Scaling wireless to the next level

August 28, 2006 - TechRepublic

Takeaway:
At the enterprise level, wireless scalability takes on a whole new meaning. Centralized management for multiple access points and new topologies allow you to extend the WLAN across even the largest organization.

About a year ago, this column took a look at popular wireless technologies--802.11a, b and g--from the standpoint of scalability. We examined how such factors as bandwidth/speed, distance ranges and reliability impact scalability. But we were still looking at wireless on a relatively small scale, from the perspective of deploying a single or a few WAPs in the organization.

This time, we're interested in how wireless can scale up to the enterprise level, to serve hundreds or even thousands of users and to accommodate high bandwidth applications such as VoIP and video communications. Toward that end, we'll discuss deployment strategies that can be used to make wireless computing available throughout a large network.

What enterprises need

You've heard the old F. Scott Fitzgerald pronouncement that "the rich are different from you and me." Well, enterprises likewise are different from small and medium businesses in more ways than having more users (and more money). Their networking needs--and solutions--are different, as well.

Along with the obvious need to support a larger number of users, enterprises often need support for a larger variety of applications. For example, VoWLAN (Voice over Wireless LAN) is gaining popularity in the enterprise space. Wi-Max long range wireless may be needed for large company campus type environments.

According to the recent 2006 Webtorials "WLAN State of the Market" report by Joanie Wexler of Network World, wireless technology tied with VPN at the top of the list of most important technologies to the enterprises surveyed. One of the most interesting points in the report is that wireless networking is no longer being used only as a "hot spot" solution for lobbies, conference rooms and other common areas, but is now being deployed more widely across the organization. You can read the full report at http://www.webtorials.com/abstracts/WLAN2006.htm (registration required).

One of the most important needs for WLAN administrators in the enterprise environment is the ability to centrally manage multiple access points.

Centralized WLAN management and security

There are a plethora of products available for providing centralized management of enterprise-class WLANs. The move toward centralization has resulted in a corresponding move away from more "intelligent" WAPs and toward so-called "light" access points (also called Wireless Termination Points or WTPs) that are controlled by a centralized controller in a switch.

There are a couple of ways to implement this model. According to the Internet Engineering Task Force's Control and Provisioning of Wireless Access Points (CAPWAP) working group, the two categories for centralized wireless architecture are:

- Split MAC: all security functions are handled by the centralized switch/controller
- Split Access Point (local MAC): the centralized controller handles 802.1x authentication and the AP handles cryptography
- You can find out more about CAPWAP at http://www.ietf.org/html.charters/capwap-charter.html.

Many of the centralized WLAN products, such as ManageEngineWiFi Manager (http://manageengine.adventnet.com/products/wifi-manager/index.html), not only allow you to configure multiple APs, but also include security mechanisms to detect and block rogue access points and protect against WLAN intrusions and attacks.

Migrating to centralized management

Several companies are offering solutions to help companies with traditional wireless LANs migrate to a centralized management architecture more easily. In July 2006, Aruba Networks and AirWave Wireless announced they were teaming up to provide support by AirWave's Wireless Management Suite to Aruba's APs, making it possible to centrally manage both legacy standalone APs and modern "light" APs from the same console. You can read more about it here:

http://www.networkcomputing.com/channels/wireless/showArticle.jhtml?articleID=190700110

Voice over WLAN

Certainly one of the most demanding applications faced by wireless networks is VoWLAN. Voice communications are mission-critical applications for most organizations, so the ability to make telephone calls over wireless LANs requires high levels of availability and bandwidth capacity.

One of the biggest obstacles to implementing VoWLAN is bandwidth. An 11 Mbps 802.11b WLAN doesn't have much bandwidth to spare. But as wireless technologies increase in speed (54 Mbps for standard 802.11a and g, and with the 802.11n standards, expected to be completed in 2007, providing theoretical transfer speeds over 500 Mbps and estimated actual throughput of 100 -- 180 Mbps), VoWLAN becomes a much more attractive proposition. You can read about 802.11n here:

http://www.wired.com/news/technology/wireless/0,70806-0.html

One implementation of VoWLAN that may be coming into its own soon is UMA (Unlicensed Mobile Access). Mobile phones are being tested by some cellular companies that allow GSM and GPRS cell phones to operate over 802.11 wi-fi networks. With dual-mode telephone handsets, users can roam between the cellular network and unlicensed wi-fi networks -- both public hotspots and private WLANs. You can read more about UMA here:

http://www.umatechnology.org/overview/

WLAN topology in the enterprise

It's important to remember that wireless networking components are actually radio transmitters and receivers that use specific frequencies and channels within those frequencies. For example, the standard for 802.11b defines 14 channels. 802.11b is said to operate at the 2.4GHz frequency, but within that frequency range you could have different WAPs with one operating on channel 1, at 2.412 GHz, and another on channel 2 at 2.417 GHz and so forth.

The FCC allows the use of channels 1 through 11 in the U.S., whereas in Europe you can use channels 1 through 13. The problem is that there's overlap of signal so that you can't actually use channels 1 and 2 within the distance range of 802.11b because they would interfere with each other. Due to the overlap, only three of the 11 channels can be used at the same location (channels 1, 6 and 11). This means you have to plan carefully if you need more than three access points. Channels need to be assigned so that there's little or (ideally) no overlap of signal.

Thus large multiple AP WLANs are usually designed in a "cellular" topology, where the APs are located to create coverage in much the same way cell phone towers are distributed. The APs that use the same channel have to be far enough away from one another to avoid interference.

There are a number of disadvantages to this type of architecture, including latency when communications are "handed off" from one AP to another on a different channel when users are mobile, and collisions when there are large numbers of users on the WLAN who transmit at the same time.

There are alternatives to the cell-based topology, such as the "channel blanket" topology offered by Extricom, which uses UltraThin access points controlled by a central switch that directs all of the wireless traffic. You can find out more about their solution at http://www.extricom.com/.

Summary

Wireless networking at the enterprise level is different -- but there are many products and services out there that make it easier to implement one or more WLANs in a large organization, that can support high bandwidth applications such as VoWLAN.