

## True-Sizing the Network

### Finding the Golden Mean in Wire Line and Wireless Networks

**Stan Schatt**

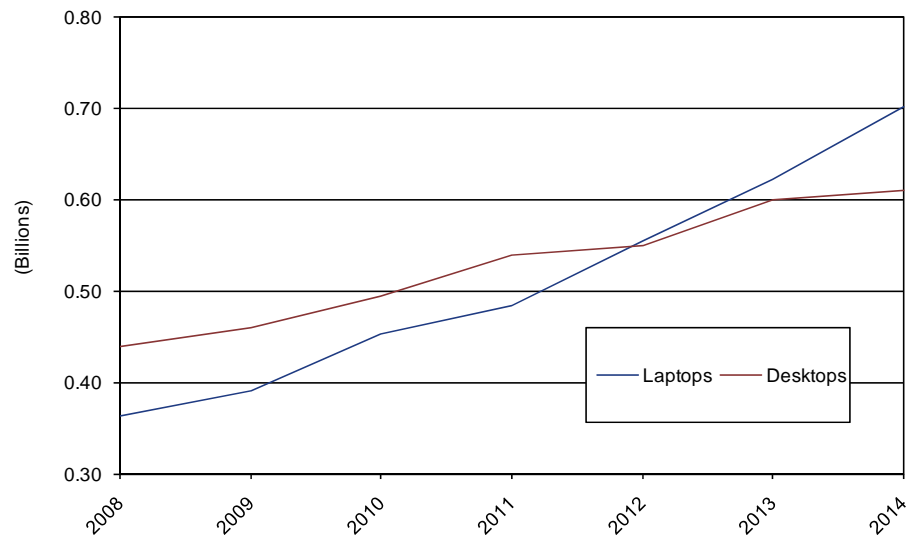
Vice President and Practice Director, Wireless Connectivity

#### Executive Summary

As sales of IEEE 802.11n wireless LAN equipment have increased over the past year, there has been a general outcry from some vendors who sell WLAN products exclusively for IT managers; they want to move to all wireless networks. Some skeptical IT managers have questioned the objectivity of such vendors and pointed to famed psychologist Abraham Maslow's observation that "if you only have a hammer, then you tend to see every problem as a nail." There are legitimate reasons to consider wireless LAN deployments just as there are good reasons to deploy wire line solutions. The purpose of this research brief is to look at the current network infrastructure landscape, consider the advantages and disadvantages of both types of solutions, and determine a common sense strategy for IT managers and CIOs, who are in the process of trying to determine the best course of action for their own particular network environments. Determining their own network technology roadmap requires honest answers to a number of questions rather than succumbing to vendor hype and hyperbole.

- The evolution of wireless LAN technology over the past few years has been very dramatic. IEEE 802.11n products address many of the limitations of earlier generations of WLAN equipment including far greater bandwidth and improved coverage while the IEEE 802.11i standard has strengthened WLAN security. The latest generation of wireless LAN equipment satisfies a serious need enterprise IT managers have for employee mobility, guest access, and network access for road warriors. While security has improved dramatically, there are still issues with a few devices that do not support AES encryption or anything above MAC authentication. Similarly, while reliability and fault tolerance has vastly improved, wireless LANs still lack the five 9's reliability found in wire line networks. Finally, the next two years will see very significant improvements in wireless LAN management tools and general management functionality in key areas including voice over Wi-Fi applications and video over Wi-Fi applications.
- Wire line networking technology has also evolved steadily over the past several years. Fast Ethernet backbones have given way to Gigabit and 10 Gigabit backbones, while desktop connectivity has moved from a shared 10 Mbps connection to a dedicated, switched Fast Ethernet or Gigabit Ethernet connection. Ethernet vendors have been able to leverage the vast installed base of CAT 5 and 6 cabling by ensuring that there is a clear roadmap for faster versions that will continue to support this cabling.
- Rather than an either-or proposition, many IT managers are finding, after careful consideration of their current network infrastructure as well as their roadmap for future applications, that the best solution is an Aristotelian "Golden Mean" solution that includes using both wire line technology and wireless technology wherever each is most effective. In other words, they are letting their own particular needs dictate the most appropriate solution.

**Chart 1.1 Installed Base of Commercial PCs by Type, Market Forecast: 2008 to 2014**



(Source: ABI Research)

## Section 1. THE CURRENT STATE OF THE ENTERPRISE NETWORK

CIOs and network managers have always faced tough decisions when it comes to designing the most efficient network. A little more than a decade ago much of the decision making involved calculating the expense involved in migrating from Token Ring to Ethernet. In fact, Ethernet was still transitioning from a hub-based shared medium product to a switch-based product. In the euphoric days of the dot-com bubble it was easy to overlook the fact that an upstart IEEE 802.11 standard for wireless LANs had recently been approved and the Wi-Fi Alliance was in the process of being formed.

Today the dot-com days are just a distant memory. Meanwhile, the enterprise networks designed a decade ago have undergone many upgrades. A 10 Mbps shared Ethernet connection has evolved to a dedicated 1Gbps switched connection to the desktop. While 10Gbps backbones are common on many of today's enterprise networks, next year should see approval of standards for 40Gbps and 100Gbps Ethernet designed to run on existing cabling infrastructures. At the same time the price per user of a 1Gbps switched Ethernet connection at the desktop continues to drop to well below \$50 per user.

For the past decade, wireless LAN vendors have urged IT managers to add an overlay of wireless LAN technology to their wire line network. Today, these same vendors are now urging anyone who will listen to move quickly to an all-wireless network. Certainly despite the fact some banks and insurance companies have banned all wireless LAN technology, there are ample reasons to add wireless LAN technology to almost every enterprise network design in order to enhance mobility where required, but that does not mean wire line networks are suddenly antiquated or of limited value.

This research brief examines the current state of the enterprise network and provides recommendations that follow a path that is both eminently sensible and affordable. It is based in part on interviews with network managers who are accountable for the direction their networks will take.

## 1.1 The Steady Growth of Wi-Fi in the Enterprise

The first generation of 802.11b wireless LANs provided desperately needed mobility but suffered from limited bandwidth (around 5 Mbps throughput under the best of circumstances) and limited scalability. These “fat” access points were expensive and difficult to manage. These early deployments often consisted of hotspots designed to support road warriors when they returned to corporate offices. They also provided Internet service for corporate guests and contractors. Conference rooms were another early location for 802.11b access points.

The development of WLAN equipment built around a centralized architecture with less expensive “thin” access points along with the release of 802.11g spurred the growth of Wi-Fi in enterprises because 802.11g provided greater bandwidth (around 20 Mbps throughput) and the new architecture provided better scalability and manageability. As corporations began to refresh their laptops, a growing installed base of models with embedded Wi-Fi encouraged network managers to broaden wireless coverage. Enterprise wireless LANs proliferated as security improved from very weak WEP to robust WPA2 encryption.

Today enterprises are enthusiastically adding 802.11n wireless LAN technology. There are many reasons for this trend. These products offer a quantum increase in bandwidth (as much as 195 Mbps in throughput) as well as far better coverage and the promise of less interference at least in the 5 GHz range.

## 1.2 Drivers

There are a number of drivers for the proliferation of enterprise wireless LANs including the following:

**Mobility required or expected:** IT managers are finding that their mobile work force absolutely requires network access. That group includes salespeople, specialized professionals such as physicians, nurses, college professors and students, warehouse workers, manufacturing plant supervisors, etc. Also, corporate guests and contractors expect to be able to have Internet access available. Hospitals are finding that patients and their visitors expect Wi-Fi hotspot availability.

**The availability of Wi-Fi-ready PCs:** Since 2005, laptops, generally sold with embedded Wi-Fi radios, have outsold desktop PCs. As companies refresh their PCs, a higher percentage of computing equipment becomes Wi-Fi ready without the need to buy Wi-Fi cards. Historically IT managers have disliked add-on cards because of their tendency to break as well as the difficulty of keeping track of them.

- **Higher bandwidth:** It is true that early Wi-Fi equipment was very limited as far as throughput; the small size of early deployments kept performance from deteriorating. Today’s larger Wi-Fi deployments are based in part on the availability of higher speed 802.11a/g and 802.11n radios.

- **Less security concern:** While IT managers often still list security as a major concern when it comes to purchasing Wi-Fi equipment, the 802.11i standard has greatly enhanced security because of AES encryption.
- **Pricing:** While the cost per user of wireless LAN equipment still exceeds the cost per user of wired connections in environments where cabling already is installed, there is no question but that the cost of access points is decreasing each year.
- **Software improvement:** While network management for wired networks is still more mature and provides more functionality than wireless network management platforms, the gap is closing. In fact, vendors who sell both wired and wireless network equipment are beginning to move towards integrated network management platforms to provide a single, uniform view of both networks.

### 1.3 Challenges

There are still significant challenges to an all-wireless Enterprise network including the following:

**The crowded 2.4 GHz spectrum:** Many companies in urban environments are beginning to complain about the sheer amount of “noise” coming from the growing number of neighborhood wireless LANs as well as more and more equipment such as microwave ovens and medical equipment that broadcast in the 2.4 GHz range. While vendors suggest moving much of wireless traffic to the wide open 5 GHz range, a significant amount of installed base wireless LAN equipment supports only the 2.4 GHz spectrum. Upgrading pads the wallets of wireless LAN vendors but may not be the most prudent action for IT managers to take during an economic downturn. In fact, many customers are lengthening their refresh cycles for all IT equipment.

- **Security:** There is no question but that the adoption of the IEEE 802.11i security specification has strengthened wireless network security. The problem lies, though, in a large number of installed base equipment including specialized devices as well as older PCs that do not support this standard. In many cases, specialized handheld supply chain and medical device manufacturers do not offer newer models that support 802.11i. Since the strongest security chain is only as strong as its weakest link, security can still be an issue. Wired networks are still more secure because data cannot be intercepted outside a facility since it does not travel over the air.
- **Scalability:** While there are reports of some very large wireless LANs deployed, closer inspection reveals that many of these deployments are still in early phases. Deploying a large wireless only network in an environment with data-intensive applications is still an experiment in progress.
- **Bandwidth and the nature of wireless transmission:** Simply put, a switched Ethernet connection to a desktop provides dedicated bandwidth. A wireless LAN connection is a shared connection on a contention-based network. Since wireless radios listen before they transmit packets, the absolute worst situation in such a network is one where data traffic is uniformly heavy rather than sporadic. The situation is analogous to a careful driver trying to break into freeway traffic during rush hour. Prudent drivers slow way down to avoid accidents as do wireless LAN radios transmitting packets. Even wireless LAN schemes that prioritize traffic run into difficulties when traffic is uniformly heavy since that means that certain applications have to be “starved.” The result of prioritization can mean that a voice call is completed but that e-mail access is so slow that productivity suffers.

- **Immediate expenditures:** Wireless LAN equipment vendors who propose an all wireless network argue that customers will save enormous sums of money because they will be able to eliminate unused switching capacity, cancel maintenance contracts, etc. They are quick to offer a calculator to show that in several years, the savings will be astronomical. The problem with such an approach is that it ignores the financial reality that switches and cabling are already installed and in many cases still being depreciated. Many companies are lengthening their equipment refresh cycles now just as they did during the dot-com economic slowdown.

Capital expenditure budgets have been trimmed and in some cases eliminated entirely until customer revenue picks up. Many IT managers are reluctant to spend to fix something that is not yet broken. Upgrading all 802.11a/b/g equipment to 802.11n becomes a “nice-to-have” rather than a “must-have.” That is especially true because moving from relatively small wireless LAN deployments to far larger installations generally requires add-ons that WLAN equipment vendors are not quick to mention including additional sensors for wireless intrusion and detection systems, additional wireless network management software licenses, and additional trouble-shooting tools.

- **Pay now and pay later:** Because historically the refresh cycle for wireless LAN equipment has been much shorter than for wire line equipment, there is the distinct possibility that IT managers will have to upgrade whatever wireless equipment they purchase long before they have to upgrade their wired switching equipment.

#### 1.4 The Maturation of Ethernet in the Enterprise

Virtually all enterprise networks now have some form of switched Ethernet. The sheer economies of scale in the shipment of billions of Ethernet ports have resulted in prices that keep dropping. Virtually all PCs shipping now have built-in 10/100/1000 Ethernet ports. Concerns about the quality of older twisted pair cabling when gigabit Ethernet over copper was first announced resulted in most firms upgrading their copper cabling. Since cabling installation remains the major cost per user of an Ethernet deployment, that cost is no longer an issue since it already been absorbed and written off the corporate books.

#### 1.5 Why Ethernet Is Still Relevant

There are many reasons why IT managers still prefer a wired component to their overall network design including the following:

- **Future proof:** Ethernet vendors have designed roadmaps for faster versions of Ethernet that make use of existing copper and fiber cabling. Replacing a switch module is far more economical than having to replace access points or even controllers as wireless technology evolves.
- **Application contingency planning:** Many IT managers envision video playing a more significant role on enterprise networks in the near future. They are not sure how many video-enabled applications they will support, but video conferencing and even telepresence are likely to play more significant roles in the future. High-definition video is likely to play a more significant role in training which might take place at an employee’s desktop. In any event, there is a comfort level with a wired Ethernet desktop connection because a dedicated 1Gbps connection should provide ample room for network capacity growth.

- **Security:** The air will always be less secure than a wired connection because of far more potential access by outsiders. Particularly in the case where the wireless LAN is an overlay network, endpoint security and network access control are still much stronger on the wire line side than on the wireless side. Equally important, vendors are still grappling with the challenge of integrating what up until now have largely been two separate approaches to security.
- **Reliability:** Fault tolerance is still at a higher level in wired network equipment than wireless network equipment. One area where reliability is of particular concern is corporate telecommunications. Voice over Wi-Fi is still a relative new technology with limited troubleshooting tools. While that situation will change in time, it is a reality today.

## 1.6 Higher Education, Wi-Fi, and Wired Networks

Higher Education historically has been among the earliest of early adopters of wireless networks. It also has been an early adopter of the most advanced wired network technology available. One reason is that colleges have always had very knowledgeable IT departments that were eager for equipment that provided greater bandwidth and were willing to work with pre-standards-based technology. In fact, this group has always been at the cutting edge of technology in order to meet the needs of faculty who always push the envelope.

Universities were among the first institutions to build Gigabit Ethernet networks and to add Wi-Fi networks. They have been the leading adopter so far of IEEE 802.11n wireless networks for a number of reasons:

- Students often have newer laptops that support 802.11n, and they expect the bandwidth 802.11n offers.
- Increasingly, professors expect students to access the Internet during lectures. A large lecture hall full of students with the need for Internet access means a lot of bandwidth is required, and 802.11b/g simply is not adequate.
- Students and faculty expect to be able to access the Internet anywhere on campus including in cafeterias and other public areas both inside and outside. Wireless meets that need for mobility and access.
- Students are accessing more video content which also increases bandwidth requirements.

Some universities are in the process of building out very large Wi-Fi deployments. A number of IT managers at some of this country's largest universities have told ABI Research that they have considered the possibilities of going wireless. One college IT manager said that he had been told to "look into wireless as an alternative to see if he could save any money." He concluded after doing due diligence that in good conscience he could not pull the plug on his wired network for a number of reasons:

- Several key applications on the roadmap including telepresence require far more bandwidth than he could support with his wireless network, but could support with his wired network.
- He felt it was far more economical to leverage his existing wired infrastructure to ensure that every classroom had a couple of Ethernet drops for faculty multimedia presentations and possible telepresence as well as an access point. Lecture halls were a different story and he was contemplating adding 802.11n access points to handle the needs of hundreds of students in a confined space.

- He felt more comfortable with the reliability and manageability of his wired network. In particular, he has been asked to add voice over IP, and he felt the wired network would ensure his phone system was always available.
- Finally, the IT manager worried about future applications that were not even on his radar screen yet. He felt the most economic and prudent solution for the next couple of years was to leverage his investment in wired network infrastructure particularly for faculty and administrative applications and complement it with wireless LANs wherever mobility was required.

While there are a few higher education institutions that have tried going all wireless, most university IT managers appear to agree that the best policy at present is to use wire line and wireless technologies in a complementary way. The Student Technology Center at the University of California Los Angeles campus, for example, advises students on its web site as following:

*The wireless network is not meant to replace the wired network, rather it is provided as a convenience and provides overlay with the wired network. STC recommends students use a wired connection when possible as it provides a faster, more reliable and secure connection than a wireless connection.*

Source: UCLA portal Article ID: 1003604

Stanford's residential computing web page uses a tongue in cheek approach to advise students about the roles of wire line and wireless networks:

***What are the pros and cons of the wireless network versus the wired one?***

*A. The wired network is faster, more secure and more reliable. Because the wireless network is a shared resource, the speed of the signal decreases as more people use the network. Also, while we tried to provide maximum coverage through strategic placement of the APs, the signal may be weaker, or even non-existent, in some areas. For example, if you're sitting in the metal bathroom of your concrete bunker with a metal helmet and your computer is wrapped in tin foil to protect it from the prying eyes of the CIA, you might not get a wireless signal. Additionally, the wireless network is less secure since it is not a switched environment (as opposed to the wired network). On the wired network, only traffic meant for your computer goes to your computer. On the wireless network, traffic is broadcast into the air and your computer has to pick off traffic meant for itself, making the nature of the network less secure. However, in the end, any encrypted traffic, such as your username and password when you login using MacLeland, PC-Leland or Web authentication, is equally secure on both networks.*

*Despite the disadvantages of the wireless network, there are many advantages to remember: the wireless network allows you to connect to the Internet anywhere there is a signal available- in your room, your friend's room, the hallway, the lounge, the dining hall and even outside. This is great for study groups, RT office hours, or just getting outside. Moreover, you can move locations as well- you could be working in the dining hall and move to your room or the lounge without dropping your connection.*

Source: Stanford University Residential Computing Web Site

## 1.7 Healthcare at the Nexus of Wire Line and Wireless Networks

Healthcare also has been among the earliest of early adopters of both wire line and wireless network technology. The primary reason it was an early adopter of wireless LANs has been need physicians and nurses have for mobility. Hospitals have been adding Wi-Fi real time location systems so that doctors and nurses not only can be reached anywhere within a facility, but they also can be located. Wi-Fi phones have replaced cell phones that often did not work well in hospitals because of interference from medical equipment.

Hospitals were among the earliest customers to purchase Wi-Fi bridges to transmit X-rays across parking lots to physician offices so that doctors could examine a patient's X-ray before even leaving an office to see the patient. Asset management using Wi-Fi tags have resulted in savings of 15-20% by locating misplaced equipment rather than classifying such equipment as lost and re-ordering it. Some hospitals use these same wireless equipment tags to keep utilization records that provide them with information on when equipment is fully utilized and additional equipment must be ordered.

While hospitals have major investments in Wi-Fi equipment, they have been slower than universities in upgrading to 802.11n networks. One reason has been the type of applications running on their wireless networks. Most hospitals use their wired networks to handle large video files and administrative data. Bandwidth certainly is a consideration, but concern over HIPAA requirements for data security is also an issue. One example of the headaches HIPAA can cause for hospital IT directors is the growing number of Wi-Fi enabled medical devices. Many of these devices transmit patient data but fail to meet the authentication and encryption requirements of the IEEE 802.11i standard for wireless LAN security. This situation eventually will resolve itself as medical device manufacturers upgrade their equipment offerings, but for the present time, it is unlikely most hospitals will risk violating HIPAA requirements until their risk assessments assure them patient data is absolutely secure.

While many hospital items including computers on wheels are Wi-Fi enabled, many hospital administrators still draw the line when it comes to mission critical equipment. When a patient's life is on the line, they still prefer the reliability of a wire line network.

Hospitals make up a small part of the total Healthcare industry. A large company that focuses on supporting the pharmaceutical industry told ABI Research that is in the process of selectively migrating some of its 802.11g wireless LAN access points to 802.11n. Its goal is to have wireless access everywhere but still offer switched 10/100/1000 Ethernet connections on every desktop. As it opens new facilities, its concession to the added bandwidth offered by 802.11n is to engineer each desktop at one 10/100/1000 Ethernet drop + 20% to cover printing and other network needs rather than a historical two drops per desktop. The company is anticipating much more reliance on video applications in the near future and wants to hedge its bets to ensure enough bandwidth. One point the IT manager made was that many healthcare institutions have modular Ethernet switches that have been refreshed with Gigabit Ethernet upgrades. He felt that there was little need to upgrade switches in the near term. Given his current cabling infrastructure, his wired infrastructure did not require any capital expenditures and was set for the immediate future so he could proceed with purchasing wireless LAN equipment on an as-needed basis and wait for the price of 802.11n technology to drop even further before large-scale upgrades.

## 1.8 Developing a Realistic Network Infrastructure Plan

There is no question but that wireless LANs will continue to enjoy an expanding role in the overall enterprise network infrastructure. Certainly the increasing deployment of 802.11n access points will provide far greater bandwidth and range than previously available. There are a number of factors network managers should take into account when developing their future roadmaps for both Ethernet and wireless LANs.

### 1.8.1 Mobility & Bandwidth Requirements

It is necessary to categorize employees' mobility requirements now and for the near future. What percentage of PCs are desktops versus laptops? While shipments of laptops now surpass those of desktops, the installed base of enterprise desktops still exceeds that of laptops. Chart 1.1 shows that while the tipping point between laptops and desktops already has happened when it comes to shipments, there is still a larger installed base of enterprise desktop PCs than enterprise laptops. Obviously the mix varies considerably by specific vertical market segment. Clearly there are certain environments where mobility and wireless access are critical including the following:

- Network access for road warriors, who periodically return to corporate offices,
- Network access for corridor warriors, professionals who spend their time in meetings or collaborate with other individuals and thus need wireless access to corporate resources while away from their desk,
- Network access for guests and contractors as well as conference room access if a large portion of users have laptops,
- Network access for those employees where mobility is a major part of their job such as hospital physicians and nurses, retail salespeople, etc.

Conversely, there are environments where a wired connection remains critical including the following:

- Environments where employees have desktop PCs and rarely leave their desks,
- Environments that currently require desk workers to work with data intensive applications where very low latency is required,
- Facilities where a premium is placed on absolutely reliable toll quality desktop IP telephony,
- Environments where real-time backups and software delivery are required,
- Environments where ERP and CRM applications are mission-critical,
- Companies planning high-speed future applications including video conferencing and telepresence as well as future proofing for tomorrow's applications such as desktop virtualization that require adequate bandwidth and performance,
- Environments with network powered applications such as sensors, cameras, set-to-boxes, and digital signage.

### 1.8.2 Ensure Cost Comparisons are Accurate

Calculate the cost of wire line and wireless LAN equipment based on apples versus apples comparisons. That means not looking at theoretical green field costs but using real world numbers that take into account that the wire line cabling infrastructure has already been paid for as have existing switches.

### 1.8.3 Security Requirements

There are certain types of facilities where the possible security threat from hackers breaking into a wireless network makes such technology unacceptable. In fact such companies often purchase intrusion detection and protection systems for the sole purpose of identifying any illegal internal deployment of wireless LANs. Despite the latest encryption and authentication schemes, wire line networks likely will always be more secure than wireless LANs because data access is restricted to those with network access.

### 1.8.4 Management Requirements

Wireless LAN management is improving every year but still trails wired network management functionality. Ask yourself what kind of management functionality is required right now as well as what will be required in the future. As an example, over the next two years the Wi-Fi Alliance will launch a number of certification programs including WMM admission control, wireless network management for performance, voice-enterprise testing in multiple access point environments. Enterprise quality voice over Wi-Fi troubleshooting is still in an embryonic state with improvements coming from several vendors within a couple of years.

### 1.8.5 Consider Wire Line and Wireless Complementary Rather Than Competitive Technologies

Plan on leveraging the strengths of both wire line and wireless LAN technologies. Deploy wireless LANs where mobility is absolutely a requirement, but if mobility is not a prime requirement, give employees the benefit of a dedicated, faster wire line connection. If a portion of the workforce requires mobility while the vast majority of employees are desk workers, consider a unified communications approach which includes leveraging the existing Ethernet infrastructure for a wire line phone VoIP connection for most employees and a wireless VoIP connection for those who need it.

Develop a plan for an integrated wire line and wireless network that takes into account the level of wireless congestion at your company's location as well as possible sources of interference. In other words, use the tool that best meets your needs whether it is wire line or wireless connectivity. Abraham Maslow, the renowned psychologist, once said that "if you only have a hammer, then you tend to see every problem as a nail." An unbiased look at the state of network technology today clearly points to a golden mean as the most sensible solution. A hammer is only effective if a nail is the right solution to a problem.

Published 3Q 2009

©2009 ABI Research  
PO Box 452  
249 South Street  
Oyster Bay, NY 11771 USA  
Tel: +1 516-624-2500  
Fax: +1 516-624-2501

<http://www.abiresearch.com/analystinquiry.jsp>

**ALL RIGHTS RESERVED.** No part of this document may be reproduced, recorded, photocopied, entered into a spreadsheet or information storage and/or retrieval system of any kind by any means, electronic, mechanical, or otherwise without the expressed written permission of the publisher.

Exceptions: Government data and other data obtained from public sources found in this report are not protected by copyright or intellectual property claims. The owners of this data may or may not be so noted where this data appears.

Electronic intellectual property licenses are available for site use. Please call ABI Research to find out about a site license.