

Eliminating the Mobile Blind Spot — Extending Enterprise Security Coverage and IT Reach with the Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian

While wireless broadband delivers continuous access to enterprise networks and boosts the productivity of mobile professionals, it also makes it increasingly difficult for IT managers to ensure the health of mobile laptops and the security of the sensitive data they contain.

Laptops that leave the enterprise fall into a “mobile blind spot”, outside the reach of IT’s protective measures. They are vulnerable to loss, theft and intrusion and are unlikely to be fully patched and backed up while on the move. Enterprise IT staff need a simple, secure way to bring visibility to the laptops caught in the mobile blind spot.

This paper presents the Alcatel-Lucent approach to eliminating the mobile blind spot by extending security coverage and IT reach beyond the walls of the enterprise with 24/7 mobile laptop tracking, troubleshooting and management capabilities.

Table of Contents

- 1 Introduction**
- 2 Addressing the Mobile Blind Spot**
 - 2.1 Protecting Sensitive Data
 - 2.2 Streamlining Laptop Management
 - 2.3 Improving the End User Experience
- 3 The Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian**
 - 3.1 The Card
 - 3.2 The Laptop Client
 - 3.3 The Gateway Server
- 4 Extending IT Control to Other Applications**
 - 4.1 Application Programming Interface
 - 4.2 Assisted File Transfer
 - 4.3 Assisted Web Transfer Utility
- 5 Conclusion**
- 6 Acronyms**

1 Introduction

For the enterprise IT organization, the wide adoption of laptops and mobility offers unique productivity gains, but also introduces a mobile blind spot. When a mobile laptop leaves the enterprise, the IT department loses visibility of the laptop and, as a result, loses its ability to protect either the laptop or its sensitive data.

In this blind spot, corporate resources cannot be protected by a simple perimeter security approach because mobile laptops can connect to the public Internet using network interfaces that are no longer subject to the security controls of the IT organization. Uncontrolled Internet access can compromise the mobile laptop. For example, malicious software may run undisturbed for several hours or even days before the IT administrator detects it and applies the necessary safety measures. Most critically, an infected laptop can 'leak' sensitive information onto the public Internet, creating a nightmare scenario for the enterprise.

Regular software updates and data backups provide a level of defense against these dangers. However, it is difficult and sometimes impossible to protect mobile laptops because end users are often not willing to run key laptop management processes at inconsistent link speeds. Significant amounts of proprietary information may be stored on these laptops, with the potential for major financial liabilities to the enterprise in case of loss or theft.

IT organizations need a way to address these challenges while continuing to capitalize on the mobility benefits provided by broadband wireless networks.

The Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian (NLG) puts continuous laptop access and control back in the hands of the enterprise. With this control, enterprises can proactively safeguard the sensitive data on employees' mobile laptops anytime, anywhere, even when the laptop is powered off.

From off-hour downloads of patches, updates and backups to proactive, real-time response to security loopholes arising through public Internet access, the OmniAccess 3500 NLG increases productivity, helps enforce 100 percent IT policy compliance and improves business continuity.

2 Addressing the Mobile Blind Spot

Enterprise efforts to protect laptops, the data they contain, and the enterprise network itself are currently focused around solutions that:

- Attempt to protect the network from a corrupt endpoint so viruses do not propagate throughout the enterprise
- Encrypt some or all of the data on the device
- Attempt to track the hardware itself when it is lost or stolen

One of the most popular approaches to restricting network access is with endpoint policy enforcement applications based on schemes such as network access control (NAC) and network access protection (NAP). These mechanisms restrict network access for hosts with software that does not comply with current corporate policies. When a policy violation is detected while connecting to the enterprise network, the protection mechanisms validate the host software and quarantine the host to a restricted portion of the enterprise network.

While quarantined, the host receives the software patches and updates needed to restore policy compliance and regain full network access. In most cases, network access is not restricted if the host is not connected to the enterprise network. For example, a trojan or virus that infects a laptop can easily leak corporate data while the laptop is outside the enterprise perimeter, connected to a public WiFi hot-spot or a private LAN.

An even greater vulnerability exists when users bypass connectivity to or through the enterprise and connect directly to the Internet or other networks. A new paradigm is required to protect the mobile laptop and its data independent of whether the laptop is connected to the enterprise.

By removing all spatial and temporal connectivity boundaries and exercising full control of the laptop connection to the enterprise network, the Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian separates policy enforcement from network logon. It interoperates with and complements third-party NAC and NAP mechanisms, providing network access control irrespective of the laptop location or the available connectivity.

A platform that empowers the existing security infrastructure and enables new security features is pointless if the platform itself is not adequately protected. With the OmniAccess 3500 NLG, the server and management components are protected within the enterprise network perimeter and the client component is protected in a separate hardware device (a wireless broadband card) that is inaccessible to the end user and to malicious code.

2.1 Protecting Sensitive Data

The exposure of corporate and customer data from lost and stolen laptops is on the rise. According to a 2006 survey released by the Ponemon Institute, 81 percent of companies surveyed admitted losing at least one laptop containing sensitive information during the previous 12 months.

The OmniAccess 3500 NLG protects against exposure of data in case of laptop theft or loss by:

- Preventing unauthorized users from retrieving sensitive information in stolen or poorly-guarded laptops
- Recovering data lost both accidentally (a disk crash) or by external attack (a virus)

The data on the laptop is protected whether the card is in the laptop or removed.

To enable this level of security, the OmniAccess 3500 NLG interoperates with encryption software to provide a second level of authentication before data is decrypted. Encryption keys are stored on the card, rather than on the laptop.

The OmniAccess 3500 NLG also protects against data loss from laptop theft by issuing a 'kill pill' upon suspicion of theft. This security protocol remotely initiates destruction of the encryption keys (stored on the card), automatically deletes authentication credentials on brute force attempts, and provides geographical tracking of the missing or stolen laptop. In addition, the platform creates a log of which data was stored on the encrypted volume and which was not protected so the enterprise can assess potential issues.

If the laptop is later recovered, the encryption keys and authentication certificates can be re-created over the air to allow the end user to immediately resume work.

Most enterprises implement systematic backups to alleviate the potential damage that can be caused accidentally or by external attacks. However, these backups rely on frequent transfers of large amounts of information. An employee faced with inconsistent access speeds or only a few minutes a day to log on to the enterprise network may not wait for the daily backup to complete before taking control of the access connection. Employees commonly postpone imminent backups. As a result, overdue backups may build up to the point where large amounts of critical information are exposed to potential risk.

The OmniAccess 3500 NLG allows incremental backups to be staged in the client card and uploaded overnight when the user does not need access to the laptop. This minimizes the disruption and maximizes the probability that an up-to-date image of the laptop content is securely stored within the enterprise.

2.2 Streamlining Laptop Management

Software update distributions and inventory collections streamline computer management in enterprises with a large base of managed computers. But this can be difficult to sustain when a sizable number of laptops are assigned to mobile employees.

A mobile worker may rarely be within the enterprise and may access the corporate network only sporadically from off-site locations. This usage pattern creates IT maintenance procedures and software installations that are bulkier than normal and most often conducted through low-capacity access links.

More content and less bandwidth imply longer transactions, with higher consumption of IT resources and increased probability of failure. Applications for email and device management rely on file transfers that can be quite large. Depending on the capacity of the access link, a large file transfer may or may not complete during a single access session. To avoid wasting the resources consumed for the initial portion of an incomplete file transfer, individual applications must have built-in file transfer management capabilities. These can differ across applications and can even interfere with each other when deployed in a common environment.

In addition, the distribution and installation of software updates usually consumes large portions of access link and CPU capacity, which can be a heavy inconvenience to the end user. For example, a software patch distribution may start when the end user is attending an important meeting and needs immediate access to Intranet resources, making those resources unreachable at the most critical time.

The OmniAccess 3500 NLG separates remote management transactions from an end user's network-access activity. This mitigates the effects of remote management tasks on IT resources and reduces user inconvenience.

To do this, the OmniAccess 3500 NLG includes a secure file transfer utility that operates independently of the laptop's state (on, sleep, hibernate, off). This utility is optimized for unreliable access links with an open interface that all enterprise IT applications can share.

This means a patch or a policy update can be distributed to mobile laptops overnight, even if the laptop is turned off. The patch or new policy is applied to the laptop as soon as it is turned on, irrespective of whether network connectivity is available at that time.

2.3 Improving the End User Experience

While security threats, data protection and laptop management issues must all be addressed, enterprise IT organizations must also ensure ease-of-use and a high quality of experience for end users.

For employees who are regularly on the move, remote access often means nuisances such as:

- Having to manually select the access interface (3G, WiFi, LAN, dial-up modem) based on network availability
- Having to run multiple interactive sessions to establish secure connectivity into the corporate network
- Inconsistent network application performance
- Abrupt degradations of computing capacity during bulky transactions such as backups and patch downloads

End users benefit when operational tasks such as software patches and virus updates are completed offline. With the OmniAccess 3500 NLG, these types of operational events can take place overnight when the laptop is turned off.

Ease-of-use is also improved with the access-network handoff and automatic virtual private network (VPN) features built into the OmniAccess 3500 NLG.

The availability of multiple network interfaces on a laptop creates the opportunity to choose the network that offers the best access performance at any time. To take full advantage of this opportunity, the laptop should transfer its access link without disrupting any running network application. Existing mobility management solutions can maintain a secure access session when the laptop switches between access points within the same network (within a WiFi network, for example) but not when it switches between access networks (from a WiFi network to a 3G or a local area network, for example).

Sharing the goal of new mobility standards being developed within the IEEE and the IETF, the OmniAccess 3500 NLG includes a proprietary mechanism that ensures network applications are not disrupted when the laptop switches between access networks.

Likewise, end users currently spend an inordinate amount of time worrying about access and connecting back to the enterprise. End users must enter data and authentication information each time a VPN must be established or re-established. The OmniAccess 3500 NLG enables a secure single sign-on procedure that reduces both the number of passwords needed by the end user and IT costs.

3 The Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian

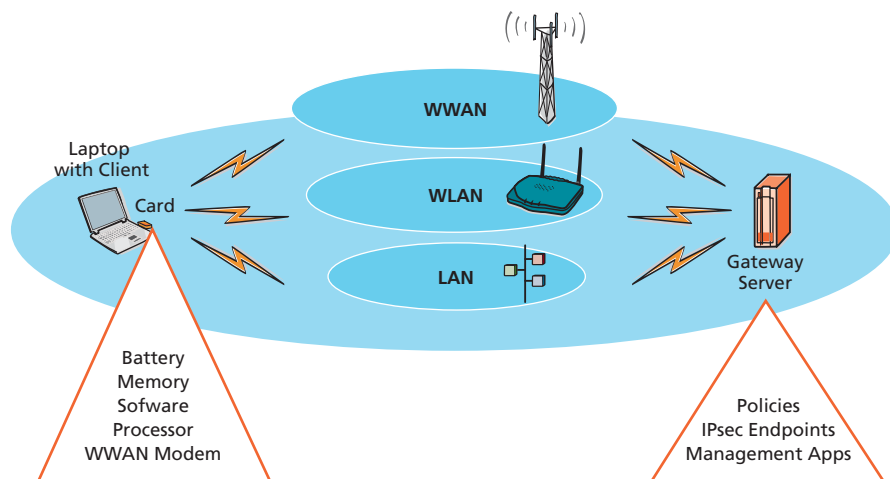
The Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian is an always-available, secure, service delivery platform for enterprise remote access and device management. It satisfies the broad necessities of the key players in today's remote-access and device-management space:

- The IT administrator, who needs an affordable means to minimize threat-reaction latencies and continuously monitor the health of off-site laptops
- The mobile employee, who needs a streamlined network access experience with conflict-free automatic backups and software updates
- The broadband wireless access service provider, who needs compelling applications to expand its subscription base and increase network utilization during off-peak hours

The platform is built on several key components, as shown in Figure 1.

- A PCMCIA data card for remote laptops that:
 - Embeds a wireless wide area network (WWAN) modem, a processor, a battery, and non-volatile memory
 - Independently establishes the IPsec tunnel that secures the remote access connection
 - Makes the laptop reachable by the IT organization through the WWAN interface, virtually anytime and anywhere
- A laptop client that contains the end-user graphical user interface (GUI) and a link between the capabilities on the card and the laptop so the card can watch over the laptop and key applications
- A gateway server, which is deployed within the enterprise network perimeter to:
 - Host the enterprise endpoints of the IPsec tunnels
 - Exploit the extended reachability of the laptop to improve the effectiveness of all remote management functions
 - Manage all OmniAccess 3500 NLG components

Figure 1. Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian Components



3.1 The Card

The PCMCIA data card keeps the mobile laptop within the security perimeter of the enterprise network at all times. It is a Cardbus PC Card compatible with most PC platforms that support a Type-II PCMCIA slot. The card combines the following physical and functional elements:

- A rechargeable battery that supplies power to the card when the laptop is in standby, hibernate, or shutdown state. During normal operation, the card draws power directly from the laptop.
- A wireless modem that provides IP connectivity over a public or private wireless network. Different versions of the card support different wireless interfaces. 1xEV-DO and EV-DORevA are supported in initial releases. HSDPA, HSUPA and WiMAX will be supported in future releases.
- Non-volatile flash memory for storage of persistent data, security certificates, and client synchronization data. The memory is partitioned into user and system space. The system partition is not accessible to the laptop.
- An embedded CPU.
- An embedded Linux platform that hosts on-card remote-access functions, applications and services such as:
 - Link management to the OmniAccess 3500 NLG server, which enables capabilities such as tunnel monitoring, software and firmware updates and remote assistance
 - Authentication to associate an end user with unique instances of the card and the laptop
 - Data traffic extension processing capabilities, including stateful packet inspection, full IP stack operation, PPP encapsulation, and IPsec encapsulation/encryption/decryption
 - Interface management capabilities for monitoring the quality of the access links offered by the surrounding networks and seamlessly switching between them
- An external on/off switch that, together with the on-card rechargeable battery, makes the power state of the card independent of the power state of the host laptop. The switch makes it possible to turn the card off when the use of radio equipment is prohibited by official regulations (during takeoff and landing of commercial airplanes, for example).
- An internal antenna.

Figure 2. Card Component



Working as a standalone network node attached to the laptop, the card:

- Independently establishes and maintains the IPsec tunnel that provides authentication and encryption to the remote connection with the enterprise network, even when the laptop is powered off
- Hosts a personal firewall that applies the latest filtering policies set by the enterprise to all laptop-terminated traffic
- Stages the file transfers between the laptop and the enterprise
- Provides temporary storage for device management and end-user applications when the laptop is powered off

3.2 The Laptop Client

The laptop client software is installed on the laptop to support the functionality of the card. This Windows XP software provides the laptop with the routing adjustments and peering entities needed for communication with the card. The client includes tamper-proof drivers and services that prevent the end user from accessing or disabling software components as well as application modules that:

- Display interface statistics and current connection states
- Provide configuration parameters (the accessible parameters and the extent of their control by the end user are defined by enterprise policy)
- Facilitate secure network connectivity from constrained environments (hotels, WiFi hotspots, etc.) where a public IP address must be negotiated with a local access point provider before an IPsec procedure can start

3.3 The Gateway Server

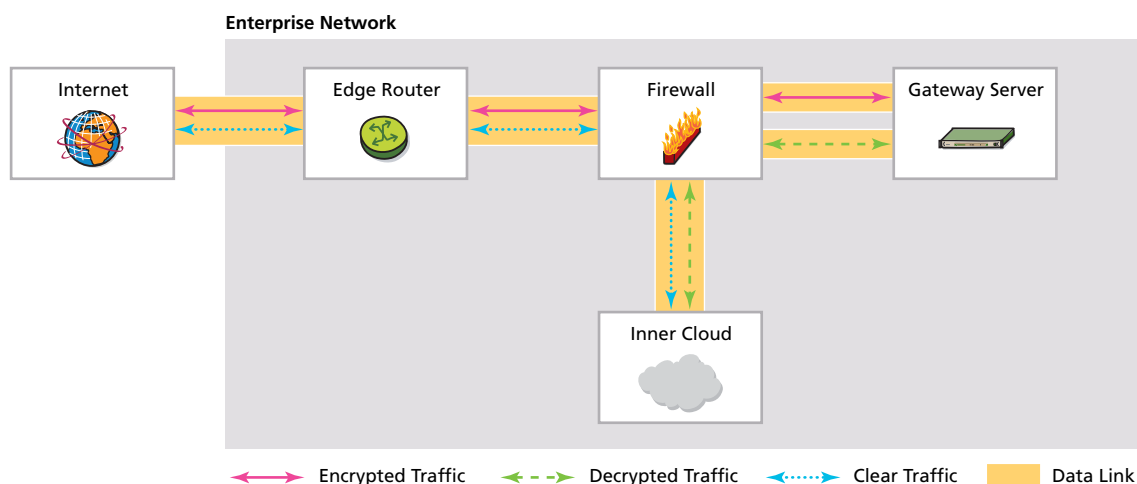
The gateway server is deployed on the enterprise premises. It combines:

- Two network interfaces (10/100/1000 Mb/s Ethernet) — one that is external (to handle traffic to and from the public Internet) and one that is internal (to handle traffic in the inner portion of the enterprise network)
- A processing subsystem (CPU, OS, and management software) that implements OmniAccess 3500 NLG functions
- A hardware acceleration module for IPsec encryption/decryption, key management and compression
- A hard disk for storage of local information and application caching
- A secure management interface for driving all OmniAccess 3500 NLG operation, administration, management and provisioning (OAM&P) procedures

The server terminates the secure tunnels, manages user credentials and security policies and provides storage and file transfer capabilities in support of third-party remote access and device management applications. The server also cooperates with the card to ensure that vertical handovers do not disrupt network applications that are running.

The server is best deployed as a stub of the enterprise firewall, as shown in Figure 3.

Figure 3. Recommended Placement of the Alcatel-Lucent OmniAccess 3500 NLG Server within the Enterprise Network



The firewall and the server exchange encrypted traffic over the external interface of the server and decrypted traffic over the internal interface. The firewall applies full protection to both the external interface of the server and the inner portion of the enterprise network.

Alternative arrangements can also be adopted to match requirements of pre-existing network infrastructures. In addition, multiple instances of the server can be deployed within the same enterprise network to increase capacity and extend geographical coverage and service availability.

To support network activity, the server includes management software that drives the OAM&P functions for the server, the card, and, by extension, the laptop.

The server is also the repository for all policies, audit data, configuration information and application data, including the asset inventories for the laptops controlled by the OmniAccess 3500 NLG. It supports backup, restore, recovery and encryption for all of its data.

4 Extending IT Control to Other Applications

The Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian is designed so partners can easily take advantage of its APIs to extend the 24/7 access, anti-tampering, location, and health/visibility capabilities to their own enterprise applications.

4.1 Application Programming Interface

Applications can be integrated with either the card or the server component of the OmniAccess 3500 NLG, opening the door to a wide array of technology advances for partner applications, including:

- Patch management, by enabling delivery of software updates to laptops that are not connected to the enterprise
- Encryption, through remote management of certificates and keys
- Backup and restore, by enabling data backups for laptops that are rarely or never connected to the enterprise
- Endpoint security, through 24/7 policy management, regardless of connection type
- Network access control, by protecting the laptop and its sensitive data, not just the network
- Configuration management, by providing 24/7 access to and control over all device configurations

- Business applications, by enabling IT access irrespective of location
- Two-factor authentication, by eliminating the need for additional authentication devices

4.2 Assisted File Transfer

The assisted file transfer (AFT) feature included in the OmniAccess 3500 NLG offers another way for third-party applications to take advantage of the product's capability to transfer data between the enterprise and mobile laptops, irrespective of the power state of the laptop (sleep/hibernate/off).

Today, applications that require file transfers with mobile laptops for tasks such as patches and backups are severely limited in their ability to accomplish the file transfer due to the very nature of mobility. Users may only connect intermittently and may override bulk data transfers that consume large portions of the laptop computing capacity and interfere with the operation of the laptop. For applications that have loose real-time requirements, such as routine file backups and uplink email transfers, avoiding conflicts with end users' needs can improve productivity.

To enable the temporal separation of non-real-time application transactions from the ordinary operation of the laptop, the OmniAccess 3500 NLG opens a second, three-legged path between the laptop and the enterprise application servers using the AFT. This path allows data to be temporarily cached in the client card and uploads/downloads to occur even when the laptop is not powered on.

For example, when a backup application initiates a data upload, the data is cached in the client card and is not directly transferred to the enterprise. The upload to enterprise servers is performed at a later stage, when the user is not using the network or the laptop, or when network connectivity charges are lower (overnight).

The AFT is a generic file transfer utility that enables advanced controls on committed file transfers, including priority- and location-driven scheduling, rate limiting, status monitoring, and pause/resume/cancel commands.

Third-party applications can use AFT path transport services transparently or integrate the AFT path in their client-server exchanges. The OmniAccess 3500 NLG is integrated with the Microsoft SMS patch management application using the AFT capability.

4.3 Assisted Web Transfer Utility

Remote directory synchronization is not the only paradigm adopted by commercial IT applications for triggering and executing the transfer of software packages. Popular products, such as the PatchLink Update patch and vulnerability management solution, rely on web-based client-server transactions to deliver software updates.

In an ordinary environment, the laptop periodically queries the application server with web requests. When new content is available, the server distributes that content with the subsequent web response. These operations can be performed only when the laptop is connected to the enterprise network and are often limited by the network access speed.

However, the server can be easily overwhelmed if it receives multiple simultaneous requests. This delays the deployment of much-needed patches. Using web proxy caches in the path between the laptops and the server is one way to avoid overloading the server. However, when many laptops obtain network access from low-capacity wireless links, congestion and heavy delays can occur on the paths between the laptops and the web caches.

The independent storage, power, and networking capabilities of the card component of the OmniAccess 3500 NLG offer a unique opportunity to remove the wireless link and connectivity bottleneck from the path between the laptop and the closest web cache. The product's assisted web transfer utility relies on the installation of web proxy caches and corresponding cache controllers in both the gateway and the card. This reduces client-server web transactions and allows for rapid exchanges between the laptop and the card.

Because the laptop card is always on, the caches can be synchronized overnight over a 3G network connection. This means content is delivered to the laptop even when the laptop is turned off. Important patches or software updates are made available to users immediately and wireless access speed problems are avoided.

5 Conclusion

The Alcatel-Lucent OmniAccess 3500 Nonstop Laptop Guardian enables the extension of the security perimeter of the enterprise network beyond the physical boundaries of the enterprise. It allows enterprise IT managers to manage and secure mobile laptops as easily as they do desktops, effectively eliminating the mobile blind spot. With this complete remote endpoint management platform, enterprises can take full advantage of the benefits mobility offers, while minimizing the risks associated with having laptops outside their secure network.

In addition, enterprise employees can capitalize on the mobility benefits provided by broadband wireless networks. The OmniAccess 3500 NLG provides secure and continuous access to the enterprise, reduces data security concerns, streamlines network access and log in and manages backups and software updates more efficiently.

This complete mobile laptop management platform provides IT managers with 24/7 visibility of mobile laptop location and health for tracking, troubleshooting and management. Most importantly, it offers continuous access to remote and mobile laptops even when they are powered off or offline.

6 Acronyms

3G	third generation
API	application programming interface
BWA	broadband wireless access
CPU	central processing unit
EPPE	endpoint policy enforcement
EV-DO	Evolution-Data optimized
EV-DOrA	Evolution-Data optimized release A
HSDPA	high-speed downlink packet access
HSUPA	high-speed uplink packet access
IP	Internet protocol
IPsec	Internet protocol security
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IT	information technology
LAN	local area network
NAC	network access control
NAP	network access protection
OAM&P	operation, administration, maintenance and provisioning
OS	operating system
PCMCIA	personal computer memory card international association
VPN	virtual private network
WiFi	wireless fidelity
WiMAX	worldwide interoperability for microwave access
WWAN	wireless wide area network
WiFi	wireless fidelity
WiMAX	worldwide interoperability for microwave access
WWAN	wireless wide area network

www.alcatel-lucent.com

Alcatel, Lucent, Alcatel-Lucent and Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.
© 2007 Alcatel-Lucent. All rights reserved. 21888 (04)

