

The Pros and Cons of Using NOCs for Wireless E-Mail

Ken Dulaney, Monica Basso, Leif-Olof Wallin

Gartner explains the workings of architectures for enterprise wireless push e-mail. We describe the advantages and shortcomings of those that use network operation centers (NOCs).

Key Findings

- Systems for enterprise wireless push e-mail that connect to mobile handsets' native e-mail applications typically have two main components: a redirector that acts as a proxy for each e-mail account on the user organization's e-mail server and a routing gateway.
- The gateway can be located 1) behind the organization's firewall, 2) in its "demilitarized zone" or 3) in the external wireless network, either as part of a mobile operator's infrastructure or at an independent site run by the vendor of the wireless e-mail system. When at an independent site, the gateway is often called a NOC.
- Many vendors are moving to NOC-based products, in the hope of emulating the success of Research In Motion's architecture. Vendors can charge for a NOC, and buyers think a NOC simplifies the management of their links to operators. But customers' requirements may change if Microsoft succeeds in providing a comparable service without a NOC.

Predictions

- Through to 2007, NOC-based systems will provide the highest-quality service.
- After 2007, the advantages of NOC-based systems will diminish significantly.

Recommendations

- Through to 2007, favor NOC-based wireless e-mail systems if your organization:
- Has workers needing a capable, reliable service during frequent trips abroad. But global enterprises with staff who travel in small countries should check the extent of e-mail roaming.
- Needs a cost-effective way to outsource the job of managing links with mobile operators.
- Uses a non-NOC system but needs a reliable alternative for its most important staff.

If you are worried about the security of NOCs, request a private one that you can manage directly.

TABLE OF CONTENTS

1.0 Introduction: NOCs or Not?	3
1.1 Overview of Enterprise Wireless E-Mail Architecture.....	3
1.1.1 Firewall Ports Used for Connections	5
1.1.2 Ways to Keep Connections Active	6
1.1.3 GPRS Public and Private APNs for Routing Wireless Access.....	6
1.1.4 Push vs. Pull Architectures.....	7
1.1.5 Security Issues of NOC-Based Systems.....	10
2.0 Strengths and Weaknesses of NOC-Based Architecture.....	10
3.0 What the Future Holds.....	12

LIST OF FIGURES

Figure 1. Network Architectures for Enterprise Wireless "Push" E-Mail	4
Figure 2. Vendors' Approaches to Enterprise Wireless E-Mail Architecture, by Position of Routing Gateway.....	5
Figure 3. Research In Motion's BlackBerry Architecture for Enterprise Wireless E-Mail	9

1.0 Introduction: NOCs or Not?

Choosing a wireless e-mail system is a hard task for any organization, as the market for these products is characterized by mergers and acquisitions and rapid technological change. It's made more complex by a basic difference of approach toward the underlying architecture: several vendors, including the leader, use an infrastructure component called a network operations center (NOC); others don't. This document aims to clarify the role and importance of these components. It also discusses the role of public and private access point nodes (APNs) in NOC-based systems and others.

The most successful wireless e-mail architecture is BlackBerry, from Canadian company Research In Motion (RIM). It uses two NOCs: one for the Americas and Asia/Pacific, and one for Europe, the Middle East and Africa. Through these, e-mail traffic is routed worldwide.

Other vendors that offer NOCs are Good Technology, Visto, Seven Networks and Intellisync. Good and Intellisync, like RIM, provide IT-based systems. Visto and Seven offer operator-based systems not normally requested by Gartner's clients.

Vendors of NOC-based systems claim their architecture has many benefits for customers. These include better performance for push e-mail, longer battery life for mobile devices and increased security. They also point out that this kind of setup lets customers outsource the management of relationships with mobile operators.

Microsoft is in the other camp. Service Pack 2 (SP2) for its Exchange Server 2003 software promises to deliver an equivalent system without a NOC. Microsoft has three main aims here: to lower customers' organizational costs by eliminating servers that redirect messages from their native e-mail systems to the mobile Internet; to cut customers' monthly costs by doing away with charges for NOCs; and to let organizations negotiate contracts for wireless data rates independent of the supplier of wireless e-mail technology. By contrast, RIM's customers have to install a separate server and pay a special higher rate for data services each month, one that includes a payment to RIM for the NOC.

1.1 Overview of Enterprise Wireless E-Mail Architecture

- Push-based architectures for enterprise wireless e-mail that deliver messages and information to the applications that come with many mobile handsets typically have at least two main components: a redirector and a routing gateway.
- The redirector acts as a proxy for each e-mail account on the user organization's e-mail server. It must be located behind that organization's firewall, in order to work securely with the corporate e-mail server (see "Don't Be Paranoid About Wireless E-Mail Security").
- The routing gateway establishes, maintains and secures connections between the redirector and the mobile devices. It can be in one of three places, depending on the vendor's approach: 1) behind the user organization's firewall; 2) in the "demilitarized zone" between the organization's internal network and the Internet; or 3) in the external wireless network, either as part of a mobile operator's infrastructure, or, as a NOC, at an independent site run by the vendor of the wireless e-mail system.

Figure 1 shows the typical routing of e-mails for each position of gateway.

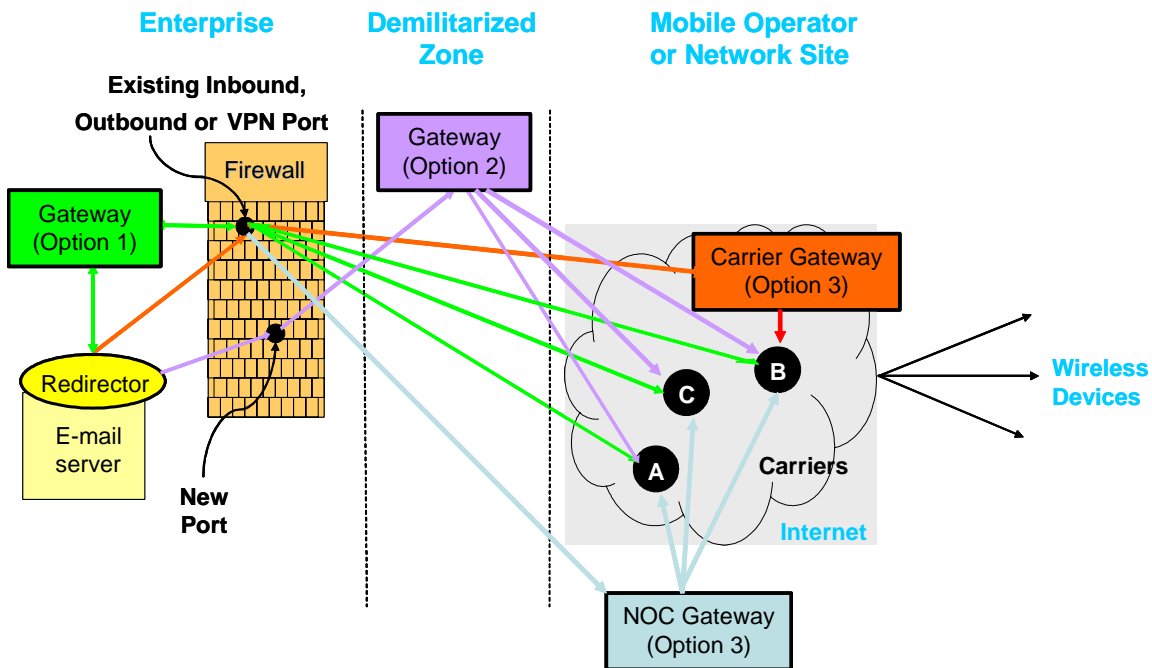
Option 1 generally involves a virtual private network (VPN) connection to each mobile operator that provides e-mail service. Responsibility for managing these connections lies with the customer.

Option 2 also requires separate connections to each mobile operator, but typically establishes them using a proprietary tunneling scheme. Also, e-mails reach the enterprise through a different port, which must be opened if other applications don't already use it.

Option 3, using a NOC, connects to the enterprise through a VPN port via a proprietary Internet tunnel, and to mobile networks or the Internet via the NOC. The NOC can connect to multiple mobile operators — and so provide flexible network connectivity — using a variety of secure methods.

For Option 3 gateways hosted at the mobile operator, the connection to the enterprise is made similarly, but there is only a connection to the hosting mobile operator. Consequently, enterprises cannot route e-mail to other operators.

Figure 1. Network Architectures for Enterprise Wireless "Push" E-Mail



Source: Gartner (November 2005)

Figure 2 shows the options offered by leading vendors.

Extended Systems, which is now owned by Sybase, and Intellisync offer Options 1 and 2 (see below for Intellisync's Option 3 offerings).

Microsoft, with its Exchange Server software, uses a modified form of Option 1 with neither redirector nor gateway. It also supports Option 2 for clients that have front-end servers in the demilitarized zone, but doesn't recommend this option for new installations.

Intellisync, Good Technology and RIM offer Option 3, with the redirector behind the customer's firewall and the routing gateway (NOC) at an independent location. Intellisync can also position a gateway at a mobile operator's site.

Vendors such as Seven Networks and Visto that provide "white label" — that is, unbranded — systems to mobile operators also offer Option 3, placing the gateway in the mobile operator's facilities (they offer Option 1 in some cases, too). Seven and Visto are included here for completeness, but are not discussed further because they do not sell directly to enterprises.

Mobile operators that deliver wireless e-mail from ISPs via POP3 or IMAP systems use a modified form of Option 3. This approach has no need of a redirector, as the e-mail system is built and controlled by the carrier.

Figure 2. Vendors' Approaches to Enterprise Wireless E-Mail Architecture, by Position of Routing Gateway

Wireless E-Mail Provider	Option 1 (Behind Firewall)	Option 2 (Demilitarized Zone)	Option 3 (Mobile Operator)	
			Operator-Located	NOC-Located
Extended Systems (Sybase)	✓	✓		
Good Technology				✓
Intellisync	✓	✓	✓	✓
Microsoft	✓ (No redirector required)	✓ (No redirector required)		
Notify Technology		✓		
OpenHand	✓			
Research in Motion				✓
Seven Networks			✓	
Visto			✓	

Note: Colors correspond to those of Figure 1

Source: Gartner (November 2005)

1.1.1 Firewall Ports Used for Connections

In each architecture, outbound e-mail normally uses the customer's VPN port. This avoids the need to open other ports — something many organizations prefer to avoid for reasons of security.

Some vendors do open a new port for outgoing e-mail. But, more often, they open one just as a notification channel, through which they send Short Message Service (SMS) messages telling mobile devices to reconnect to the e-mail server. But even this practice is being abandoned, as it's unreliable, drains batteries when messages are not downloaded for long periods, and can be expensive.

RIM's BlackBerry architecture uses firewall port 3101 when integrating with Microsoft Exchange Server 2003 software located in the demilitarized zone. Some organizations associated with the U.K. government are worried about this, but it shouldn't be a major issue for most enterprises, since opening a firewall port for a server's outgoing traffic is standard procedure. Organizations with very strict security requirements should opt for a private leased line, or a private frame relay or Internet Protocol/Multiprotocol Label Switching (IP/MPLS) connection, to connect to the NOC.

For inbound traffic, the VPN port is avoided. This reduces the chance of an external entity breaching security by connecting to a VPN concentrator using credentials supplied to the software provider. Instead, vendors use their own proprietary protocols, often employing User Datagram Protocol (UDP) or Secure Sockets Layer (SSL) technology.

High-level encryption, generally using the Triple Data Encryption Standard (3DES) or the Advanced Encryption Standard (AES), is the norm for traffic traveling in either direction.

1.1.2 Ways to Keep Connections Active

In today's wireless e-mail architectures, routing gateways have to work to keep in touch with mobile devices. That's because e-mail can only be "pushed" to these devices when there's a stable IP connection between them and the e-mail server — and that's not always the case.

With version 4 of the Internet Protocol (IPv4) — the basis of the modern Internet — mobile devices can always find the e-mail server, because it rarely moves and has a stable entry in the Internet's Domain Name System (DNS). But the pool of IP addresses is far smaller than the vast number of devices that require them, and this forces operators to avoid using static IP addresses for mobile devices. This, in turn, means that the server sometimes loses contact with these devices: their IP addresses often change when they enter a new area of network coverage or a mobile operator assigns them new ones.

There are two main ways of tackling this problem.

In some systems the gateway sends out SMS messages telling the recipient mobile devices to wake up and connect to the e-mail server. But, as noted earlier, this method is being abandoned.

The second approach, known as the "heartbeat" method, has mobile devices stay connected to the e-mail server by sending it small packets of IP data over cellular links. The rate at which these are sent can be fixed or adapted to suit specific networks and combinations of devices. (Networks with small pools of IP addresses reuse them more often than those with large ones, so the pattern of timeout and reuse varies from minutes to days.) The reverse process, whereby the server sends packets to the devices, can also be used. Products from Good Technology, Microsoft and some other vendors enable ping rates to be configured dynamically. This boosts efficiency by tuning the rate to the operator's timeout pattern: a ping occurs just before the operator takes away the address.

Microsoft recommends that firewall timeouts be set to 30 minutes for its non-NOC system. But this may increase an organization's security exposure, so Gartner doesn't recommend changing this setting. Organizations that use Microsoft's system but leave the setting below 30 minutes because of network address timeouts may suffer occasional delays in delivering e-mail — a disadvantage of Microsoft's approach.

1.1.3 GPRS Public and Private APNs for Routing Wireless Access

Note: Code division multiple access (CDMA) technology takes a different approach from general packet radio service (GPRS) and is not discussed here.

With GPRS cellular technology, each wireless device connects to the mobile network through a serving GPRS support node (SGSN) — a type of router located at the mobile operator's facilities. The SGSN communicates with a gateway GPRS support node (GGSN) — an external router — at which point the wireless device receives a network IP address via a Dynamic Host Configuration Protocol (DHCP) server.

The services a device can receive are provided through a logical connection called an access point node (APN). There are public APNs that provide public services such as Internet access and private APNs that provide private access over a secure link to an external entity.

Every mobile operator provides a public APN with access to the Internet. The public APN method works for push e-mail on the user's home network and for any operator with a GPRS Roaming Exchange (GRX) agreement with the user's home operator. The wireless e-mail gateway vendor secures the link from either the NOC (if there is one) or the gateway behind the firewall to the wireless device using a proprietary tunneling mechanism.

RIM's BlackBerry architecture works differently. Once a handset has been assigned a public address as just described, the handset seeks RIM's private APN by connecting to RIM's blackberry.net Internet site. Communication then passes through a GGSN over a secure link to RIM's NOC (where the private APN is "exposed"). At the NOC, RIM maintains tables that constantly map the operator's IP addresses to the device's embedded personal identification number (PIN). This use of a private APN requires the cooperation of mobile operators. Hence, each SIM card has to be prepared for use with BlackBerry: one cannot simply put a SIM card that accepts IP services into a mobile phone and expect to receive push e-mail from RIM.

A private APN confers all the benefits — among them security and control — of connecting users directly to an organization's internal network, without having to extend a VPN to a mobile operator. Consequently, there isn't the problem of running VPN protocols over GPRS technology — something they're not suited to. What's more, with private APNs, mobile devices need no special software to secure the link between themselves and the server. This reduces the performance requirements for those devices. Finally, RIM's constant knowledge of handsets' IP addresses means it can fine-tune the delivery of e-mail.

Overall, a system that uses private APNs is more efficient than one that uses public APNs, which results in benefits for battery life and data usage. But the gains may prove slight. (It's hard to obtain performance comparisons, but users of both types of system generally report acceptable performance.)

1.1.4 Push vs. Pull Architectures

For Gartner, three things distinguish push technology from other e-mail synchronization methods:

- Users need not monitor their wireless coverage.
- Data can be sent through a continuously open channel between source and destination.
- The recipient need not manage the delivery of information.

Vendors' common use of the word "push" in relation to technology that synchronizes wireless e-mail client software with e-mail servers disguises at least four different mechanisms, which correspond to different architectures. Not all of them are genuinely "push" in nature.

BlackBerry push. Only RIM uses this mechanism. It uses a NOC and private APNs — one for each operator — directly connected to mobile networks. RIM can adapt its service-level agreements (SLAs) to suit the characteristics of different operators.

Figure 3 shows how this mechanism works. Each mobile handset connects to its home NOC down one of three paths (see Figure 3):

1. Traffic from handsets operating on the user's home mobile network — which must have a direct connection to RIM's NOC and support a private APN — passes over that network and then through a leased line to the NOC, to which it's then exposed. It then

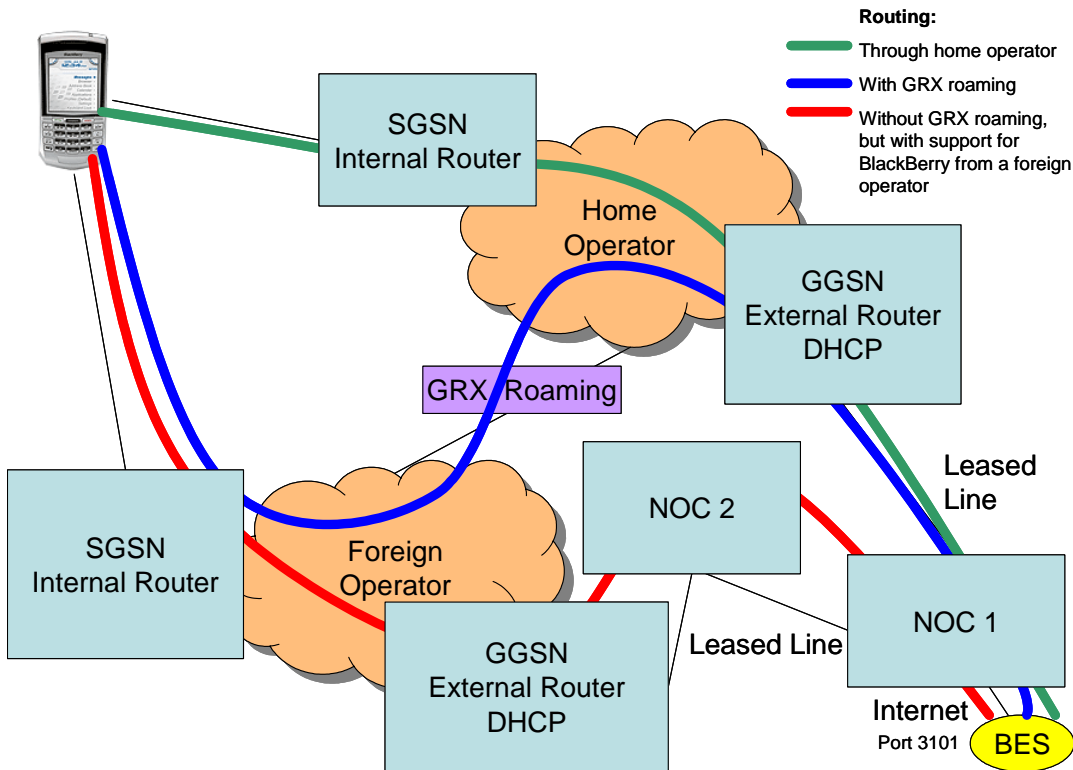
moves on from the NOC, over a secure Internet connection, to the BlackBerry Enterprise Server (BES) at the customer's premises. This path is shown by the green line (top).

2. When a handset roams on to a mobile network belonging to a foreign operator that has a GRX agreement with the home operator, the route is similar but passes through both of them. This path is shown by the blue line (middle).
3. If a user roams on to the network of an operator that lacks a GRX roaming agreement with his or her home operator but that has an agreement with RIM to support its NOC and private APN, traffic follows the path shown in red (bottom). Two NOCs are involved only if the foreign operator is geographically distant and its NOC differs from the one supported by the home operator. Roaming users cannot connect in situations where there is no GRX roaming agreement and no relationship between RIM and the foreign operator.

However, as mentioned earlier, if a mobile device's SIM card is not set up to connect to RIM's private APN — as would be the case when someone buys a SIM card abroad for temporary use — push e-mail is not possible. Also, even when using a properly provisioned SIM card, if the user's home operator doesn't have a GRX roaming agreement with the foreign operator, and that foreign operator lacks a private APN link to RIM, push e-mail won't work.

Organizations buying a RIM system have to purchase it from a mobile operator — generally their main carrier. RIM places no constraints on connecting mobile devices to other operators that support BlackBerry, but moving BlackBerry handsets to other carriers can still be a problem, as some operators lock them for use only on their network.

Figure 3. Research In Motion's BlackBerry Architecture for Enterprise Wireless E-Mail



BES = BlackBerry Enterprise Server
 DHCP = Dynamic Host Configuration Protocol
 GGSN = gateway GPRS support node
 GPRS = general packet radio service
 GRX = GPRS Roaming Exchange
 NOC = network operations center
 SGSN = serving GPRS support node

Source: Gartner (November 2005)

IP push. This is the mechanism used by Good Technology, Intellisync, Visto and Seven Networks, among others. Their architecture may or may not have a NOC and uses public or private APNs. The systems of Visto and Seven are tied to individual mobile operators; the other vendors' architectures have no specific ties to operators.

Vendors that use public APNs in this way can support almost any mobile operator, since all they require is Internet access from the home operator or a foreign one. Consequently, these vendors often support more operators than RIM does. In the case of Good, though, the increase is reduced slightly by the company's requirement that its NOC understand the address timeout parameters of operators.

Direct push. This is Microsoft's approach with SP2 for Exchange Server 2003. There is no NOC and the APNs are public, which means customers can use a standard data plan from any mobile operator. This method is merely "push-like" — it's better defined as notification-based synchronization — and works as follows.

A wireless device sends an HTTP request to the Exchange Server software, to alert the server to its availability and ask about changes to the in-box (e-mail, calendar, contacts and tasks). On receiving this request, the Exchange Server checks the in-box and immediately notifies the

device when changes occur. The device then issues a synchronization request to retrieve the changes. This communication loop maintains an open connection between device and server.

Microsoft's approach builds "intelligence" into both the wireless device and the Exchange Server software to allow for the maximum time between update packets (known as the "heartbeat interval") required to keep the connection alive. This interval is reconfigured automatically as the device moves from one area of network coverage to another and as network conditions change.

IP pull. Extended Systems uses this mechanism. It's also an option offered by Intellisync in its enterprise solutions (this vendor's carrier-based solutions work differently). There is no NOC, and public APNs are used. The wireless handset initiates all communication sessions upon notification by any of several means, such as the receipt of an SMS message. Whenever the handset is involved, more battery power is generally used, but the amount varies and may be insignificant.

1.1.5 Security Issues of NOC-Based Systems

The ideal security system for wireless e-mail is one in which messages are "pushed" from the home server to wireless devices only when they are active and ready to receive them. But because wireless network connectivity is naturally intermittent, temporary storage is often unavoidable. Systems, such as Microsoft's, that don't use NOCs are often thought the most secure, but NOC-based systems that encrypt messages can offer equal security.

That said, NOC-based architectures do raise some security concerns.

Firstly, in certain implementations — such as those of RIM and Good — the NOC sometimes stores e-mail temporarily, when mobile devices are out of its range. Even so, when the encryption keys are known only to the mobile devices and the e-mail server, the risk to security is low, as e-mails stored temporarily at NOCs are hard to decrypt in the time available. Therefore, for many organizations, this approach shouldn't be a worry — provided they trust the NOC's supplier. E-mails decrypted at the NOC and then re-encrypted for their onward journey could present a bigger risk, but this approach is now uncommon.

Secondly, if a NOC's security is breached, any undetected hostile traffic entering the NOC has full access to the mobile gateway, and from there to the e-mail gateway. This would be especially dangerous if the mobile gateway has full administrative access rights to the enterprise's e-mail server — as is the case, for example, with RIM's BES when connected to Microsoft's Exchange Server. Organizations should therefore avoid this type of arrangement, unless they completely trust the provider of the NOC.

Thirdly, the location of NOCs can be an issue. Some may be outside the customer's home country, which could be a problem, especially for organizations that have to observe compliance policies and regulations for IT security. Some enterprises in the U.K., France, Germany and the Netherlands have chosen not to use NOC-based systems because their e-mail would be stored temporarily abroad and so would sometimes be beyond their control. A possible solution here is to ask the e-mail system vendor to deploy a private NOC under the customer's control. Some enterprises have persuaded major vendors to do just that, but the cost is often very high.

2.0 Strengths and Weaknesses of NOC-Based Architecture

All the vendors named in this document offer competent products, but there are trade-offs in areas such as security, battery life, performance and reliability. These differences are often slight, but it's still important for customers to know about them, so that they can choose the most suitable system.

For user organizations, the main advantages of NOC-based architecture are that it:

- *Lets them offload responsibility for managing connections with mobile operators.* Also, with a NOC, it's easier for them to use a variety of operators or move to new ones without changing wireless e-mail technology.
- *Can improve security.* Earlier we discussed some potential security weaknesses of NOC-based architecture, but in many situations a NOC can actually improve security. This kind of architecture doesn't require organizations to open inbound ports in their firewalls — something many are reluctant to do for fear of external attack. All communications to the NOC are made using either an outbound port in the firewall or a private line (often a leased line, frame relay or IP/MPLS connection). That said, this advantage may not be significant. In Microsoft's architecture, ports may have been opened for Outlook Web Access, in which case there is no new security risk.
- *Provides an alternative way for staff to communicate if the home telecom system fails in, say, a natural disaster or a terrorist attack.* RIM's BlackBerry PIN messaging system was used extensively in New York during the terrorist attacks of September 11, when cellular networks went down. However, concerns have been raised about the lack of message tracking in such peer-to-peer systems, and RIM's PIN messaging doesn't work well between Europe and the U.S.
- *Offers flexible transferability.* Moving users between networks may be simpler because the enterprise doesn't have to set up physical links to mobile operators.

For user organizations, the main drawbacks of NOC-based architecture are:

- *Security concerns* (see earlier).
- *Potentially higher costs*, because of service charges covering the cost of the NOC and additional infrastructure that sits outside the enterprise's e-mail server.
- *Limited availability of service and cost of roaming, in some cases.* NOCs that use private APN services require the establishment of a direct relationship with each mobile operator. Thus, RIM's customers have to buy services from a local mobile operator that is a partner of RIM. If there is no such partner locally, they have to buy from a foreign operator and incur hefty charges for international data roaming. Also, when roaming on networks run by operators that aren't partners of the home wireless e-mail operator and that don't have agreements with RIM, the user has no wireless e-mail service at all. Some implementations — such as Good's — do not suffer from this problem, as, by using public APNs to access the Internet, they are independent of mobile operators.
- *Greater potential for unreliability.* To deliver a good service, all connections between the gateway, the NOC and the mobile network must be working. If any of these links, or the NOC itself, fails, then the e-mail service suffers major disruption. This risk can be mitigated by adding redundant equipment and placing multiple NOCs in disparate locations, but it remains more complex than the approach in which enterprise, mobile operator and wireless device are connected by the basic Internet.

For vendors of wireless e-mail systems and mobile operators, NOC-based architecture can improve their chances of retaining customers, because:

- *Direct connections between NOCs and mobile networks enable vendors to offer better SLAs than those that don't use NOCs.* With "heartbeat" signaling, a NOC can closely monitor all user access and collect data to optimize the rate at which data packets are transmitted when keeping in touch with mobile devices. Also, with NOC-based systems,

the transmission of data over mobile networks tends to be highly efficient, so reducing the number of packets and bytes sent, compared with most non-NOC architectures.

- *Tight integration confers more control over wireless devices*, including individual identities — each RIM BlackBerry handset, for instance, has its own PIN. In addition, messages are delivered promptly, as the NOC sees and addresses each device with low latency.
- *NOC systems confer, in certain respects, more control over customers*. Some RIM users, for example, are not given open access to the Internet. Suppliers can even limit customers' ability to switch to rival products.

3.0 What the Future Holds

Heartened by RIM's success, many vendors in the field of enterprise wireless e-mail systems are moving to a NOC-based approach. Intellisync, for example, now offers NOCs in various product offerings. Others, such as Visto and Seven, have always sold NOC-based offerings — though, unlike RIM, they use public APNs.

Microsoft, though, still thinks NOCs are unnecessary. If it can prove its case and produce a system that works as well as the others, customers' views about the desirability of NOCs may change.

- Gartner believes that, until the end of 2007, NOC-based offerings will offer the most value for organizations needing the highest quality of wireless e-mail service. But there are reasons for thinking that the advantages of NOC-based architecture will diminish after 2007:
- Wireless devices are getting more "intelligent." As such, e-mail servers will have less trouble communicating with them when IP addresses change.
- Cellular networks are the only wireless networks that need NOCs. IP-based networks like Wi-Fi, WiMAX and fourth-generation mobile networks won't. And, as more networks and multimode devices appear, the number of situations in which it's desirable to use a NOC may fall.
- As mobile operators offer better data-roaming arrangements and give handsets freer access to the Internet, the need for a separate NOC architecture for wireless e-mail will lessen.
- "Pull" e-mail systems that don't require constant synchronization between mobile devices and e-mail servers may become more widely accepted, eliminating the need for push delivery. These systems will attract buyers because they will be marketed as "push," and it won't be obvious that they are slightly less efficient.
- IPv6 could dramatically change the way wireless services are delivered, by making all systems directly addressable at fixed addresses. But it's almost certain that IPv6 won't be in widespread use within the next five years.
- Emerging push e-mail standards from the Internet Engineering Taskforce (IETF) could reduce the need for proprietary architectures. But this is unlikely in the next five years.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509