



WHITE PAPER

WIRELESS LANs—TOTAL COST OF OWNERSHIP

EXECUTIVE SUMMARY

After being proven in vertical market segments such as healthcare, education, and retail, wireless LANs are being increasingly deployed in traditional office settings. Wireless LAN deployments often start small and then grow. A wireless LAN solution that appears to be appropriate and cost-effective for a workgroup or department may be inappropriate and costly for a companywide deployment—many wireless LAN offerings lack an architecture that scales well, or fail to take advantage of the proven network infrastructure already in place.

To avoid heading down a costly and difficult path, an organization needs to plan for the future—a companywide wireless LAN supporting many applications for nearly every user—before embarking on its initial wireless LAN deployment. Parallel or overlay networks are inefficient and complex to manage, resulting in a high total cost of ownership (TCO). The best way to control costs and manage bandwidth is to take advantage of the existing wired infrastructure not only as the backbone for wireless LANs, but also as the provider of critical services for wireless LAN security, quality of service (QoS), and management.

When estimating TCO, an organization should keep in mind that equipment purchase price is a small percentage of total cost. Other costs include:

- Radio frequency (RF) planning to determine how many access points are needed, and where they should be placed
- Installation, including mounting access points (often above ceiling panels), running Ethernet cables to access points, and mounting antennas
- Ongoing support and maintenance, such as reconfiguring and upgrading access points

A solution that integrates wired and wireless delivers the lowest TCO.

WIRELESS LANs: FROM VERTICAL MARKETS TO OFFICES

Wireless LANs have become a business imperative in vertical market segments such as healthcare, education, and retail. These segments were early adopters of wireless LAN technology, and organizations within these segments have broad wireless LAN deployments for business-critical applications that include bedside nursing and point-of-care physician applications, classroom and campus access, and point-of-sale retailing. Thanks in part to widespread production deployments in these segments, wireless LAN technology has become technically secure, cost-effective, and robust across many broad mobile computing environments.

Many analysts (and Cisco Systems®) believe that the next major market for wireless adoption is within the “carpeted office”, where most office workers now carry laptops, PDAs, and mobile phones everywhere they go, and have a need to be constantly in touch. An increasing number of the devices used by office workers have embedded wireless LAN adapters—they are “wireless-ready” for their existing applications that use IP.

Given this broad proliferation of wireless-ready devices, the growing mobility needs of the office worker, and the maturity of wireless LANs, Fortune 1000 firms are beginning to take wireless LAN technology seriously. Recognizing that wireless LANs increase employee productivity, firms are starting pilot deployments within highly mobile workgroups. Sales, event marketing, information technology, manufacturing, and even engineering departments are becoming mobile. These workgroups quickly see the benefits of wireless when there is a need for real-time communications and/or collaboration.

In addition to improving productivity, wireless LANs support flexible networking topologies, especially in environments that lack sufficient Ethernet ports in important areas such as conference rooms and common areas. Overloaded work sites can be more easily expanded with wireless connection

points and ad-hoc seating designs. Wireless LANs also provide a proven means of guest access, enabling contractors, customers, and other guests to have Internet access without intruding on the established corporate network.

DEPLOYMENTS—START SMALL, THINK LARGE

Wireless LAN deployments often start small and then grow rapidly. Typically, one workgroup identifies the need for the increased productivity that wireless offers and, based upon a business justification, receives a budget large enough to support the addition of wireless for the employees within that workgroup. Once wireless is deployed within one workgroup, it quickly becomes desired across multiple departments, floors, and buildings. It is short-sighted to consider wireless as a small pilot trial without considering the scalability and the TCO benefits across multiple organizations and buildings.

Often, the initial workgroup piloting wireless does not understand broader infrastructure requirements, including scalability, security, operations management, and recurring support costs; as a result, these requirements are not considered when choosing a wireless LAN solution. While it is easy to make a workgroup-level decision on a wireless LAN deployment, the chosen solution often lacks the feature scope and the cost/scalability analysis to be deployed across the entire company. A workgroup decision can become an infrastructure integration challenge, as demand for wireless causes the addition of many wireless devices to the network, and the initial small pilots are often unable to scale across the enterprise.

THE VALUE OF WIRED/WIRELESS INTEGRATION

As a wireless LAN deployment grows from a workgroup or department to the entire organization, it begins to have an impact on the existing network infrastructure, touching wiring closets, firewalls, authentication, authorization, and accounting (AAA) servers and user directories, and other networking components. Every element—and combination of elements—must be secure, scalable, and manageable. While it may seem simple to get a wireless LAN project going as an overlay to the wired network, separate wireless buildouts are more costly than integrating wireless LANs into the existing IP communications infrastructure.

In all cases, wireless LANs deployed independently of the wired infrastructure represent a poor use of capital assets, because of the inefficiency of parallel networks. The best way to control costs and manage bandwidth is to use the existing wired infrastructure as the “backbone” for wireless LANs. The wired backbone can handle the interconnection of wireless LAN access points. When additional services are needed for wireless LANs, upgrading the wired infrastructure is less expensive and yields more feature-richness than adding “wireless switches”—essentially, specialized gateways.

In addition to considering the total cost to deploy a wireless LAN infrastructure, an IT organization must also consider the following before beginning a wireless LAN pilot:

- How well the wireless solution can integrate into the existing infrastructure
- What features of the existing infrastructure can be used to help absorb the overall cost of the wireless deployment
- What best practices from the wired infrastructure can be applied to the wireless buildout in the areas of management, authentication, and intrusion detection

If the access points and other products installed for a pilot or workgroup-level deployment are not the right products for the companywide deployment, IT must choose between removing and replacing the products or leaving them in place to run alongside another wireless LAN solution. The former solution results in high costs for repetitive labor, as well as the inability to realize sufficient benefit from the products used for the initial deployment. The latter results in high operational costs associated with managing disparate solutions. Given the likelihood of a wider deployment, any workgroup or pilot wireless deployment should be evaluated based on its overall scalability and on the future need to integrate this into the wired infrastructure, rather than having to tear out the pilot deployment and replace it when a more universal decision is made.

The view that a new type of network should be an overlay is nothing new. When workgroups began adopting PCs in the late 1980s, people created small LANs to share access at the workgroup level. As these shared LANs became mainstream, the responsibility for an integrated, scalable network became a centralized IT responsibility. In almost all cases, the central IT department was forced to re-engineer the network and replace workgroup deployments with a corporate switched infrastructure. Similarly, workgroup-level wireless LANs that are network overlays are likely to be ripped out and replaced by integrated solutions that achieve economies of scale and can be centrally managed using familiar tools and procedures. Why implement a throwaway architecture for wireless LANs?

TCO VARIABLES

When considering a wireless LAN deployment, you should determine your needs over a three-to-five-year period, based on both today's workgroup needs and the increase in wireless as it grows throughout the enterprise. The most important cost elements of wireless networks are:

- 1. Costs of the access points**—Access points are the mounted devices that provide connectivity between wireless clients and the wired infrastructure. Deployed appropriately, access points provide wireless coverage everywhere that it is needed. Important TCO questions are:
 - Should access points support 802.11b/g, 802.11a, or both?
 - What areas need to be covered?
 - How many users will be in each area?
 - What applications will they use?
 - How many access points are sufficient to provide the needed coverage, bandwidth, and application support?
 - What will it cost to install the access points?
 - What will be the ongoing maintenance costs to reconfigure access points and upgrade them to support new features?
- 2. Access point planning and deployment costs**—Designing a wireless network is significantly different than designing a wired network. As cited above, determining what areas need to be covered and the expected usage patterns in those areas results in an estimate of the number of access points required. RF coverage is affected by building construction materials, metal shelves, RF interference sources, and other factors, so a site survey is required in nearly every facility. Because access points often are mounted above ceiling tiles for theft protection, a good understanding of the ceiling cable plants, mounting points, and labor to install these is required. If careful planning does not precede deployment, the result is an inefficient patchwork of access points deployed randomly. Done correctly, planning should be a one-time, upfront effort for each building. However, if the initially deployed solution does not offer scalability benefits as wireless expands, much of the plan and physical deployment will need to be reworked, and access points and switches may need to be upgraded or replaced.
- 3. Costs of the infrastructure switch (or switches) for connecting access points together and into the wired infrastructure**—In addition to serving as the backbone for all traffic that travels to and from wireless clients, switches can be the intelligent point for wireless roaming, client authentication, and centralized security features. As more client devices support 802.11g and 802.11a, every access point will be expected to deliver throughput of 30 Mbps or more. For a small deployment of 100 access points connected together into the centralized switch, this can mean 3 Gbps or more of switching throughput. When switches support features such as caching of authentication credentials, access control lists (ACLs), multicast, desktop remediation, QoS, and guest access, more processing load is placed on these switches. It is critical that the wireless backbone be engineered with sufficient processing performance to handle these features. A distributed switch architecture in which the processing is shared between switches, roaming, high availability, and configuration consistency can compromise a system, and its management complexity drives TCO higher.
- 4. Network management costs**—Managing a wireless network has several added areas of complexity when compared to the management of wired client access ports (Ethernet jacks). Managing access points involves more than managing physical devices. It is important to:
 - **Manage coverage**—Access points provide wireless coverage. Because coverage patterns can change due to environmental factors and sources of RF interference, customers want real-time maps showing access point layout and coverage. Customers also want the ability to alter coverage patterns by changing access point settings.

- Report on client activities—Access points serve clients, and customers want up-to-date and trend information on legitimate client access (including authentication), as well as potential intrusion. Location tracking for clients and for assets with 802.11 tags is increasingly vital.
- Deploy and upgrade access points—Customer want centralized tools for quick deployment of new access points, upgrading of access point firmware, and reconfiguring of access points and other networking gear.

There are numerous costs associated with wireless implementation, including configuration, monitoring, graphical layout, logging and reporting, and revision management. As the number of access points increases, consolidated management reduces daily operational costs. Reducing the number of management appliances and interconnected wireless switches reduces the complexity and TCO of the wireless system.

5. **Costs of connecting access points into the wiring closet**—As stated above, access points need to be interconnected through a wired switching infrastructure. The most common architecture for accomplishing this includes a centralized intelligent switch implementation for roaming, security, management, and authentication, and feeder switches from the access connection points, better known as wiring closet switches. Given the broad adoption of wired Ethernet in a majority of enterprises today, existing wiring closet infrastructures can be used to aggregate the access points into a centralized switch, and to perform the functions mentioned above. From a TCO perspective, the more these existing wiring closet infrastructures can be used, the better—these existing wiring closet switches typically have available slots for adding more ports, and/or can be upgraded with higher-density modules when needing additional ports for connecting into the access ports. Further, these switches already have well-defined operating procedures, with operational tools for managing them. Adding new wireless switches within the wiring closet, with different management tools, operational procedures, configurations, and support contracts, can increase the cost of wireless deployment, especially as wireless grows throughout the enterprise.

DETERMINING TCO

When making a wireless decision, it is important to consider all of the above component costs over a three-to-five-year period, and to recognize that wireless becomes part of the core infrastructure once users begin realizing the benefits. As the wireless network grows and evolves, bandwidth, complexity, and management efforts will increase over time. These increases in scale, bandwidth, and complexity should be factored into the TCO equation.

Cisco has developed a TCO calculator, which models the following:

- Initial investment in access points, the switches required to interconnect the access points, and the management tools for deployment and day-to-day operations
- Growth in the size of the wireless network with the addition of access points for greater bandwidth to support an increasing amount of users and devices, which drives higher capacity and throughput with the switch interconnects
- Support costs across a five-year period
- Software costs such as software upgrades, added security capabilities, and added management features such as location services
- Comparison of Cisco's TCO to competitive offerings, with customer input on the capital equipment costs of this competitive equipment, as well as access-point-to-switch ratios and the additional cost of security and management software

Cisco has services available for the planning, analysis, and deployment of wireless networks. Cisco also has wireless-specialized, trained channel partners that can offer the same services. Please contact your Cisco Account Manager for more information.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)

204113_ETMG_SD_11.04

Printed in the USA

