Position Paper

Strategic Networking Imperatives for the Real-Time Enterprise

New business realities bring profound implications for network and information management strategies. IT executives have had to reassess the way they build, manage, and use the IT infrastructure. Under constant pressure to do more with less, they have to constantly push for more competitive and proactive information management models.

The networking technology advances of the last decade -- particularly optical, Ethernet and IP networking, and broadband wireless -- have fundamentally reshaped business environments in ways that are simultaneously advantageous and detrimental. In a business climate that is more punishing than ever to the inefficient and the slow-moving, businesses are under pressure to manage their information assets more effectively, efficiently, and wisely.

The IT infrastructure is no longer an adjunct support structure; it is the essential foundation for enterprise performance. How information is obtained, validated, stored, accessed, distributed, and how real-time collaboration is realized across an increasingly virtualized organization ... these issues are central to organizational survival and profitability. The role of the CIO has clearly transitioned from managing a cost center to a strategic partner in the business at the cabinet table, recognizing the importance of the IT infrastructure has on business operations, workflow and relationship with customers.

Can the IT infrastructure be leveraged to make employees more productive? Can it be leveraged to create new revenue opportunities and help create stronger engagement with customers? Can IT revolutionize the very nature of how business is done? How customer contacts take place? How information about suppliers and customers is shared and used?

Nortel says yes. The three business realities identified in this paper drive the definition of three networking strategic imperatives for IT, which support the delivery of these values. Partnering with Nortel can position the enterprise to win.

Business Realities Facing IT

Business Reality #1: *The rules of the game have changed: Meeting regulatory compliance and security requirements are table stakes.*

There was a time when the business world operated like a Monopoly game -- Stay on a predictable path that marches around the board, deal with the cards as they fall, grow as big as possible. Do this, and you are virtually assured of accumulating wealth. Those old rules have changed. Today's business game is more like the reality TV show "Survivor," where success rests on the ability to forge close alliances and constantly adapt to new challenges. In August 2003, viruses, along with overt and covert hacker attacks, caused $32.8 billion in economic damages, according to a report from mi2g, a digital risk assessment company based in London. mi2g also notes that the "Sobig" virus alone accounted for $29.7 billion of economic damages worldwide.

Security breaches, and resulting loss of productivity and access to confidential data, is costing enterprises millions of dollars, but the security imperative goes beyond these financial incentives. Government regulations are placing additional requirements on enterprises. Examples include the Sarbanes Oxley Act on corporate governance and the US Patriot Act; industry specific regulations such as the Gramm-Leach-Bliley Act for the financial industry and the Health Insurance Portability and Accountability Act (HIPAA); and security-related regulations

outside of the US such as the Data Protection Directive in the EU. These have wide-ranging impacts on security, including requirements for encryption, disaster recovery and business continuity, archiving and consumer privacy. Failure to comply with these regulations can bring civil and criminal penalties.

Regulations at all levels, accelerating security attacks and vulnerable networks -- no wonder IT executives are putting security and disaster recovery at the top of their investment priorities.

IOS vulnerabilities already out there or yet to be discovered present a major challenge to network administrators and security professionals. It is increasingly difficult not only to plug the operating system's security holes. Patching IOS requires replacing each IOS version with an updated version, then rebooting the system and making sure that the improved IOS doesn't interfere with network cards or other network devices plugged into the router or switch. "To fix it, you have to put a whole new image on a device and restart it," said John Pescatore, VP for Internet security at IT advisory firm Gartner. [1]

Business Reality #2: *Time to X is the key metric: Reducing time to decision, time to service and time to revenues is the path to the real-time enterprise*

Speed to market is critical in their industry. This has as much to do with business processes and the ability to access business information in a timely fashion, as it has to do with providing increasingly distributed employees with the collaborative tools, starting with business-grade telephony, to work more effectively across the virtual enterprise. Jack Welch, the legendary CEO of GE, has been quoted as saying "An organization's ability to learn, and translate that learning into action rapidly, is the ultimate competitive business advantage."

What is impeding enterprises as they attempt to increase their real-time communications effectiveness? Knowledge workers and others with the need to communicate and/or collaborate are faced with a number of pain points including:

- Losing productivity when away from the office (the lack of geographic flexibility).
- Using disparate systems (e.g. telephones, room video conferencing, email, Instant Messaging, file servers) to communicate across teams.
- Managing multiple contact numbers and inboxes (the lack of service ubiquity).

In addition, many enterprises see regulatory and security liabilities arising from employees using public communications services, especially Instant Messaging, email and other Internet-centric services.

On the customer side, the impacts can be even more dramatic. Now that customers can leap to the competition with the click of a mouse, organizations need to manage the intrinsic value in relationships -- looking at the full dynamics of interactions with customers. That requires a technology infrastructure that supports a unified, relationship-based view of customers, spanning all touch points and systems.

The technology reality is that virtually all vendors and most enterprises are adopting IP Telephony as the foundation to address real-time collaboration and mobility requirements of enterprises, business continuity and to enhance customer engagement through virtualization and enrichment of contact centers. Nortel's view is that IP Telephony is a key enabler of what it refers to as "real-time converged communications" (aka Unified Communications by the Gartner Group, and more generally multimedia communications), made up of voice, Instant Messaging, video and application sharing, conferencing, combined with presence and ultimately location intelligence. While each of these modalities can be deployed on a one-of basis, converged communications brings these together and provides a seamless user experience across all these media. These capabilities come together to enable the real-time enterprise and result in dramatically more effective collaboration with resulting shortened time to decision. They provide the ability to enable engaged applications to further productivity and to enhance the enterprise customer experience. They allow the organization to engage the right resources to

[1] "Next Big Target" by Larry Greenemeier, Information Week, November 7, 2005

address the opportunity at hand, whether these are in the office or out of the office, on the local area network or wide area network, connected over wireless or wireline connections or using voice or data communications.

Gartner Group (February 2005) positioned Nortel a leading player in their Magic Quadrant analysis, high on ability to execute and high on vision in the Unified Communications market. At the same time, Gartner Group positioned Cisco as a niche player, low on ability to execute and low on vision in the Unified Communications market.

Nortel proof points:

- *Nortel itself has deployed 20000 SIP multimedia clients across its highly distributed and mobile work force.*
- *A 100-person investment bank is first to deploy SIP and real-time converged communications across the entire company.*
- *A financial stock exchange has deployed a high capacity pico-cell wireless LAN to provide reliable mobility across its trading floor.*

Gartner in its Cisco IP Telephony Update (April 2004) said that "The trust Cisco has built up in data networking has given companies a false sense of security in relation to its voice business. Cisco has also been party to some high profile failures" citing a state government (400,000 end points), a city government (8500 end points) and a financial institution (7500 end points).

Business Reality #3: *You have to do more with less: Too much money and resources on day-to-day operation!*

CIOs face several difficult challenges in this regard. Security threats continue to grow in sophistication and intensity. Enterprise traffic continues to grow from increased use and from new enterprise-wide applications.

IT staff are already stretched to the limits with the daily tasks of managing, upgrading and engineering their networking and computing environments, and yet are expected to address new opportunities whether in the form of new customer service initiatives or mobility. Meanwhile it's not getting any easier to find, hire, train, and retain skilled staff to run these complex IT environments.

If you keep doing the same thing, you'll keep getting the same results. It's an old adage, but still true. If the present enterprise network architecture is expensive to manage, troublesome to maintain, short on bandwidth, and inflexible to growth and change, deploying more of the same equipment or adding additional features and functions isn't going to solve the problem. If the network grows in 'intelligence' and the expense of performance, IT headaches only turn into migraines.

This reality has two components: capex and opex. Replacing network switches and routers that can't do the job may be a necessity, but paying high premiums due to procurement policies or vendor lock-in just serves to exacerbate the budgetary crunch. Opex is heavily driven by device complexity, and for those running IOS this can be a serious drain on resources. Opex is also driven by network complexity, caused by moving network intelligence out to every wiring closet or even wireless LAN access point.

"IOS has become large, monolithic, and bloated with features and functions," said Forrester Research analyst Robert Whiteley. "It is increasingly difficult ... to get customers to update to the newest versions. The customer heel-dragging is caused by IOS complexity and by the work involved in upgrading."[2]

"Cisco charges up to 70% more than rivals…Some customers are sick of getting squeezed like that" *Business Week Online, February 2003*

Strategic IT Networking Imperatives

Many enterprises have to face the fact that the networks they have deployed do not and often cannot deliver the security, reliability, short delays and lossless operation required by real-time converged communications. For example, loss of voice can result in

[2] "Next Big Target" by Larry Greenemeier, Information Week, November 7, 2005

incoherent speech, while excessive delays introduce intolerable echoes and unnatural pauses in human interaction, making interruptions awkward and positive responses appear hesitant. Confidentiality of voice conversations is another sensitive area; clearly safeguards must be deployed to guard against eavesdropping from desktop PCs. Protecting voice and multimedia communications also means making firewalls aware of related signaling protocols. There are other dimensions to this challenge ranging from power over Ethernet, to quality of service, resilient designs and proper bandwidth engineering. Not having proper technologies in place or not engineering the networks to support voice and multimedia can impact employee productivity as well as customer service.

The following three networking strategic imperatives are offered as the response to these challenges.

Strategic Imperative #1: *Think Layered Defense for business continuity*

The layered defense approach ensures that there are no single points of security failure in a network. This is accomplished by using multiple approaches to security enforcement and reliability in different parts of the network. Layered defense approach is also bolstered by leveraging systems that utilize security capabilities and products from best-of-breed security vendors. Platform security ensures that all networking and network-attached platforms are hardened across the management, media and control planes. In addition to platform security there are four other important elements to a Layered Defense approach to security and business continuity.

The goal of Endpoint security is to ensure valid user identity, and device security policy compliance (e.g. most recent anti-virus software). Endpoint security is applied across wired and wireless endpoints within the network as well as those at remote sites, where there is less control over the users' devices. Perimeter security, the second key element of Layered Defense, is applied to control traffic traveling between zones of trust, and can be applied at internal perimeters, at the external edge of the network (the DMZ), around data centers, around secure multimedia zones to protect multimedia and IP Telephony call servers, and even around a single critical user. Keeping watch for malicious software and traffic anomalies, enforcing network policy, and enabling survivability is the role of Core network security in a Layered Defense approach. Continually monitoring the network for malicious activity is key to ensuring that if an attack slips through other layers of security that a network will detect it and take appropriate action to block the attack and ensure survivability. Time to isolate the effects of security attacks is a key parameter to minimize the business and reliability impacts of attacks. Secure Communications (focused on Multimedia) is the final element of layered defense. This protects corporate and customer information from unauthorized discovery, eavesdropping or misappropriation, while stored or in transit across networks, using technologies such as IPSec, Secure Sockets Layer (SSL), Secure RTP (SRTP) and Transport Layer Security (TLS). The direction is that these will increasingly work in a closed loop fashion (configure, monitor, detect, adjust) leading to autonomic controls that are managed with business policies.

IP Telephony enables the deployment of robust disaster recovery and business continuity solutions for telephony, much the way SAN extensions have provided this for data. In fact, Nortel has lead the market with its business continuity and disaster recovery Storage Area Network extension solutions, developed and certified with its partners such as EMC, HP, IBM and Sun. Nortel now offers industry-leading active-active back-up solutions for its IP Telephony systems allowing one provincial government to deploy a centralized IP Telephony system operated out of two data centers, for hundreds of sites and 45000 users.

The implications on the networking infrastructure are that security needs to be embedded in the network, with centralization of security functions wherever feasible, to decrease the cost of ownership. For example, security-related functionality in LAN edge should be limited to functions such as enforcing policies and participating in endpoint security mechanisms, leaving more sophisticated mechanisms such perimeter protection, firewalls and threat protection analysis to the network core. In addition

and as discussed in the next section, security mechanisms need to be multimedia-aware and operate without introducing impairments for real-time traffic.

Nortel can offer enterprises complete multimedia-friendly security solutions using a Layered Defense approach that provides adaptive, end-to-end protection for their networks, including endpoint, perimeter, core network, and communications security, as well as security management – securing the network while enabling the virtualized enterprise. Incorporating Nortel innovation and leveraging best-in-class technologies from such companies as Check Point and Opsware Inc., these security solutions enable enterprises to not only protect against growing threats to their operations and employee productivity, but meet the heightened privacy and accuracy requirements of regulatory compliance.

Nortel proof points:

- *IT Services Firm achieves 100% business continuity for its distributed IP Telephony contact center.*
- *A NYC-based financial institution deploys multi-terabit optical network for business continuity/disaster recovery.*
- *A financial institution is deploying a secure routing layer to lead in encrypting all branch and Automated Banking Machines traffic across the WAN.*

Strategic Imperative #2: *Reliability and real-time performance to meet the needs of multimedia communications*

Enterprises should deploy networking and security products that deliver consistent Quality of Experience to users, by meeting the security, reliability, short delays and lossless operation required by real-time converged communications. Unfortunately, routers and switches that have evolved from a multi-protocol best effort data networking world may not be able to deliver the functionality and performance required, or may significantly degrade in capacity when faced with voice traffic. Voice is not just another application that runs on an IP network.

Real-time converged communications cannot tolerate packet loss since there is no time to retransmit, and must operate within an end-to-end 150msec delay window so that the interactive nature of human communications is not impacted. This drives the deployment of Quality of Service mechanisms across the network, including the bandwidth-rich LAN environment, to ensure that real-time traffic always receives priority treatment even in the presence of data traffic bursts. WAN bandwidth needs to be engineered appropriately with as much as 80Kbps required per voice call and typically 100-200Kbps for desktop video. It also drives the deployment of service management capabilities that include proactive voice quality management on an end-to-end basis.

Telephony	Property	Data
150msec max	**End-to-end delay**	>1 sec response times
Very low	**Tolerance to variable delay**	High
None	**Tolerance to data loss**	High: TCP for retransmission
30-80 Kbps per call	**Bandwidth needs**	Adaptable to availability
Expected	**Confidentiality**	Desired

Table 1: Comparison of voice (and real-time multimedia) and data networking requirements

Security mechanisms, wherever they are deployed, also need to be made aware of multimedia protocols (typically achieved through software upgrades), and not introduce performance impairments that will effect the user quality of experience. The latter is problematic since security platform architectures that were designed for data may not be acceptable for real-time applications, and may need to be replaced.

The fact that the packetization processes for voice aimed at minimizing latency, creates very short IP packets is a significant challenge for router networks, particularly when various security mechanisms, such as firewalls, VPNs and Access Control Lists have been activated. In fact, in most router architectures, turning on security functions and handling

short voice packets results in a drop of up to 80% in packet handling capacity.

The telephony world refers to 99.999 percent base system reliability based on a mean time between failure measured in tens of years and redundant common control (for large systems). For IP Telephony, the definition of base system reliability is as much a function of how IP Telephony functions are distributed and designed, as of the underlying IP networking infrastructure. Clearly, a comprehensive approach is required to meet the reliability expectations of IP telephony users. Ultra-reliable networking is achieved at the nodal, link and network levels. Time to recover is a key metric in this new real time communications converged network.

Nortel solutions have been deployed in some of the most mission-critical environments: Air traffic control systems, healthcare institutions, stock exchanges and financial institutions, utilities, military field systems and service provider networks.

Nodal reliability is achieved (particularly in the core) through traditional means including redundant switching fabrics, power and fans, and hot swap ability, but also through voice-driven capabilities including sub-second switchover, short system reboot and software upgrade times. Nortel has decades of experience in building some of the most reliable systems in the world. Its Enterprise Routing Switch 8600 is one of the most resilient routing switch platforms in the industry, forming the backbones of many enterprise *and* carrier networks. Link level reliability recognizes the fact that IP routing system can take a long time to converge after failures, measured in minutes in large networks. Therefore Nortel has invested heavily in providing rapid recovery from failures at the link level. For example, Ethernet link aggregation including Nortel extensions provides sub-second recovery from link failures even across dual homed nodes (between core switches or between wiring closets and core switches). Nortel was also a pioneer in resilient packet rings that combine optical ring and Ethernet technology to provide 50-ms recovery from failures. Network level redundancy leverages various IP networking techniques to provide load balancing across paths and additional levels of LAN and WAN redundancy. These capabilities meet the demanding needs of IP telephony and real-time multimedia, but also deliver the benefits of increased reliability for all applications running across the network.

Nortel offers a full-range of voice and multimedia friendly and aware security, wireless and wired LAN, and WAN solutions that have established Nortel as a #2 player in the networking space. These have been architected with secure multimedia as an upfront requirement. In this way, Nortel can help enterprise evolve converged networking, enabling real-time applications that enhance employee productivity and business effectiveness, and increase customer engagement.

Nortel's Secure Router products, which incorporate routing, VPN and firewall functionality, excel at the low-latency, small packet throughput demanded by real-time voice and multimedia applications. Independent testing authority, Tolly Group, has demonstrated these as capable of delivering 2-7 times the throughput of equivalent routers from the competition, including Cisco.

Nortel's link aggregation solutions, referred to as Split Multilink Trunking, recover four times faster than comparable solutions from Cisco, according to tests undertaken by Tolly Group. Split Multilink Trunking is also much simpler to configure than schemes based on Fast Spanning Tree Protocols.

Strategic Imperative #3: *Strategic vendor partnerships for lower cost and increased agility*

The path to lowest total cost of ownership starts with architecting systems that concentrate network intelligence in the core and keeps the edge relatively simple, while adhering to open standards. For example, with 80% of LAN investment in the wiring closet, it makes sense to keep the LAN edge as operational simple as possible while striving to achieve the lowest cost per port to support required security and traffic management functionality. In the WAN, similar thinking can be applied to the branch

network achieved through centralization of functionality wherever possible. For example, many enterprises are centralizing their IP Telephony systems including unified messaging, and virtualizing their contact centers with an eye for lowest TCO.

This leads to an opportunity to partition the network and select a strategic vendor in each area, while keeping the number of vendors to a manageable number. Partitioning can be done on a functional basis (voice and data) or by site type (branch vs. head office) or even on a regional basis. This allows the enterprise to create a more competitive environment among its strategic vendors which at the end of the day is in the best interest of all stakeholders. Concerned about the maturity of standards? The reality of IP networking as see in the Internet is that it is a highly multivendor environment today. Juniper's success in taking away significant share from Cisco in public core networks is testimony to this. The reality of IP Telephony today (and of telephony over the decades) is that, even if a single strategic vendor is selected, it is a multivendor environment when looking at unified messaging, conferencing, contact center and CTI applications. Moreover, the industry is now talking about business-transforming real-time converged communications across the virtual enterprise, embracing partners and customers. It's a whole ecosystem that is multivendor by its very nature, including clients and applications, with interoperability assured through open standards, including for example SIP, Web Services, XML and SAML.

Some would advocate going with a single vendor for telephony and networking because this eases the task of ensuring that performance requirements of voice are met. Others would say that since IP telephony is a real-time application running on an IP network, selecting a vendor who is best in breed in telephony, independently of the networking vendor is the best approach. However, enterprises too often accept vendor marketing at face value. If a vendor only has a hammer, then everything looks like a nail. If the vendor has no installed telephony base, they will argue that evolving to IP telephony "hybrid" systems is a bad thing (for their revenue stream!); at the same time, they may argue that putting IP telephony call control in a "hybrid" router is a good thing (for their revenue stream!). A data vendor may deeply discount its IP telephony offer, recovering lost revenues from network upgrades after the deployment is started. Looking beyond marketing message is critical. A vendor committed to multivendor interoperability is a lower risk in this evolution than one with a single-vendor bent. Open standards are critical to provide the flexibility the business needs to avoid dependence on vendors and leverage new technologies and innovations as they emerge.

Nortel believes a diversified approach offers more flexibility to embrace innovation. Partnering with vendors such as Nortel, who is one of two vendors that can deliver a complete end-to-end LAN/WAN data infrastructure along with market-leading real-time converged communications and engaged applications solutions for enterprises, is a clear low risk opportunity. Nortel is more than willing to submit its technologies to customer or third party testing to validate its performance claims and to demonstrate its technological differentiators in the lab, not just on paper. In addition, Nortel professional services can help enterprise bring it all together and even manage the day-to-day operation of the enterprise communications environment.

If you have or are considering Nortel as your strategic Telephony vendor, then your IT department should seriously consider leveraging the partnership in the LAN and/or branch secure routing environment as well.

Nortel real-time converged communications solutions have been certified by third parties and are supported by Nortel to operate on other vendor's networks, creating choice for the enterprise in deploying converged networks.

Nortel can deliver the IP WAN secure routing solution at a lower cost of ownership, starting with a compelling discount (typically exceeding 20% of the router market leader), while delivering superior performance. For example, configuring a firewall on the recently announced Nortel Secure Router in 20% of the time in takes to configure an IOS firewall.

The Nortel Difference

Nortel understands the challenges faced by enterprises in developing stronger customer relationships, and the critical role of IT in serving business objectives. The IT infrastructure is no longer an adjunct support structure; it is the essential foundation for enterprise performance. Nortel is one of two major vendors that addresses both enterprise and service provider markets and delivers the full spectrum of secure end-to-end converged networking solutions. Nortel is focused on delivering lower TCO, increased employee productivity and stronger customer engagement through:

- Ultra-reliable converged IP, Ethernet and optical networking that span the data centers, campus sites and remote and branch offices.
- Fully featured real-time converged communications systems including IP Telephony
- Secure on-site and off-site mobility including wireless LAN and wireless mesh networks
- Engaged applications including advanced speech self-serve and agent-assisted contact centers
- Endpoint, perimeter, core and communications security systems
- Service and network management
- Professional services

Nortel is proactively involved in standards, is committed to making multi-vendor interoperability a reality, and is expanding an ecosystem of client, security and application vendors to deliver more value to enterprise customers. With this solution breadth, and technology depth in both enterprise and carrier markets, Nortel is an ideal strategic partner for enterprises to help achieve their business objectives. While Nortel can deliver the total end-to-end converged communications solution, it represents a low risk choice in any part of the enterprise network, whether in LAN or WAN, wired or wireless, voice or data, private or hosted, or employee-facing or customer-engaging environments.

Nortel proof points:

- *Nine of 10 Fortune 500 companies rely on Nortel each day - serving as the only networking vendor to have deployed 50 million telephony lines and 50 million Ethernet ports.*
- *More than 93% of the Top 100 Manufacturing companies, including those in Aerospace, Pharmaceuticals, Automotive, and IT run on Nortel.*
- *Every single one of the world's top 20 airlines relies on Nortel.*
- *More than 80% of the Top 100 banks in the US rely on Nortel.*
- *Fifteen thousand healthcare institutions in US and Canada rely on Nortel solutions.*
- *Every single one of the top 10 largest universities in North America, serving more than 500,000 students, and 9 out of 10 of the largest public school districts in the US, serving more than 3.5 million students, run on Nortel.*

A Case In Point -- Branch Office Renewal Situation
Your branch solution was established in preparation for Y2K, and it may be time for a refresh.

Requirements: New levels of security are required, traffic has increased and VoIP has become a reality.

Voice options: Nodal voice (as today) or centralized voice served from your regional office.

Data options: General purpose Swiss-army knife branch routing platforms or specialized secure router designed to meet reliability and performance needs of voice and multimedia.

Vendor options: horizontal (voice vs. data) vs. vertical (branch vs. central site) procurement strategies.

Vendor choices: only two vendors can meet your needs (Nortel and the other vendor).

Strategic vendor partnerships: You have or are considering Nortel as your IP Telephony vendor and should consider Nortel as your strategic converged branch solution provider, possibly working into another vendor's core network.

The Nortel advantage: Rich telephony features without compromise; evolution at your own pace to multimedia collaboration and mobility; layered security- and voice-optimized wired and wireless LAN and WAN data capabilities.

Why now: The Nortel Secure Router portfolio extensions, derived from Nortel's acquisition of Tasman Networks announced in late 2005, excel at the low-latency, small packet throughput demanded by real-time voice and multimedia applications; deliver 2-7 times the throughput of equivalent competitive router products, even when running integrated VPN acceleration, secure dynamic routing and stateful packet inspection; and deliver dramatic installation simplification using a Cisco-like CLI; all at a significantly lower cost than competitor products.

In the United States:
Nortel
35 Davis Drive
Research Triangle Park, NC 27709 USA

In Canada:
Nortel
8200 Dixie Road, Suite 100
Brampton, Ontario L6T 5P6 Canada

In Caribbean and Latin America:
Nortel
1500 Concord Terrace
Sunrise, FL 33323 USA

In Europe:
Nortel
Maidenhead Office Park, Westacott Way
Maidenhead Berkshire SL6 3QH UK
Telephone: 00800 8008 9009 or
+44 (0) 870 907 9009

In Asia Pacific:
Nortel
Nortel Innovation Centre
1 Innovation Road
Macquarie University Research Park
Macquarie Park, NSW 2109
Australia
Telephone: +61 2 8870 5000

In Greater China:
Nortel
Beijing Headquarters
Nortel Tower
Sun Dong An Plaza
No 138 Wang Fu Jing Street
Beijing 100006, China
Telephone: +86 10 6510 8000

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at **www.nortel.com**.

For more information, contact your Nortel representative, or call 1-800-4NORTEL or 1-800-466-7835 from anywhere in North America.

NN114700-011606