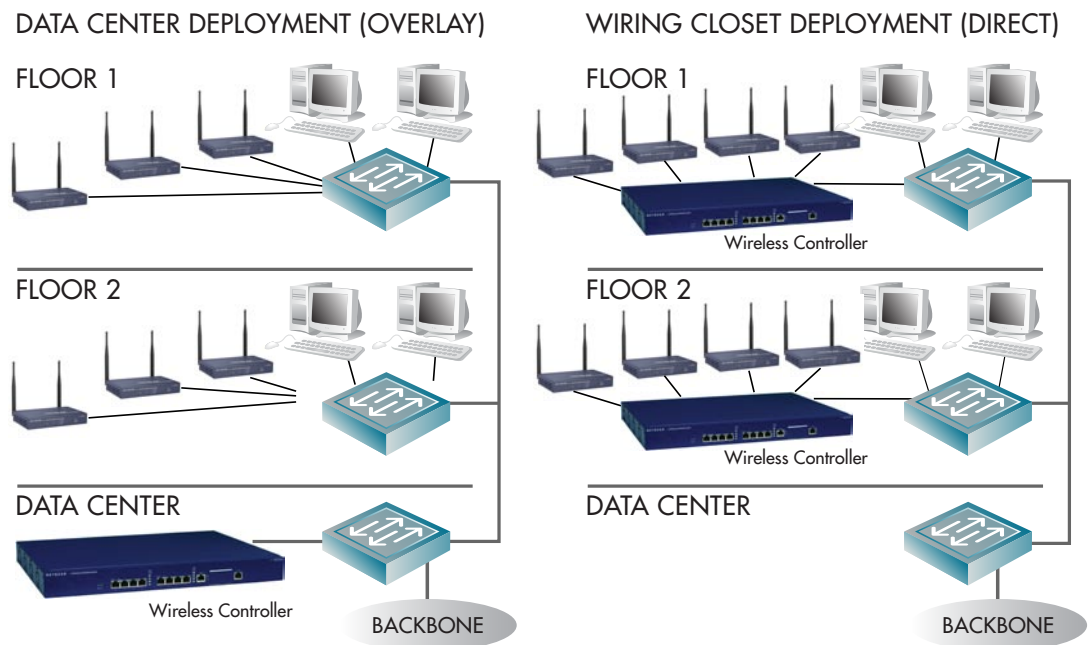
The factors that contribute significantly to high costs of deployment are pre-installation site-surveys (where to place the access point), pulling new cable and power to APs and re-configuring the existing network infrastructure including configuring the individual access points.

Wireless LAN controllers eliminate site-surveys by including intelligent RF planning software. It also provides standards-based Power over Ethernet (IEEE 802.3af), eliminating the need to draw power to each access point. It is not required for the access points to be directly connected to the wireless controller. Access points can be deployed anywhere in the network and they will be discovered and configured by the wireless controller which will set the power level, security and channel settings to optimize performance and coverage on a system-wide basis. Some typical deployment scenarios are described below:

Scenario 1: Typical Setup in a 50-person Company



Scenario 2: Multi-floor Deployment Scenarios



Simplifying Wireless Management

Ease of management and troubleshooting comes from self-configuring and self-healing wireless networks. Accurately locating each user and knowing all the characteristics of the user and AP such as location, MAC address (BSSID), channel, radio type, manufacturer, status on the network and network name eases management as well.

Since the WLAN controller is aware of the RF characteristics within the network infrastructure as a whole, it can easily detect interference between nearby APs and re-configure their power and channel settings automatically. Through the same principle, when the controller detects a coverage gap due to an AP going down, it can instruct nearby APs to increase their power levels to fill the gap.

Unifying Wired and Wireless Security

Let us focus on key features that enable rapid adoption in small and mid-sized businesses. These include:

- a. Authentication
- b. Authorization
- c. Encryption
- d. RF security

WLANs must simultaneously authenticate employees, guests and contractors using a variety of authentication methods such as 802.1x and captive portal. Wireless users cannot be treated the same as wired users. Controlling wireless users' access privileges using a variety of deterministic criteria such as authentication method, device type, and application requested is key to providing differentiated access to maintain security.

WLANs must provide state-of-the-art encryption techniques to maintain security but must also extend it over the wire until all the security policies are applied. This means not stopping the encryption at the AP but keeping WLAN traffic fully isolated until it has passed through a firewall at the WLAN controller.

Finally, being able to detect and stop unauthorized (rogue) APs and stop all unauthorized wireless connectivity in the network is a key component of WLAN security. Accurately identifying an AP as a rogue or simply as an interfering AP (i.e., “neighboring AP”) along with precisely pinpointing its location is an essential part of providing complete RF security. In turn, WLAN controllers now let small and mid-sized businesses literally “lock the air.”

Summary

As businesses continue to expand and grow, so do the needs of their wireless infrastructure. Centralized wireless controller solutions provide flexibility of deployment, thereby reducing costs, planning tools and time spent deploying a wireless network in the business. They also enable centralized monitoring of the entire wireless infrastructure, thereby reducing the total cost of ownership, and unification of wired and wireless access which future proofs the investment.

Other reasons to deploy wireless controllers include eliminating network security risk by stopping all unauthorized wireless connections. Wireless controllers also enable the deployment of voice over Wi-Fi in SMBs which provides better coverage and security at a lower cost than cellular mobile voice.

Though WLAN controllers have gained widespread acceptance, not all WLAN controllers are created equal. WLAN controllers that provide complete centralized control, comprehensive security capabilities and a full-feature set now allow for the pervasive deployment and widespread adoption of wireless within in the enterprise—leaving users unplugged but well connected.

About NETGEAR® Inc.

NETGEAR® (Nasdaq: NTGR) designs technologically advanced, branded networking products that address the specific needs of small and medium business and home users. The Company’s product offerings enable users to share Internet access, peripherals, files, digital multimedia content and applications among multiple personal computers and other Internet-enabled devices. NETGEAR offers a lifetime warranty on all its ProSafe business line products including the Wireless Controller products. NETGEAR is headquartered in Santa Clara, Calif. For more information, visit the company’s Web site at www.netgear.com or call (408) 907-8000.



NETGEAR®

©2007 NETGEAR, Inc., the NETGEAR logo, Connect with Innovation, Everybody’s connecting, FrontView, the Gear Guy logo, IntelliFi, ProSafe, RangeMax, ReadyNAS, RAIDar, RAIDiator, X-RAID, and Smart Wizard are trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Microsoft and Windows are trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved. W/P11September07-02