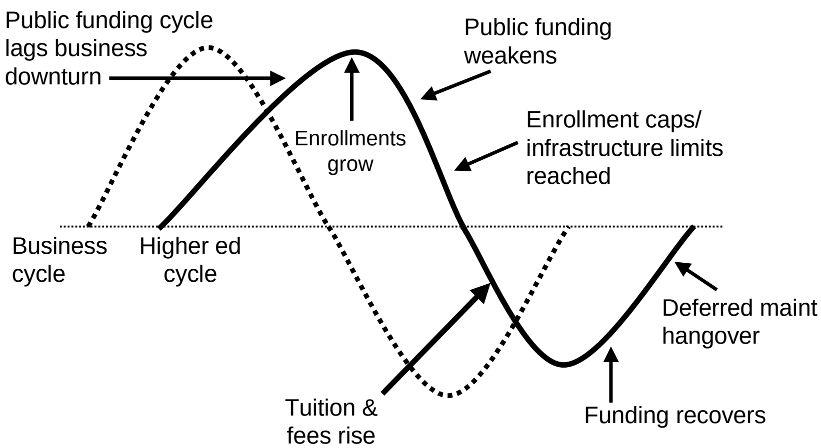
A Peek over the Horizon

Educause Integrated Communications Strategies Meeting
6 August 2003

Ron Yanosky
Principal Analyst
ron.yanosky@gartner.com

Gartner

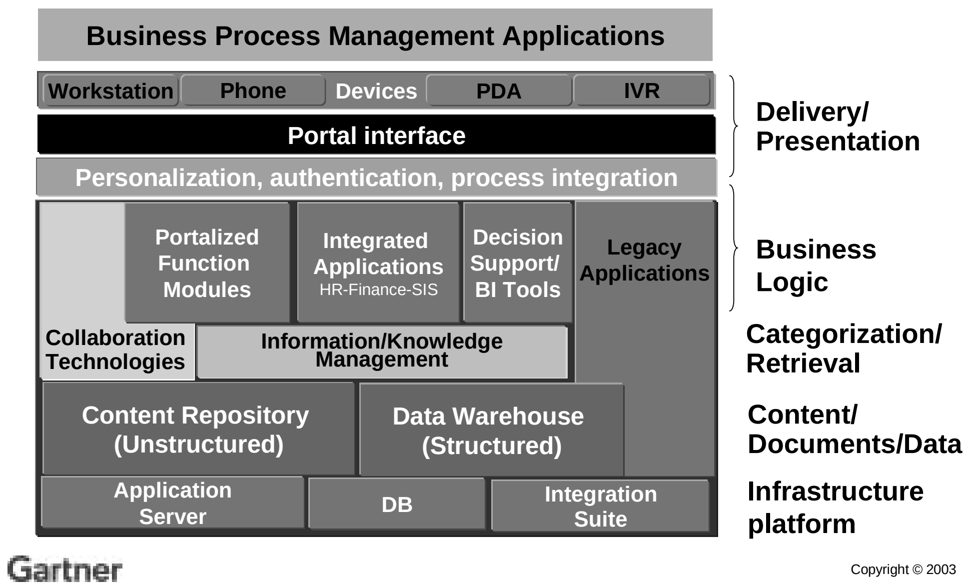
Higher education: from counter-cyclical to trailing edge



Higher education has been a bright spot for vendors of enterprise software since the US economic downturn began in 2001. Blessed with a product for which demand actually increases as the economy weakens, and fueled by a public funding pipeline which kept flowing in the early stages of the recession, higher education IT investment stayed steady or even grew while commercial enterprise software markets declined sharply. But this counter-cyclical tendency has been weakening through successive years of state tax revenue shortfalls and poor endowment performance. Sharp fee increases have made up some of the gap, but only at the cost of eroding affordability and thus threatening enrollment growth. And while there are signs of a modest economic recovery in the US, the same tendency to lag the overall economy which insulated higher education early in the downturn will keep it in the doldrums while other sectors improve, partly because tax collections are often downstream from the activity that generates them, and partly because an improving job market draws away students.

Definition: The reference architecture for business process fusion includes collaboration and content management components, plus integration capabilities based on portal standards.

Toward Business Process Fusion



The platform for BPF applications includes the full range of existing infrastructure components, as is implied by their objective to span traditional architectural silos. This, therefore, includes the base-level components of database, application server and integration broker. The data management facilities include both content management repository and data warehouse – although vendors are consolidating all these capabilities into a single unified database, currently they are delivered as separate components. Collaboration and information management are substantial differentiators from the platform for conventional business applications. BPF applications, by virtue of their end-to-end process support character, must also incorporate existing application systems. Some of this integration may be achieved at the middleware level, but integration via the portal framework will be increasingly important. Emerging portal and Web services standards will make a significant contribution. The externalization of capabilities such as personalization and role-based authentication from individual applications into the portal framework is also an important element of the composite application framework. Finally, although multichannel support (notably for wireless mobile devices) has so far been treated as a tactical addition to applications, this will also be incorporated.

Action Item: CIOs should monitor product and vendor trends that contribute to a business process fusion capability.

The ‘Holy Grail’ of Convergence

- The *converged enterprise* offers its services across multiple electronic channels, backed by a flexible architecture and security model that allow new services to be added quickly at low cost.

It also understands how to serve …

- The *converged consumer* and the *mobile knowledge worker* who access services via several interoperating devices. They will demand device-appropriate services using any channel, at any time, and from any location.

Gartner

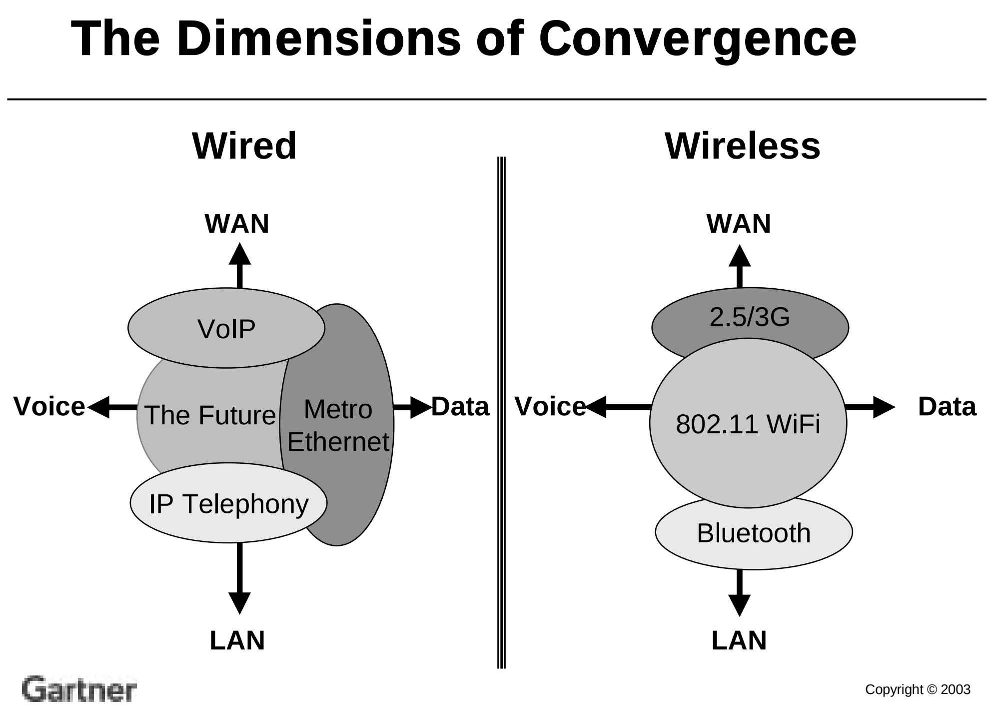
The converged enterprise is designed to serve the converged consumer and knowledge worker. There are no enterprises that can claim to have succeeded in this quest.

Some early movers, however, that are making steady progress are:

- Yahoo
- AOL Time Warner
- DoCoMo

As we have seen in the PC-Internet landscape, the cumulative, first-mover competitive advantage can be difficult to overcome for complex services and supporting infrastructures.

Strategic Planning Assumption: Through 2007, enterprises will work to reduce the number of wired networks they use, while increasing the number of wireless networks (0.9 probability).



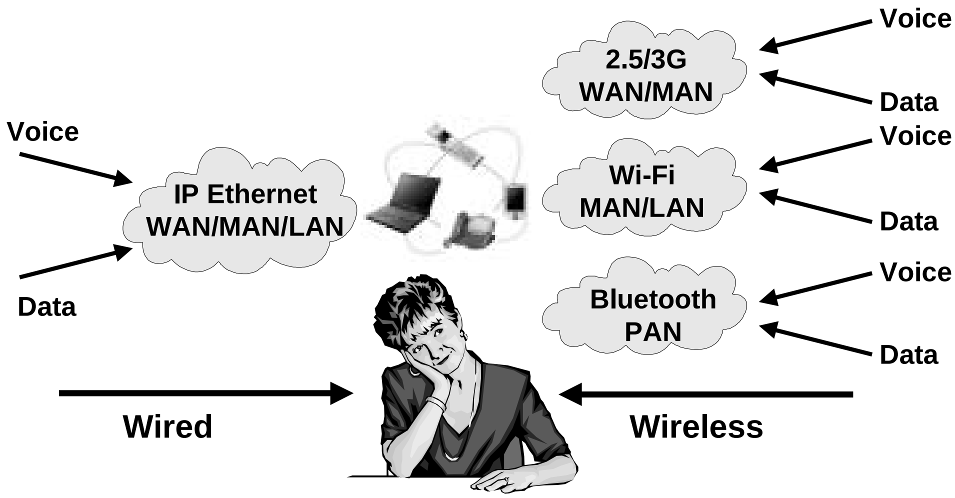
Today, enterprises have four distinct wired networks: a voice in building (LAN), a voice WAN, a data LAN and a data WAN. In the wireless world, voice and data generally already exist in each of the wireless networks; however, these networks have unique spans of control.

In the wired world, convergence will eventually bring a single ubiquitous network, but not for quite some time. There will be several phases or steps in the evolution. Some steps will be performed in parallel, some independently, but many will be interdependent. As a result, the end game and the speed at which your enterprise wants to achieve that goal needs to be well understood. A few of the steps include convergence of voice and data in the LAN, convergence of voice and data in the WAN, or the removal of the LAN / WAN demarcation (with the implementation of Ethernet WANs). Financial, functional and application requirements will drive the prioritization and order of events that an enterprise will need to undertake to achieve its individual goal.

In the wireless world, spectrum and coverage issues, as well as different standards, will force users to work with multiple technologies for the foreseeable future. It will require users and intelligent technology to understand the appropriate solution for a specific application.

Strategic Planning Assumption: By 2007, 50 percent of business devices will be capable of voice and data functionality on at least three of the four wired and wireless converged networks (0.7 probability).

Converged Wired and Wireless: In the Device, Not the Network

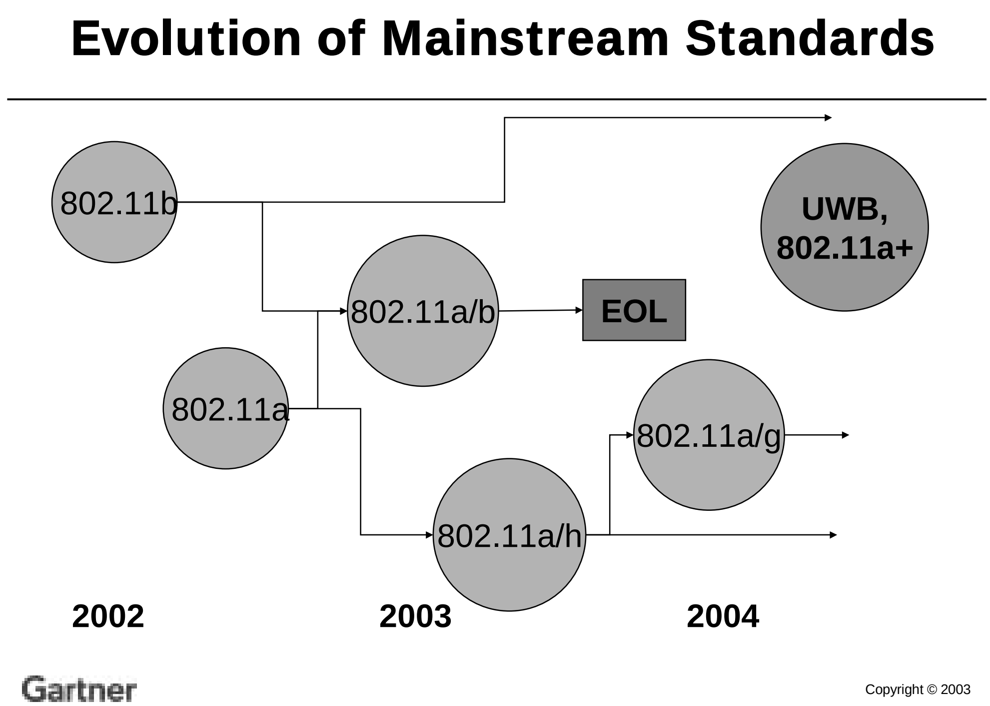


Gartner

Convergence of wired and wireless will occur at the device. The wired network has been working to converge voice and data for many years. Although there are different technologies to achieve that, the end goal will be an end-to-end IP Ethernet network — in the WAN, metropolitan-area network (MAN) and LAN. In wireless, different technologies will coexist throughout the planning horizon. Bluetooth will eventually arrive, supporting voice and data, but in the personal area network (PAN). Wi-Fi will be the MAN/LAN technology and will compete in some case with 2.5/3G, which will be used for voice and data in the WAN/MAN. Devices will be where all these networks converge. Most devices will be voice and data capable but will be engineered to function primarily in a single mode. Depending on the device, the location, the service and bandwidth required — any one of the networks could be used. For example, a person traveling may use Wi-Fi for his PC data in the airport; when he arrives at his hotel, he moves to wired IP Ethernet for voice and data; then, finally, connects to a printer in the hotel room with Bluetooth.

Action Item: Enterprises must understand how wired and wireless networks will converge and how it will affect business devices and applications.

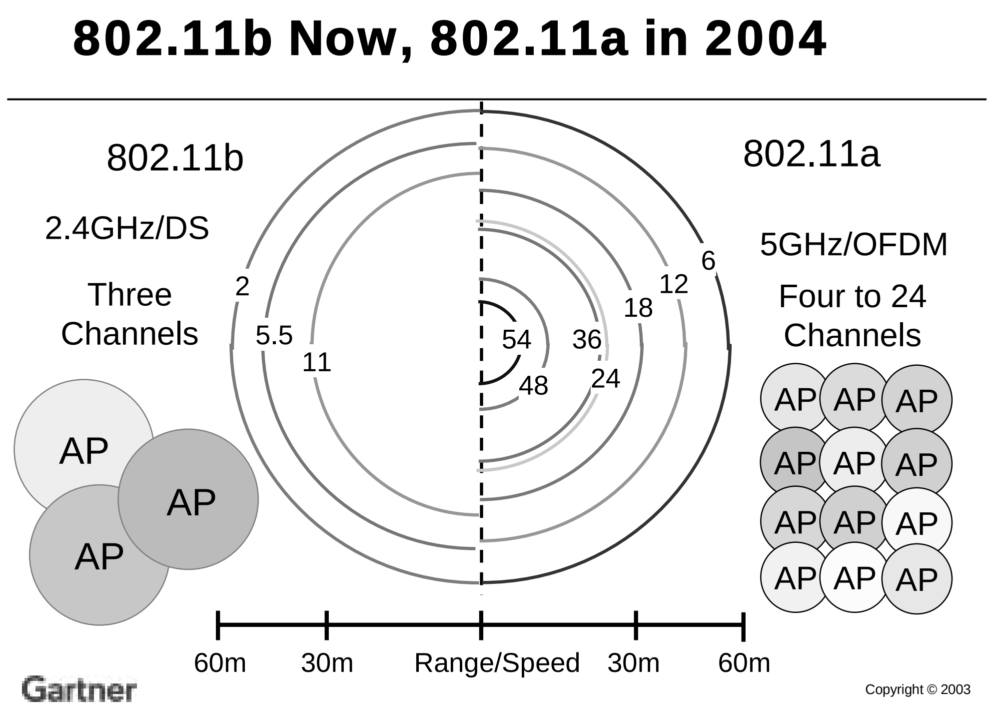
Strategic Planning Assumption: By 1H04, mainstream choices for 802.11 will consist of 802.11a/g and 802.11b technologies (0.7 probability).



Today, 802.11b is the mainstream choice for WLAN deployment. Although 802.11b provides only three channels and operates in an increasingly crowded band, it is more than sufficient for light duty needs in home offices, small offices and as complement to wired LAN systems. 802.11b will be the choice for hot-spot access and internal network interface cards (NICs) in a variety of devices that require long battery life. The next standard is 802.11a, but until 802.11h is approved for European operation and the technology is given time to mature, 802.11a should not be deployed. Many vendors, however, that are depending on 802.11a and its sister standard 802.11g, have begun to release products that they say can support future standards extensions. However, most of these statements can't be trusted because the standards have not yet received approval. Key among these are early releases of 802.11g and combination APs using 802.11a and 802.11b technologies. All these releases will be short-lived and will be eclipsed, by YE03, by 802.11a/g APs that will support 802.11a, 802.11b and 54 Mbps operation in the 2.4GHz band. 802.11b and 802.11a, supported by 802.11h for Europe, will also continue.

Action Item: Enterprises should deploy 802.11b now, and 802.11a/g starting YE03.

Strategic Planning Assumption: 802.11a (Wi-Fi5) WLAN shipments will exceed 802.11b (Wi-Fi) by 1H04 (0.6 probability).



Source: Atheros

802.11a WLANs offer significant technological advantages vs. 802.11b networks. Speeds at the center of coverage can be 54 Mbps, ranging to 6 Mbps at the coverage fringe. Operating at 5GHz, WLANs can avoid interference issues posed by Bluetooth and other consumer devices that operate at 2.4GHz. Additionally, if all 5GHz bands are used (not available in all geographies), up to 12 channels are available. If the application demands, these 12 channels can be combined to provide up to 12 times 54 Mbps — 648 Mbps. The increase in channels over the three available under 802.11b at 2.4GHz also permits more flexibility in deployment.

802.11a is poised to replace 802.11b in enterprise markets once several issues are resolved: 1) a 30-percent cost premium; 2) a lack of alternative chip vendors; 3) approval of 802.11h, which provides Dynamic Frequency Selection and Automatic Power Control to meet the requirements of European regulators for approval; and 4) the approval of 5GHz frequency use in Europe and other regions. This process will take until late 2003, at which time 802.11a will begin to ramp. By 2002, the Wireless Ethernet Compatibility Alliance (WECA) will provide Wi-Fi5 certification, which should build purchase confidence, increase volume and drive down prices.

Action Items: Enterprises can begin broad deployment of 802.11a in 2003. Enterprises should not remove 802.11b installations.

Strategic Planning Assumption: Through 2007, throughput will average 50 percent of the theoretical link rate (0.7 probability).

Link Rate vs. Throughput

5GHz		
Mbit/s	Net Mbit/s	Efficiency
6	4.6	77%
9	6.7	75%
12	8.7	73%
18	12.4	69%
24	15.8	66%
36	21.5	60%
48	26.2	55%
54	28.3	52%

2.4GHz		
Mbit/s	Net Mbit/s	Efficiency
1	0.8	82%
2	1.5	76%
5.5	3.4	62%
11	5.2	47%

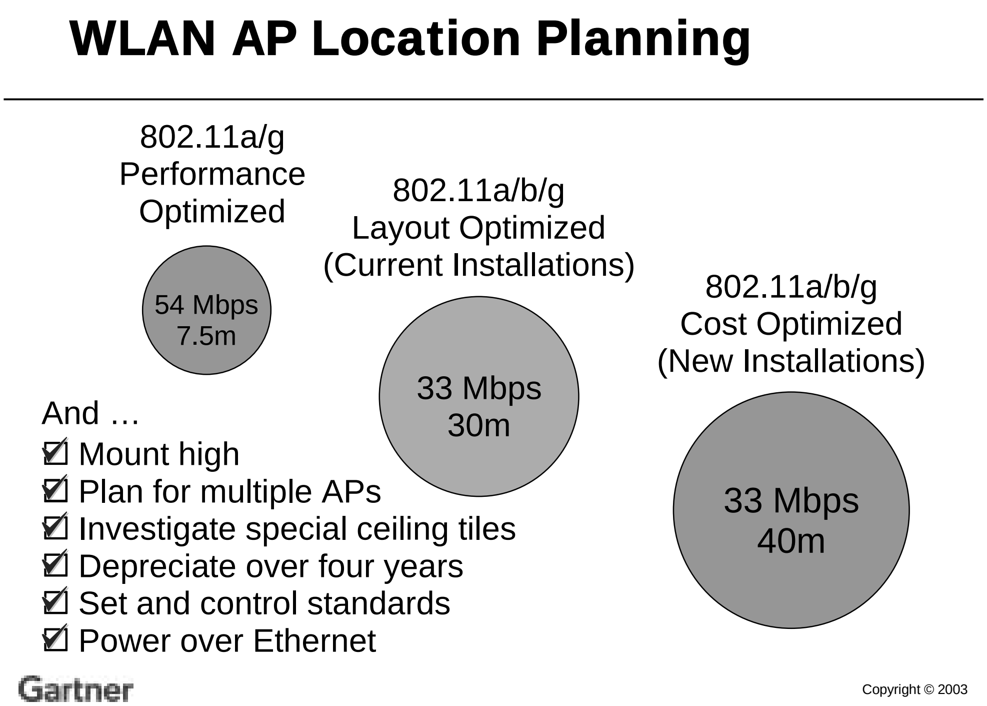
Gartner

Source: Avaya

One of the most-misleading specifications in wireless products is the promise of speed. Wireless is a shared medium, which means that throughput varies by the number of users connected to the access point (AP). The reduction in bandwidth per user is greater than in wired systems, which can employ switching mechanisms to preserve bandwidth. Also, wireless is subject to interference that causes retransmission of data at the expense of bandwidth. The theoretical maximum of any wireless network is referred to as the “link rate.” The nominal bandwidth, a figure that can vary widely based on conditions, is generally what will be expected on a lightly loaded system (listed under the Net Mbit/s column above). Higher speeds at higher frequencies are subject to greater degradation over a given range than more-modest technologies because of less-favorable properties of higher speeds and the desire by vendors to push speeds over unrealistic ranges.

Action Item: Users should plan applications for roughly half the stated link rate of any WLAN system.

Strategic Planning Assumption: Despite the emergence of 802.11a networks in 2003, 802.11b (Wi-Fi) installations will have a primary useful life of four years (0.7 probability).

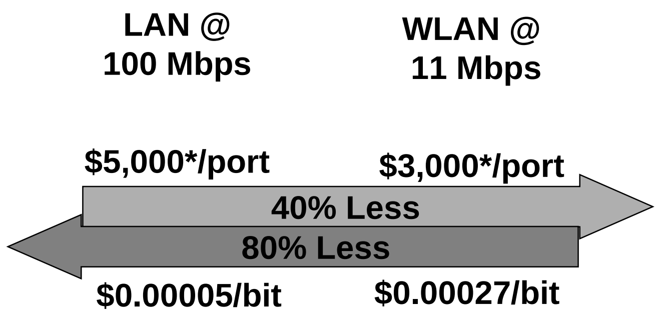


With the emergence of 802.11a and 802.11g, WLAN deployment strategies have become more complex. There are three likely scenarios that enterprises will use in planning. 1) Performance Optimized takes maximum advantage of the increased throughput available in 802.11a and 802.11g systems. The downside is that consistent 54 Mbps operation will require APs roughly every 25 feet (7.5 meters). Such throughput requirements are unusual, and most enterprises will move to 2) Layout Optimized, which will serve the needs those that already have deployed 802.11b and want to avoid running new Ethernet and power connections to new locations. This scenario trades these costs against the expected 5-percent premium for 802.11g and 30-percent premium that will need to be paid for 802.11a APs. 3) In the Cost Optimized scenario, users deploy 802.11a or 802.11g APs at a greater radius than would be used for 802.11b, to offset the cost premiums. Even at such increased distances, a significant improvement in throughput is made available vs. an 802.11b implementation. The latter scenario makes sense only for "greenfield" implementations, or where the cost of running new data cables and power is not significant.

Action Item: AP deployment at a radius of 100 feet (30 meters) will be cost-effective for most installations.

Strategic Planning Assumption: Through 2007, wired LANs will maintain an advantage in cost per bit (0.8 probability).

Cost Per Port vs Cost Per Bit



*Annual total cost of ownership based on three-year analysis

Gartner

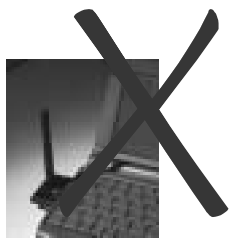
Many potential enterprise buyers have asked whether they should move to a 100-percent WLAN operation. Although it's possible to do so with several upcoming technological improvements, such as 802.11a, an analysis of costs demonstrate that this may not be an effective move when considering future needs. The key figures used to analyze this are cost per port and cost per bit. Clearly, because less wiring is needed to deliver Ethernet to users, the cost per port is much less expensive. However, if application needs include streaming video and other high-bandwidth requirements, the cost for delivering the required number of bits is much higher because of the need to create a very high-density, high-speed network. Also, for some applications, the required bandwidth may not be possible to get.

Another factor to consider is whether mobility is required. If mobility is important and the applications are typical (for example, e-mail and Microsoft Office), WLANs may be cost-effective. However, as occurs in many enterprise headquarters where wired capability is prevalent, WLANs are more likely to be viewed as adjuncts to wired networks than as replacements.

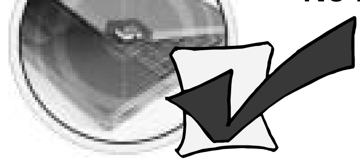
Action Item: Enterprises should deploy WLANs where mobility is required and bandwidth needs are limited relative to wired systems.

Strategic Planning Assumption: Through 2005, integrating WLANs with PC/notebook purchases will prove to be more cost-effective than post-purchase upgrades (0.7 probability).

Time to Buy Integrated WLANs



- **Better antenna design**
- **More secure**
- **Enforces standards**
- **<$100 install vs. $250 upgrade cost**
- **No lost cards**
- **No broken antennas**



Gartner

Internal WLAN options can be found on most notebooks and increasingly are becoming available on personal digital assistants (PDAs). Cellular phones also may have WLAN capability within several years. The general consensus in the client base is to purchase PCs and notebooks with sufficient resources so that they do not have to be upgraded during their three- to four-year lifetime. The cost of an upgrade often is deemed to be more expensive than the purchase of extra resources at the time of initial acquisition. Therefore, Gartner recommends that notebooks be purchased with a maximum configuration of memory and disk. We estimate that it will cost an IS organization approximately $250 to have a technician service a notebook computer for the purpose of upgrade to an internal WLAN. The cost of an internal WLAN option is about $100 and should decline to $50 or less by YE03, making this a viable purchase option. External cards would be far-less costly, but they provide less range, can get lost or the antennas can be broken off. This strategy would not make sense if there is no need or if the enterprise does not believe that WLANs will be mainstream within the life of the product.

Action Item: If funds are available, enterprises should purchase notebooks with 802.11b internal WLAN capability.

Tactical Guideline: WiFi Protected Access certified WLAN equipment will provide business strength security with multi-vendor interoperability by 4Q03.

Wireless Security Standards Are Neither Secure nor Standard

- WEP is broken but better than nothing
- WPA (2Q03) will bring WLAN to business level security but…
  - Need to move to AES at next refresh cycle
- Simple access points with smart switches are the way to go long term
- Still need to worry about end point security
- Don't forget about public hot spots

Gartner

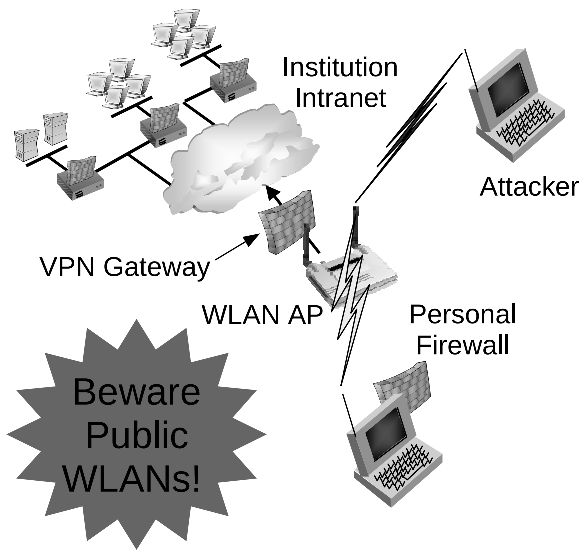
What will be the most urgent security issues for mobile and wireless users in the next five years?

In the early days of the Internet, standards bodies were happy places, where engineers from competing companies worked together to make the Internet more usable for the good of all. This is no longer true in the wired world, as companies jockey to drive standards for competitive advantage, and the unique makeup of the wireless world has meant that it has never been true there. Software vendors, hardware vendors, carriers, handheld device vendors and service providers are all vying for supremacy in the nascent wireless world.

The bottom line is that the slow pace of wireless security standards requires vendors to ship insecure products as the lowest common denominator and the offer proprietary implementations for higher security capabilities. This had driven Gartner to recommend that enterprises rely on application or transport level security, such as SSL or IPSec, rather than the security built into wireless devices. The major vendors agreeing on the WPA standard and certification process will provide a cross-vendor de facto industry standard by the end of 2003.

Tactical Guideline: Sensitive WLAN interfaces should be placed on a dedicated segment of a virtual LAN (VLAN) and should be audited regularly. “Visitor-grade WLANs,” if allowed, should be isolated from direct access to internal resources.

Security Directives for WLANS



Defensive Measures

- Policies
- Proprietary security

or

- Upgrade to WPA; buy WPA Q403
- Run VPN
- WLAN “sniffers”
- Device firewall
- TKIP

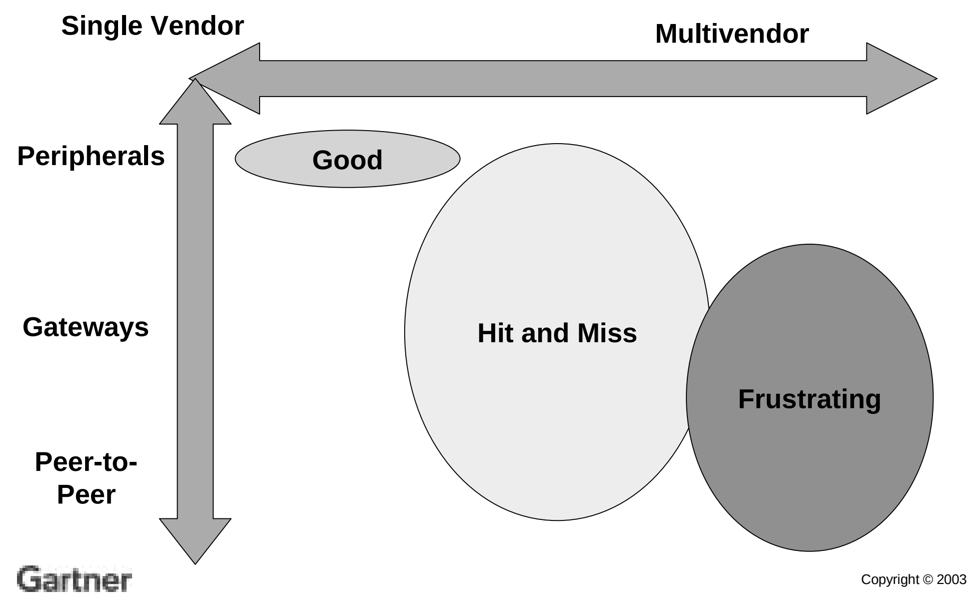
Gartner

Because current WLANs use radio frequency (RF) signals in the 2.5GHz range to carry network traffic, they are vulnerable to eavesdropping by anyone with a PC and a wireless NIC or inexpensive frequency scanner. For sensitive WLAN deployments, we recommend that enterprises follow these tactical guidelines:

- Change the security. Do not use default Service Set Identifier (SSID) numbers or null SSIDs.
- Implement wireless APs on switched network ports.
- Support departmental wireless networks.
- Use 128 Data Encryption Standard with dynamic session keys. Do not use 40-bit Wired Equivalent Privacy (WEP).
- Implement message authentication code (MAC) address tracking to control network security.
- Monitor access logs: Track network access attempts via Internet Protocol (IP) address. If an attacker attempts access, the logs will point to the source address and make it easier to track and stop. (Current monitoring tools are immature.)
- Evaluate physical security perimeters. Where possible, observe the grounds out to the limits of coverage, and advise the security department to look out for suspicious activity.

Strategic Planning Assumptions: Through 2005, Bluetooth certification will not include interoperability testing through a single body (0.7 probability). By YE04, Microsoft will exert itself as the de facto interoperability testing organization (0.6 probability).

Bluetooth, A Support Challenge



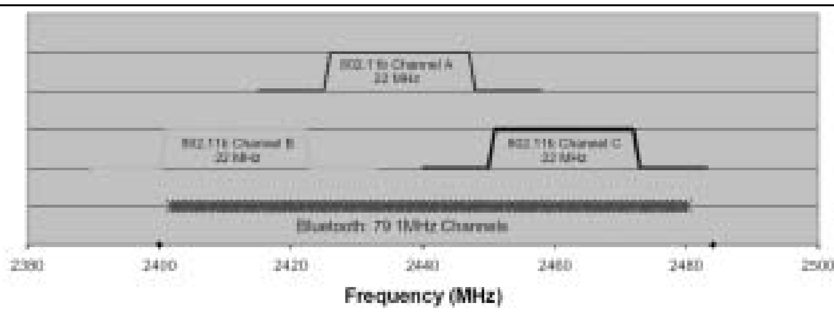
Bluetooth proliferation is upon us. Bluetooth will appear in millions of products during the next few years, and it will be a useful technology. Where Bluetooth is provided by a single vendor in all the products for a single user, the experience should be pleasant. An example would include a Bluetooth keyboard and mouse, a Bluetooth printer and a Bluetooth PDA, all provided from one vendor. Such vendors will ensure that interfaces are clean and seamless. The terminology of operation will be consistent. Any required extensions not covered in the Bluetooth specification will be implemented in the same way. Most importantly, a single vendor will stand behind the operation of Bluetooth in its products.

Some vendors will provide some of the products and recommend others backed by their commitment to test interoperability. The experience in this case should be reasonably good; however, because the vendor does not design all of the products, implementations may vary and require greater support (for example, one vendor may use the term “pairing” and another use “bonding” to designate the same function). Finally, users who make assumptions about products carrying the Bluetooth logo will continue to be frustrated by the fact that the logo simply means the product has been tested against a specification, rather than for interoperability.

Action Item: IS organizations should insist on Bluetooth interoperability testing from its vendors.

Strategic Planning Assumption: Through 2005, Bluetooth will continue as a personal-area network (PAN) technology, separate and apart from 802.11 (0.7 probability).

802.11b and Bluetooth Conflict



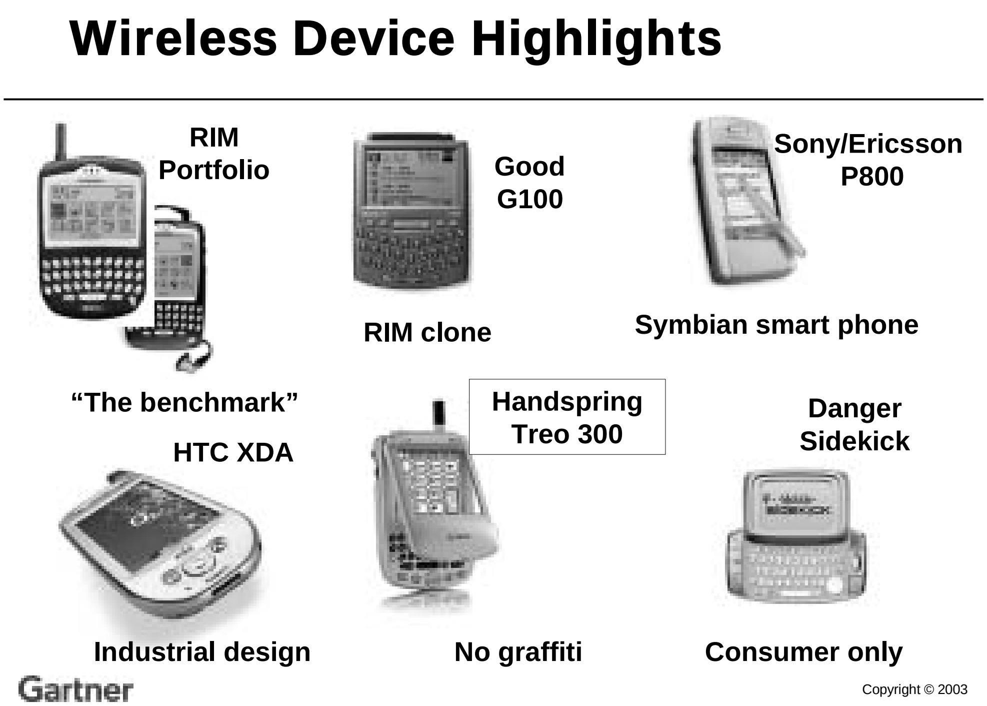
- Problems within 2 meters
- Reduced throughput . . . but mostly a minor issue
- Vendors working on combination solutions
- Adaptive hopping approved in United States
- Proprietary solutions to outstrip 802.15 efforts

Gartner

802.11 WLANs have been architected by network designers and fulfill many of the structural and management requirements of networks. Bluetooth has emerged as a much-needed PAN technology, but with little planning on how it would affect other technologies with which it shares the 2.4GHz band. Because Bluetooth is based on “frequency hopping” across the 2.4GHz band, it is both more immune to interference (because it simply hops to another location to retry transmission) and an interference creator for direct-sequence 802.11b networks. 802.11b is channelized, and it sees Bluetooth as increased noise in its band. Most tests by manufacturers have shown that, at most, Bluetooth creates a 20-percent reduction in throughput when radiating constantly within six feet (two meters) of an 802.11b transmitter/receiver. However, the Bluetooth specification permits higher-power-output schemes that could “pollute” the 2.4GHz band. Various Bluetooth manufacturers are producing APs that will reach 100 feet/35 meters, a distance comparable to 802.11b range. Should these two systems be colocated, problems will occur, especially with the volume of Bluetooth systems that we expect to be in use several years from now.

Action Item: Enterprises must manage the wireless spectrum within their buildings.

Strategic Planning Assumption: Through 2006, buyers will face dramatic shifts every six months in device designs, device capability and application development platforms for mobile phones and handheld devices (0.8 probability).

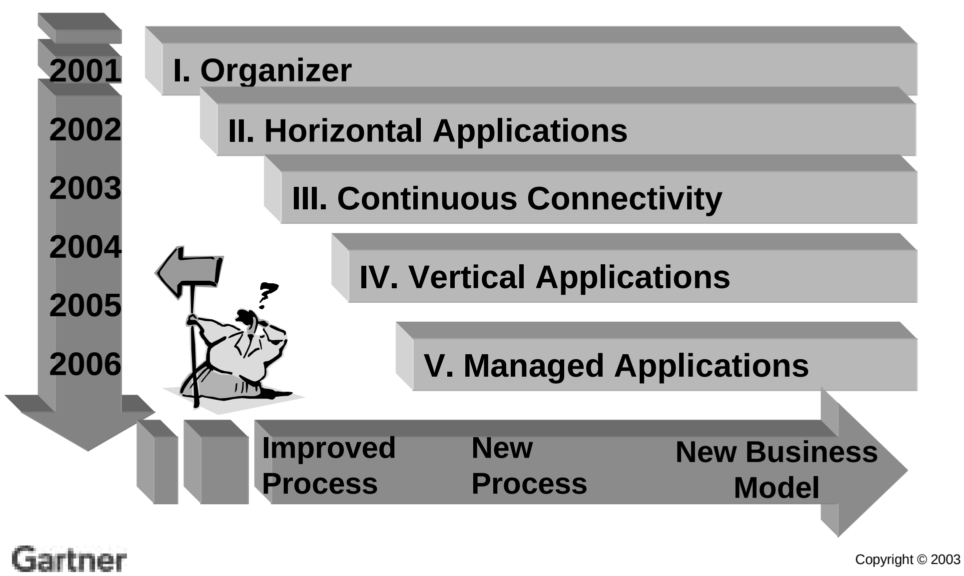


Mobile computing forces a collision among vendors with diverse areas of expertise. It is not simply technology or enterprise support that makes a product successful. There are incumbent vendors with technology prowess, but they will be challenged by marketing stalwarts, and those who understand the message of style — that mobile computers are part of one's personality. Highly mobile devices are shaped more by factors closer to the fashion industry than the PC industry. We could also see financial institutions' private-brand machines, and if the promise of phones as a form of credit card succeeds, we could see enterprises such as Visa or major brokerage houses dominate the mobile market. i-mode is an example in which a national telecom provider forced manufacturers to remove their brand names in favor of the service brand. We could see weaker vendors take advantage of emerging trends (such as wireless photography) to seize the opportunity to become stronger in the new field (for example, Canon using its expertise in cameras). More than likely, we will see vendor alliances that understand that it takes various skills to be successful. In summary, the proliferation of device choices will continue through and beyond 2006, making the process of content delivery more challenging than ever.

Action Item: Construct multichannel applications to be immune to changes in networks and devices.

Strategic Planning Assumption: By mid-2005, application designers will begin to develop new breeds of applications that will rely on the core assumption of pervasive wireless data devices (0.6 probability).

PDA / Smart Phone Generations

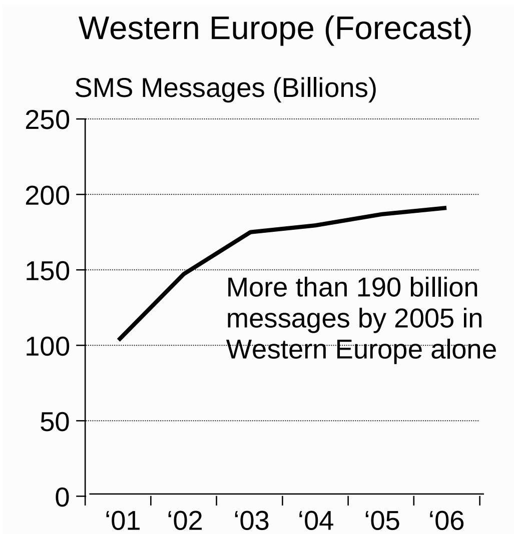


In 2001, the handheld market began to move out of its first generation, the organizer phase, where most purchasers of PDAs employed simply the contact and appointment features of the device. At present, we are entering the second generation of PDA evolution. In this phase, users will begin to expand application needs beyond the embedded applications, specifically looking for access to “horizontal content.” By “horizontal content,” we are referring to back-office and PC-based applications where no customization is required, including e-mail, databases and Microsoft Office. In 2003, the third generation will involve adding the requirement for continuous wireless connectivity to those applications. Over-the-air synchronization of back-office data will become more commonplace. Toward 2004 and 2005, the fourth generation of PDAs will signal a fundamental change in how they are viewed. In this phase, we expect enterprises will build new applications with the assumption that PDAs exist as mainstream devices. This step will be analogous to the point at which application builders can count on a PC on everyone’s desk. Prior to this point, PDA functionality will remain an awkward add-on. In the fifth generation, as is usually the case, management functions will be added as an integral component, finalizing the absorption of the PDA into mainstream computing.

Key Issue: How will mobile messaging evolve during the next five years?

Strategic Planning Assumptions: In 2005, the number of mobile messages sent monthly in Western Europe will exceed 190 billion (0.8 probability). By 2005, the average penetration of MMS-enabled mobile phones in the European Union will exceed 65 percent of the population (0.7 probability).

Everything Started With SMS



- Most-pervasive nonvoice mobile technology exists in Western Europe
- 40 percent to 60 percent of users in Europe are “textual” (growing trend)

Gartner

Source: Gartner Dataquest

The SMS market, when first introduced in 1992, was initially misunderstood. No one could have predicted its huge success. When the service was delivered as a full solution in late 1994, many believed that the key market on which to focus was the corporate / enterprise market. There was much skepticism as to whether or not it would ever be realistic to expect users to originate messages from a mobile handset. As mobile operators evolved their business models to address the consumer mass market, a new generation of mobile-phone users — predominantly young people — joined the market. With limited financial resources, a desire to have control over their spending, and an aptitude for new technology, they embraced SMS with an expected vigor that had not previously been encountered. Messaging growth was predominantly driven through viral marketing as young people became aware of this new communication medium. In June 2001, the Vodafone Group stated that 42 percent of its European customers were SMS users, accounting for a staggering 9 percent of the average revenue per user (ARPU). As shown by the above statistics, SMS is now widely embraced by the mass market. Person-to-person messaging has been a phenomenal success for the mobile phone industry in European and Asia / Pacific markets.

Action Item: Enterprises must consider mobile messaging as part of their communications strategy. Mobile messaging is now so pervasive that enterprises ignore it at their peril.

Strategic Planning Assumption: Until 2004, SMS will remain the dominant mobile messaging technology in Western Europe (0.8 probability). Privacy issues and "spam" will be the main challenge for carriers in the next 18 months (0.8 probability). Mobile-messaging penetration will increase in the United States exponentially in the next three years because of improved interoperability and consolidation of network ownership (0.7 probability).

A Compelling but Limited Technology

Technology

Value

- Allows personal content exchange
- Creates a business case for nonvoice messaging services
- Enables further applications such as advertising, gaming and voting

Limits

- Capacity and throughput
- Quality of service
- Spam, privacy and copyright
- Interoperability and cross-network connectivity

Market

Drivers

- Cheap means of communication
- Prepaid youth equals positive attitudes
- Increase in usability (e.g., T9)
- Asynchronous textual personal communication

Obstacles

- Poor interface limits adoption to young people
- Nonreliable delivery and security lacks

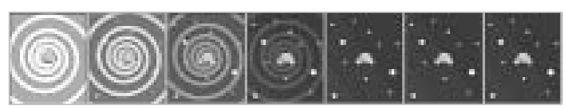
Gartner

The growth of the SMS market was predominantly driven through viral marketing as young users sent messages to each other and became aware of this new communication medium. These users responded very positively to this medium, and short messaging has become part of their lifestyle. As mobile handsets have evolved and messaging as an application has become more popular, more attention has been given to the human interface usability, introducing predictive algorithms such as T9. SMS has more recently become a vehicle for other applications, such as advertising, gaming, voting and information delivery. For example, MTV has a "jukebox style" program called "Videoclash," which invites viewers to vote for the music video they would most like to see by sending text messages to a central MTV server. Despite its success, SMS technology faces some significant challenges in many areas, such as capacity and delivery reliability. Because SMS is a "store-and-forward" technology, messages are delivered sequentially rather than broadcast. This can cause significant delay in the delivery of content sent to large audiences. This is particularly relevant when thinking about time-critical content such as information services (e.g., football scores or TV quiz shows). The lack of security may limit the possibility to offer SMS-based services to customers/end users, due to privacy issues. Permission must be sought from users to communicate directly with their mobile terminals using mobile messaging.

Action Item: When deciding to harness this technology, consider carefully the constraints of the technology and open issues affecting end users (e.g., privacy).

Market: Enhanced and multimedia messaging will start gaining mass-market acceptance during 2003, while SMS traffic growth will start declining in 2004.

Technology Evolution Toward MMS

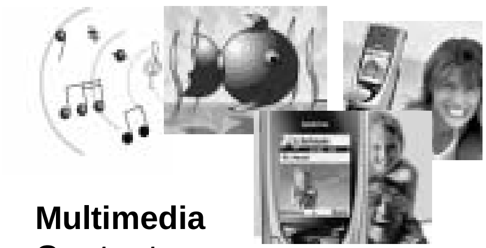
Short Message Service (SMS)	160 character text on a mobile phone	
Picture Messaging (PM)	Combines sound, pictures and enhanced text	
Multimedia Messaging Service (MMS)	Rich content, including GIF, JPEG, MP3, MPEG	

Gartner

As SMS moves into a new phase of exponential growth with new applications, such as gaming, information services and advertising, the market is poised to embrace richer messaging solutions. The new standards, PM (e.g., EMS or Nokia Smart Messaging) and MMS, enable users to further personalize messages with pictures, sounds and animations. New standards add richness to mobile messaging with the capability to not only send text, but to attach other media type, such as images and sounds. The MMS and picture messaging standards do not draw on existing messaging technology, but require new infrastructure to be deployed by the network operator; uses a wireless data bearer — e.g., General Packet Radio Service (GPRS) and third-generation (3G) networks — to deliver messages; and requires new functionality in mobile terminals. MMS is a jointly defined messaging standard by the 3GPP and the WAP Forum and will provide a broad set of new features. Central to the deployment of MMS is the MMS-Center (MMS-C), which is a distributed architecture that draws heavily on existing e-mail standards such as Multipurpose Internet Messaging Extensions (MIME) and Simple Message Transfer Protocol (SMTP), as well as the mobile standards like SMS. This approach will favor convergence of mobile services with the Internet — for example, sending MMS messages to both mobile phone numbers and e-mail addresses. *Action Item: Start now to evaluate the possible exploitation of multimedia messaging in your business.*

Strategic Planning Assumption: Multimedia messaging facilities will be present in more than 80 percent of phones shipped in the European Union in 2005 (0.7 probability).

The Value of Multimedia Messaging



Multimedia Content

Still Images +
Sounds +
Animations +
Video Clips =

High Value Contents

Gartner

Multimedia Messaging

- **Low-Cost:** Less expensive than a paper postcard with stamp.
- **Very Common:** Penetration in teenagers exceeds 75 percent in some European countries.
- **Personal Content:** People exchange their own created content.
- **Precise Identification:** A phone owner is a precise marketing target.
- **More Than Pixel:** Also bar codes, vouchers, tokens and tickets.
- **Real-Time:** Few-second delivery allows for quizzes, entertainment, etc.
- **Bidirectional:** Increasing availability of enabled phones will permit two-way messaging.

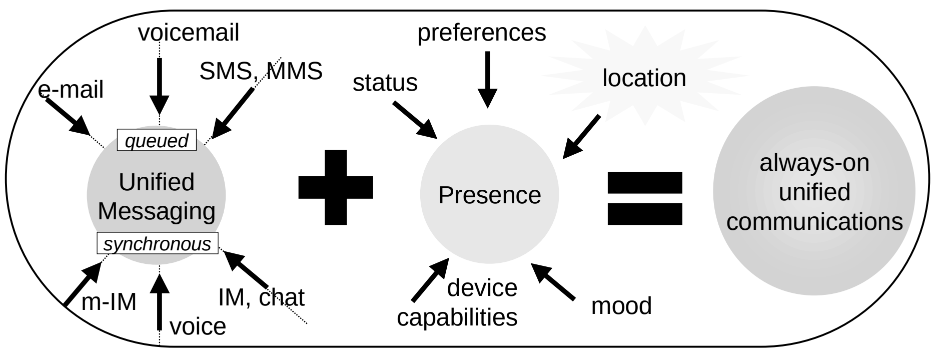
Media has value; more-sophisticated media has greater value. Media is not just a way to communicate information, but has intrinsic personal value (e.g., pictures of television stars or music clips are attractive to groups such as teenagers). Still images are potentially more valuable than text, animations more valuable than still images, and so on. Sounds, still images, animations and video clips can be used in many ways, particularly in a marketing context as incentives and rewards. The value of media, even on restricted devices, is illustrated by the fact that consumers are prepared to pay for it — consider the iMode system in Japan where subscribers pay to receive images and animations, and the fact that European mobile phone users will pay for ring tones and mobile screen saver images. The computer technology to create and manipulate sounds and images continues to improve and will, increasingly, be applied to create customized images and video clip. Technologies, such as those used to generate entirely virtual characters — like Orange's "Ananova" — will be deployed to personalize and customize images and video clips (e.g., "Happy birthday from Ananova" video clips or a "favorite star" standing next to a teenager in a picture). Such techniques can further increase the value of media clips.

Action Item: Consider which opportunities multimedia messaging offers your business.

Market: Web-based synchronous communications, such as instant messaging (IM) and chat, are becoming mainstream business utilities, used to communicate among colleagues and between customers and the enterprise. In addition to mobile queued messaging (e.g., SMS and e-mail), mobile users will increasingly demand that mobile IM and chat services be seamlessly integrated with homologous Web-based messaging.

Strategic Planning Assumption: By 2005, 80 percent of peer-to-peer messaging will be "instant" and exploit presence information, including mobile location (0.8 probability).

Future Messaging Evolution



Key Success Factors

- Personal content creation
- Peer-to-peer content sharing
- Communities creation

Presence Messaging Services

- Find-a-friend, located community
- Personal information management
- Multiperson meeting arrangement
- Sales-force tracking and coordination

Gartner

Voice call is the most traditional synchronous ("immediate" or "instant") interpersonal messaging option. E-mail and mobile short messages (SMS) are popular tools for queued communications. Progressively, Web IM and chat are emerging as communication means and will converge with queued mobile messaging and e-mail in a unified messaging model. In this model, instant messaging will be preferred to queued means. When, where and how to best reach a party will be solved by "presence" (i.e., real-time information about a person's status — such as a message that they're available, busy or in a meeting); communication capabilities (e.g., voice, GPRS and multimedia); geographical location; preferences; and the like. So far, one messaging key success factor is to allow the exchange of personal created contents. This is going to be pushed further by peer-to-peer "shared content" support, thus allowing for personal unified storage areas of pictures, music and other contents. The Wireless Village initiative is working toward this. Initial mobile location messaging services are already in place in some European countries (mainly for youth — e.g., "friend finder" allows people to invite friends in a group to be located and communicate). Future services will include agendas and multiperson meeting arrangements through location. *Action Item: Enterprises should evaluate the adoption of unified location-based instant messaging for employee-customer interaction to speed up response time.*

Case Study: MoBull Messenger, USF, Florida (U.S.).

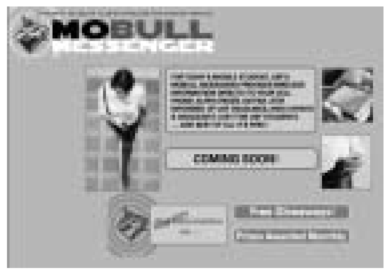
Market: MMS will not spread in the United States before 2004.

U.S. Markets Are Behind, but Demand Is Provable and Growing

University of Southern Florida (USF): Out of 37,000 students, 91 percent carry cell phones, and 9 percent carry pagers or PDAs.

Students: Desired better online communications with USF, and USF sought a new revenue source.

Mobile/Remote Application: Wireless messaging supports class changes, school closings, emergencies and payments, as well as time-value coupons and rebates from local merchants.



Results

- Built in less than three months by two staff members using Air2Web's Mobile Internet platform. Gross revenue forecast to USF of $125,000 in the first year of operation.
- Retailers seeing a return of 10 percent or better on paperless advertisements to prospects who have opted-in. Advertisements can be selectively targeted (e.g., age and geographic location).
- Two-way capability, the next phase of project, will allow correspondence with school departments and advertisers.

Gartner

The University of Southern Florida (USF) created MoBull Messenger, a wireless coupon and information program, in response to a $900,000 cutback in state funding due to an economic downturn. (MoBull stands for the Mobile Bull, a tie-in to USF's bull mascot). USF chose Air2Web to leverage commercial, off-the-shelf code and the large number of wireless services supported by Air2web's Mobile Internet. The application is straightforward and uses SMS, XML and SQL interfaces.

Between the spring and fall of 2002, almost 2,000 students signed up for the service, and signups have since accelerated in response to marketing campaigns. More than 46 retailers are participating — including local restaurants, clothing stores, bike shops, nightclubs and hair salons. Students sign up with participating businesses to receive discount coupons on their cell phones, personal digital assistants (PDAs) and pagers. They specify the types of information and offers they want to receive, as well as time periods in which they want to block messages. They can also sign up for real-time campus information updates, such as class schedule changes, school closings, emergency alerts and payment deadline reminders.

Action Item: U.S. enterprises should start now to evaluate business opportunities in SMS.

Tactical Guideline: Enterprises should define a risk management process to establish and evolve policies and processes for adoption of mobile applications and business propositions based on multimedia messaging.

Risks Are Still There

Risky Situations

- Pictures: “subjects” may not approve
- Spies: from restricted areas, confidential conversations or visuals recorded and sent outside
- Spam: marketing and advertising messages sent in large amounts to phone users
- Violence: threats to users of adult games and services (e.g., mobile dating)
- Damages: faulty services can lead to user damages (e.g., wrong traffic directions resulting in employee losses)

Categories of Risks

- Individual: an individual may perceive an MMS application as violating privacy and abandon it
- Business: employees may perceive MMS applications as intrusive and against work protection laws
- Clients/End Users: may sue for liabilities after damages

Understand Risks
Define Policies and Procedures
Monitor Risks

Gartner

There are a number of threats posed by mobile services (particularly multimedia messaging) to individual privacy and security, which originate significant risks for individuals and enterprises.

•*Individuals* will be concerned by an uncontrolled use of their image with the availability of multimedia phones. This may pose risks to their relationships with relatives, employer enterprises and government organizations. In Greece, the usage of camera-phones has been banned in certain places.

•*Enterprises* deploying MMS-based service to enhance their internal processes will face legal risks, particularly if these services generate data/images on individuals that will be used for activities like job monitoring or by players like law enforcement organizations. These services may infringe on current worker protection laws.

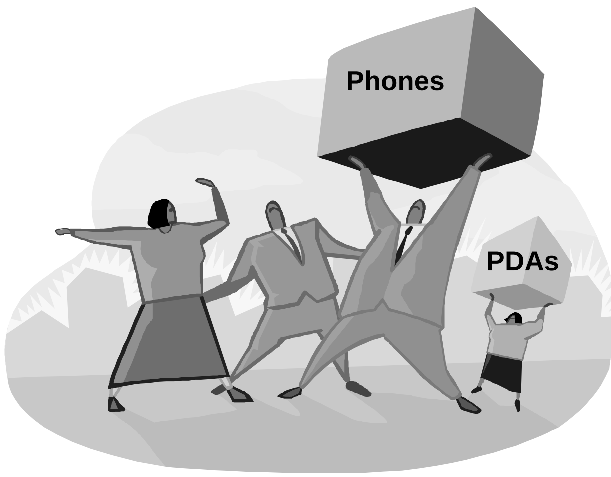
•*Clients and end users* who adopt MMS-based application and meet with damages will likely sue enterprises offering such services (e.g., a faulty traffic information service that causes a businessman to miss an appointment and lose an important contract).

Risk analysis, risk management policy development and risk review must be ongoing activities.

Action Item: Enterprises should seek legal advice to assess the implications of MMS-based service adoption, identify risks, define policies and procedures to manage risks, and establish a monitoring team.

Tactical Guideline: Enterprises must develop mobile adjuncts to client-device policies to protect information assets and to contain costs.

Building Blocks for Mobile Support



Key Tactics

- **PDAs and phones to PC group**
- **Three levels of support**
- **Install "PDA firewalls"**
- **"Cafeteria plan" for cost control**
- **Purchase mobile management tools**

Gartner

Developing a strong policy for supporting PDAs and phones starts with an initial set of steps to gain control over a rapidly changing consumer oriented technology. First, we recommend moving all PDAs and phones into the PC support group. This act recognizes that these devices are simply different forms of client-access devices for which the policies should be similar, if not identical. Phones that are now procured in the network department with mobile contracts will the most significantly affected. PC groups should provide three levels of support: 1) Fully supported standard device, a device that will receive all the support privileges of PCs, including application development support; 2) data-interface support only, a device that can be connected to enterprise information sources to retrieve information through controlled ports but for which no application or development support is provided; and 3) nonsupported device, namely a device that appears in such low volume or is so consumer-oriented that the PC group cannot provide support. The key to this strategy is level 2. By compromising on access, the IS organization can implement the first and third options. "PDA firewalls" are enterprise-controlled gateways through which all information destined to employee devices not owned by the enterprise must flow to assist in ensuring some level of data protection. The "Cafeteria Plan" is documented in research ("The 'Cafeteria Plan' for Mapping Mobile Devices to Users," July 2002), and provides a mechanism for controlling device acquisition costs. Specialized mobile tools are required to deal with the special issues of the mobile environment.

Strategic Planning Assumptions: By YE04, PDA security options will equal notebook security (0.6 probability). By YE05, smart-phone security options will equal notebook security (0.6 probability).

A Security Framework for Devices

- Device
  - Encryption
  - Authentication
    - Biometrics with back door
  - Hierarchical storage
  - Virus protection
  - Remote destruct
- Network
  - Encryption
    - WLAN (TKIP), WWAN (Default)
  - Authentication
    - WLAN/WWAN (802.1x)

Gartner

Securing PDAs and phones are serious challenges facing enterprises. These devices, originally targeting consumers, were never secure. Today some devices supplied by enterprise-class vendors are being retrofitted to meet the needs of security-conscious organizations. Equivalency to notebook computers will take several years, but it will be addressed by developing technology to defend against attacks against the device and to enterprise infrastructure via network access from the device. Secure access to the network or device requires encryption and authentication technologies. There is sufficient processing power to encrypt all information on the device, leaving authentication as the major challenge. On the device, secure mechanisms are available via password, but will be replaced by optional methods, including fingerprint recognition. HP's 5400 fingerprint reader is especially notable, because it works reliably (Note: HP needs to improve some of the software and provide for network authentication and back-door access options). Virus protection is available as well as network-based means of disabling the device. Hierarchical storage (offloading less-used information to lessen threats) is available, but in early stages of deployment. Networks follow the same trends, with the most significant improvements in WLANs.

Action Item: Enterprises should gauge security concerns and deploy primary or third-party solutions.

Strategic Planning Assumption: In 2003, 70 percent of institutions will designate an information security officer (ISO), either formally by title or informally by responsibility (0.7 probability).

Security and the IT Commons

“Connected" = Behave as "good citizens"

- Recognize and protect the IT commons
  - Educate and inform
    - Establish a social contract based on responsible behaviors
    - Depends on the responsible behavior of everyone who uses it
  - Establish policies that balance user freedom and systems integrity
- The security chain is only as strong as its weakest link

Gartner

IT security requires awareness and education. The social contract governing IT services must recognize that the health of the "IT Commons" depends on users behaving responsibly.

Security concerns will continue to dominate executive discussions in 2003:

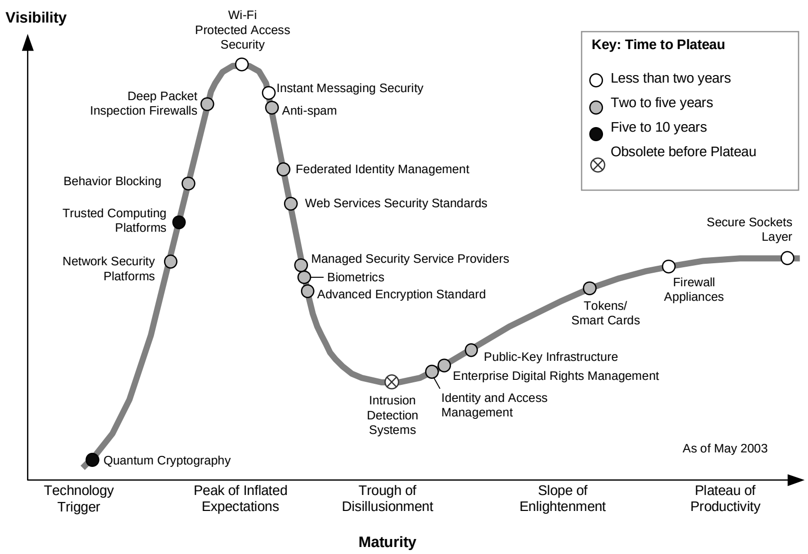
- Reallocations of budgets and staff to meet security needs
- Increased hacking activity, in both directions
- Escalating pressures from state and federal security agencies to secure campus networks and crack down on the illicit use of college networks to launch cyber attacks
- Increased use of outside resources for vulnerability audits and risk assessments
- *Increased impact from national and state security laws (e.g. SEVIS, HIPAA).*

Beyond 2003, institutions should plan to do the following:

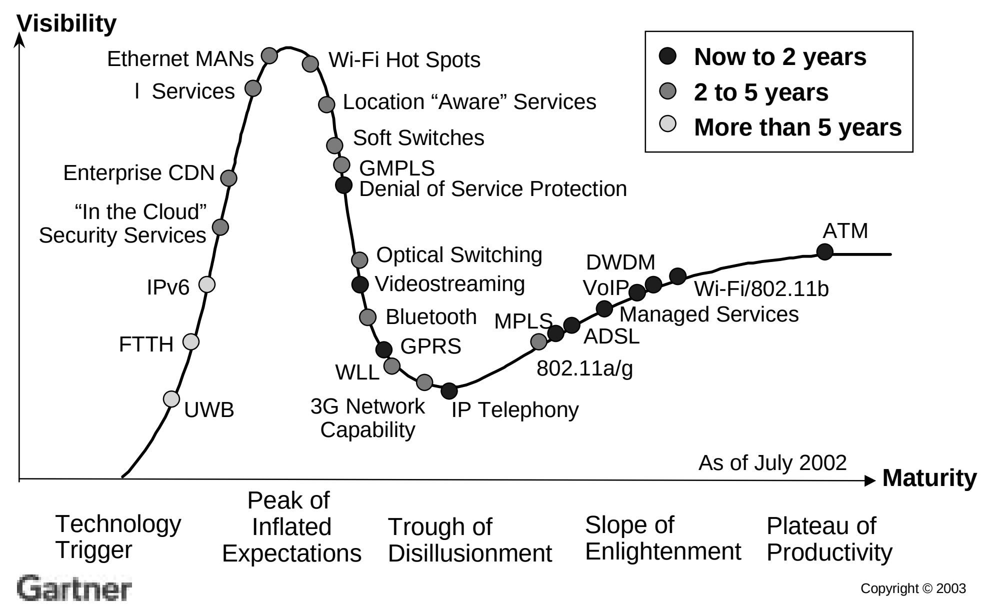
- Build *resilience* by involving business and academic leaders in *Business Continuity Planning*
- Manage risk using real-time, rigorous and continuous risk audits and assessments.
- Build robust directory services (however single sign-on, single directory remains elusive)

Action Item: Institutions must focus on education, training and awareness to build recognition and protection for the IT Commons.

Hype Cycle for Information Security:2003

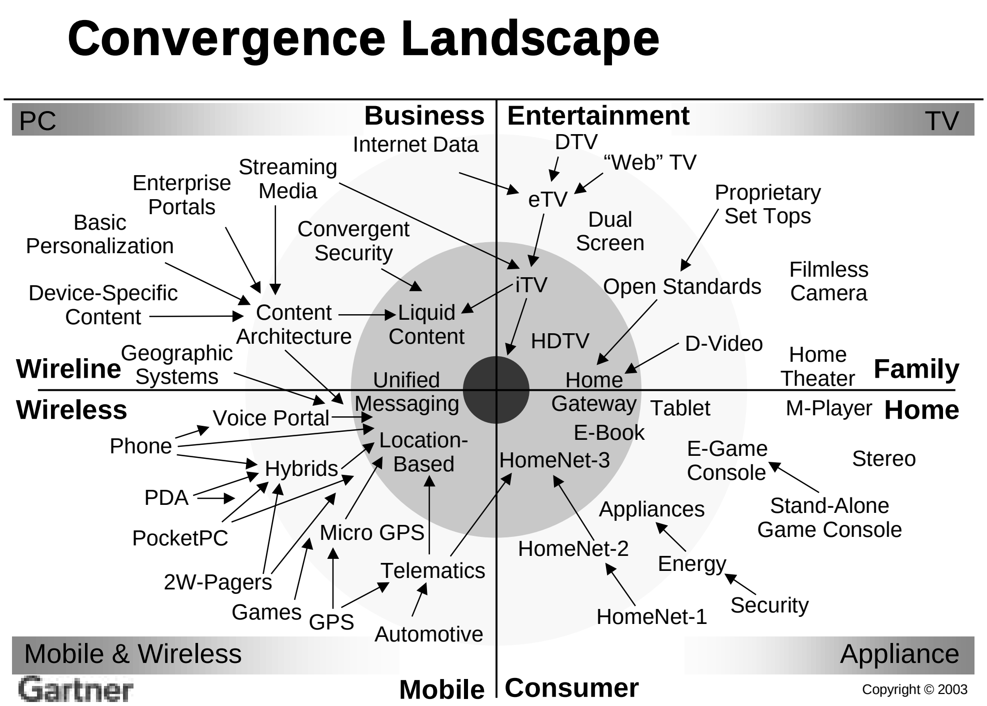


The Convergence Hype Cycle



This convergence Hype Cycle is a subset of the networking Hype Cycle. Included in this Hype Cycle are technologies that will directly or indirectly affect convergence. Technologies that are being used now or on the two-year horizon and require enterprise attention include: 802.11b (wireless LANs up to 11 Mbps), VoIP (the transport of voice as packets over an IP network), managed services, multiprotocol label switching (MPLS) services, telephony applications over IP (IP telephony), wireless general packet radio systems (GPRS), videostreaming and denial of service protection. Technologies that service providers will rely on to deliver enterprise services include: asynchronous transfer mode (ATM), optical dense wave division mulitplexers (DWDM) and asynchronous digital subscriber line (ADSL). Technologies that will be arriving in the next two to five years include: 802.11a/g (wireless LANs up to 55 Mbps), 3G network capability, wireless local links (WLLs), Bluetooth, optical switching, general multiprotocol label switching (GMPLS), soft switches, location "aware" services, Wi-Fi hot spots, Ethernet MANs, I services, enterprise content distribution networks (CDNs) and "in the cloud" security services. Further out, beyond the five-year horizon, technologies include: IPv6, fiber to the home (FTTH) and ultra-wideband (UWB) wireless. *Action Item: Enterprises should focus on short-term technologies but understand how longer-term technologies will impact future network design.*

Market: The convergence landscape will be scattered with successes and failures of enterprises that moved to converge services.



The convergence landscape is driven by the competitive necessity of providing unified (convergent) networks and services to an increasing number of devices, some of which are converging while others are diverging. The convergence landscape is broader and more crowded than most professionals realize. It covers the well-developed PC-Internet sector, the emerging interactive TV sector, the seemingly nascent appliance sector, and the "red hot" mobile and wireless sector. Sectors are expanding and overlapping, new players are emerging, and new opportunities and new threats are everywhere. Some devices are converging; others are specializing and diverging. Networks are converging around increasingly mature IP standards. Services are converging but must be offered to a wider range of access devices. Over time, the rate of change has accelerated, and many enterprises will get caught focusing on only one or two of the sectors, only to find out that three or (all) four were important to maintain competitive advantage.

The important countertrend that must be taken into consideration is that, viewed from the perspective of the CIO, device access is actually diverging, not converging. This places an increasing burden on the enterprise to provide flexible partnerships, planning models and architectures. It also places additional pressure on the need to quickly identify and incorporate emerging technologies to keep up with consumer demand and competitor services.

A Peek over the Horizon

Educause Integrated Communications Strategies Meeting
6 August 2003

Ron Yanosky
Principal Analyst
ron.yanosky@gartner.com

Gartner