



White Paper

Addressing Enterprise Network Access Requirements

By:

Jon Oltsik
Enterprise Strategy Group

August 2007

Table of Contents

Table of Contents	i
Executive Summary	2
Just what is Network Access Control (NAC)?	2
NAC: A Brief History	3
NAC Must Start With a Business Perspective	4
NAC Technology Requirements	5
Tactical NAC Can't Meet Enterprise Needs	7
NAC Must Be an Enterprise Network Initiative	8
NAC Implementation Recommendations	9
Nortel Is Taking NAC to Enterprise Networks	11
The Bottom Line	13

This ESG White Paper was developed with the assistance and funding of Nortel.

Executive Summary

Ask 10 networking and security professionals to define Network Access Control (NAC) and you will likely get 10 unique responses - a sad statement about industry hyperbole. The truth is that NAC has become an essential piece of security enforcement and network infrastructure. NAC also is critical to the business as it enables new global business processes that can drive revenue, improve productivity, and cut costs while enhancing security.

The time for NAC-based spin and confusion is over - enterprise security and business processes depend upon NAC clarity and near term deployment. This paper concludes:

- **NAC is about enabling business and security policies, not scanning PCs.** Network access control has the potential to facilitate open communications between organizations, improve corporate governance, automate IT processes, and increase security. It's important for CIOs to look at the big NAC picture and not remain trapped in a technical discussion about IP addresses, networking equipment, and security enforcement technologies.
- **Tactical point problems lead to enterprise problems.** Yes, tactical NAC appliances can ease short term pain but piecing together multiple point technologies will never amount to a strategic end-to-end NAC implementation that fits enterprise needs. In fact, a tactical approach could ultimately lead to operational overhead, security vulnerabilities, and the inability for IT to meet business requirements.
- **Think in terms of an enterprise NAC architecture.** NAC should be integrated into existing desktop and security technologies while eventually becoming part of the communications fabric itself. To support business and IT objectives, large organizations must embrace a NAC strategy that supports any user, any device, and any network.
- **NAC should grow organically.** NAC should grow through a phased implementation plan that starts small and grows over time. The Enterprise Strategy Group (ESG) recommends that CIOs: 1) Work closely with business managers, 2) Understand existing network and security capabilities, and 3) Plan on expanding NAC policies and enforcement over time.

Just what is Network Access Control (NAC)?

ESG believes that CIOs should refrain from asking this question to their technology vendors. Why? Technology executives will likely get a lot of industry spin and rhetoric but no solid definition. For example, do a Google search on the term "network access control" and you'll pull up over 1.5 million links. Talk about information overload!

It is important to start with a simple definition. The technology glossary whatis.com defines NAC as follows:

Network access control (NAC), also called network admission control, is a method of bolstering the security of a proprietary network by restricting the availability of network resources to endpoint devices that comply with a defined security policy.

In parsing this sentence, NAC can be construed as a common endpoint security policy management system for a range of network (i.e. physical and virtual networks such as LANs, WANs, and Internet-based VPNs) and device types. In most cases, security policies are centered on three things:

1. **Authentication.** Users and/or endpoint devices must authenticate themselves before they are granted access to the network. Additionally, single endpoints can authenticate once and then roam across networks and be managed from a common NAC policy server. The network can then make further policy decisions based upon user and device identity characteristics.
2. **Endpoint health status.** Before gaining network access, endpoint devices are checked for system vulnerabilities, security software configuration parameters, and malicious code signatures. Further network access decisions are based upon the results of this examination.
3. **Authorization.** NAC can be configured to limit a device to specific network assets or tasks and also be tuned for specific types of networks. For example, an IP phone may be restricted to a particular network VLAN, IP telephony gateway, and only allowed to communicate using SIP protocols.

The overall objective of NAC is simply to make better decisions about who gets access to the network (or network segment) and what they can do once they are admitted. The health check provides additional security protection by limiting or restricting access to endpoints deemed to be “unhealthy” based upon an organizations policy definition of endpoint health. In this way, NAC does not play politics. Even the CEO may be denied network access when the NAC policy engine detects that his or her antivirus signatures have not been updated for several weeks.

NAC: A Brief History

Network access is nothing new. Users are used to logging into the network with usernames and passwords as they have for decades. Network authentication technologies like network directories, authentication servers, and RADIUS have been around for years. When and why did the technology industry come up with this new term NAC?

The abbreviated industry story around NAC goes something like this. Around 2005, NAC was first introduced and presented to enterprise users as a technology framework. The main driver at that time was the preponderance of wormstorms in 2003 and 2004. In theory, NAC would inspect endpoints so that a laptop infected with the next MSBlaster or SQL Slammer worm would be prevented from bringing the entire network to its knees.

In spite of its altruistic message NAC had a fundamental flaw from the start. Users appreciated the concept but the whole notion of a “framework” brought up historical memories of huge expensive projects -- bad imagery. No one was about to rip and replace their switching infrastructure, install lots of 3rd party desktop agents, and add onto a massive new proprietary infrastructure. Needless to say, the “framework” chapter in the NAC story was rather abrupt.

Undeterred, many technology vendors came up with an opposing NAC designation. Rather than an overbearing framework, NAC could be deployed with simple network appliances to solve some specific tactical network access problems. Want to inspect endpoint devices?

Just add an appliance to the network that intercepts network log-ins and scans systems before granting admission. What could be easier?

There you have it. In a bit more than 2 years, the industry presented polar opposite pictures of NAC -- one vision of a comprehensive framework and another with a focus on technology piece parts. Little wonder why users are so confused!

This situation would be humorous if it weren't so tragic. The fact is that large organizations can benefit greatly from the secure network access controls inherent in NAC. Given these potential gains, users need a clear and succinct definition and approach to NAC as soon as possible.

NAC Must Start With a Business Perspective

Thus far NAC has centered on highly technical topics like 802.1X supplicants, Ethernet switches, and RADIUS servers. Yes, these networking components are important toward NAC operations but ESG believes that discussions should start by defining the business needs that drive NAC requirements. This dialogue should go beyond tactical requirements and take a long term view on security and business needs. When viewed in this context, NAC has the potential to help large organizations:

1. **Open the network for business benefit.** NAC can enable organizations to open their networks to outside constituencies driving new revenue opportunities, enhance productivity, or lower costs.
2. **Improve corporate governance.** NAC can enhance existing controls and provide detailed audit trails for compliance and corporate governance initiatives. This can lead to more consistent operations and lower costs across an organization.
3. **Automate IT processes.** For example, NAC can enable a number of self service applications for endpoint security remediation and patch management. This has the potential to significantly reduce desktop administration costs.
4. **Help enhance data privacy and security.** Business executives are extremely concerned (and rightly so) that their organization may be the next publicly disclosed data breach story in the *Wall Street Journal*. NAC can enable fine-grained network authorization, keeping bad guys away from valuable network assets and private data.

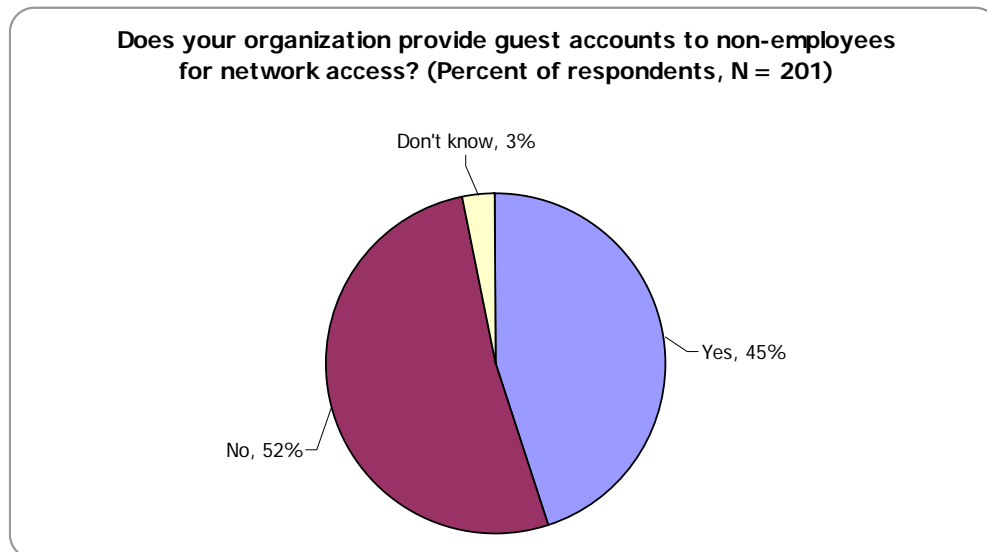
When viewed in a holistic perspective, NAC can deliver maximum benefits when CIOs align technology plans with business needs and treat NAC as a strategic initiative rather than a tactical stopgap. Additionally, NAC can be used to enhance specific vertical industry business processes. A research facility dependent on network collaboration may want to restrict network access to all but the most updated endpoint configuration while a University may grant network access to all students but throttle peer-to-peer application traffic to protect valuable bandwidth. Rather than an "all-things-to-all-people solution," NAC flexibility means it can be customized for specific users, devices, and business processes.

NAC Technology Requirements

NAC business benefits seem relatively clear but the NAC technology journey is anything but straightforward. Enterprise NAC implementations must be scalable, manageable, and auditable in order to:

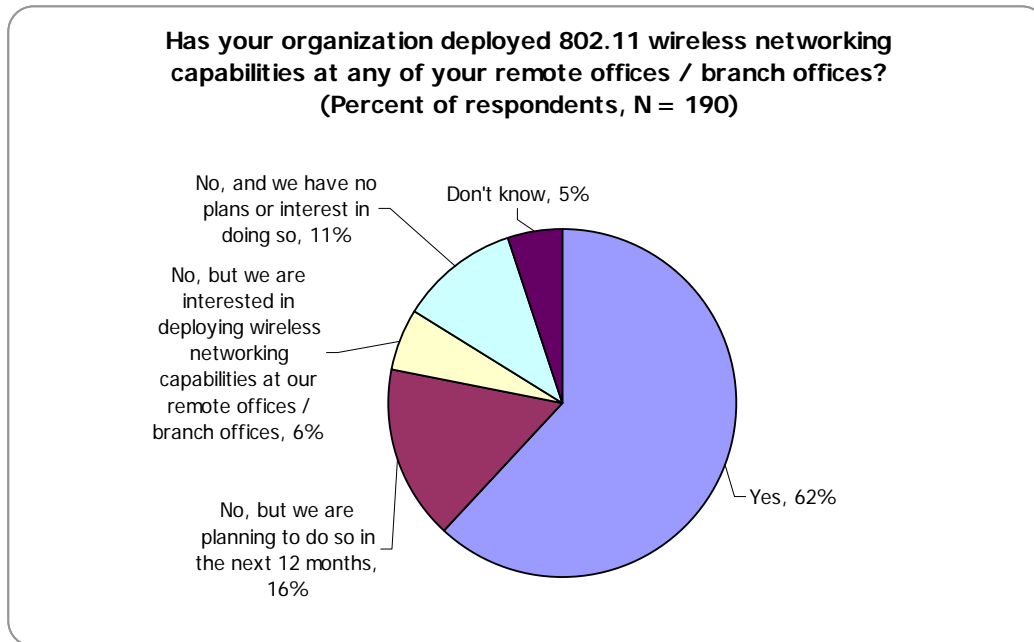
- **Accommodate a melting pot of internal and external users.** In the global 21st century business environment, employees are no longer tethered to corporate headquarters. In 2005 it was estimated that 4.5 million Americans telecommute each day, roughly 20 million telecommute for some period each month, and about 45 million telecommute at least once per year (source: *Telecommuting - The Quiet Success*, The Reason Foundation). The need for network access for non-employees is also on the rise. ESG Research reports that 45% of large organizations said that they provide network access to guest (i.e. non-employees) users (see Figure 1). Obviously, multi-national companies with internal and external users from Boston to Brussels to Bangkok need to create, monitor, and enforce granular network access policies in a consistent manner.

Figure 1. Enterprises Provide Guest Accounts to Non-Employees (source: ESG Research)



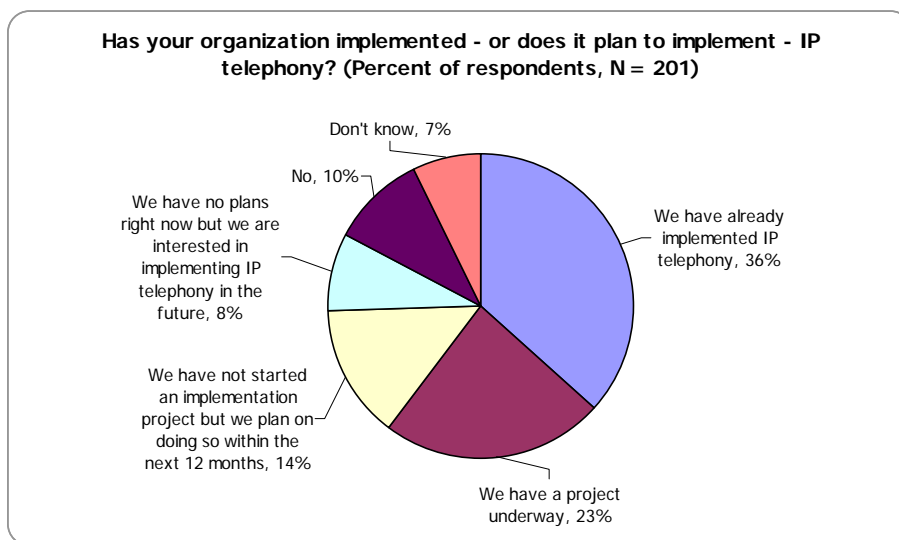
- **Deal with the increasing demand for mobility.** The year 2006 was a milestone for large corporations as they purchased an equal number of desktop and laptop computers meaning that more and more employees are connecting over wireless network access points as they roam across the corporate campus and branch offices (see Figure 2). As substantial as today's wireless network demands are, they are a mere fraction of what's coming. Over the next few years, overburdened CIOs must be ready for a new generation of smart wireless devices connecting over new types of broadband networks using technologies such as 4G and WiMax. With the onslaught of mobility and device types, the network must provide access based upon rules around network location, device type, and security concerns.

Figure 2. Wireless Networking Has Become Ubiquitous in Branch Offices (source: ESG Research)



- **Facilitate new IP-based applications.** Networks activities go beyond connecting sources and destinations. Today's network must distinguish between traffic types in order to assist latency-sensitive IP-based applications for voice, video, and storage. These are no longer niche applications. For example, nearly 60% of large organizations have already deployed IP Telephony or have an implementation project underway (see Figure 3). With latency-sensitive applications like voice, the network must recognize end-points and then set up rules for VLANing, authorization, and traffic acceleration.

Figure 3. Widespread Deployment Of IP Telephony (source: ESG Research)



All of these technical requirements must be supported by strong security across the network. Yes, this includes NAC-centric capabilities like endpoint health checking but it also demands traditional network security functionality such as intrusion prevention, firewalling, and VPN tunneling. In reality, NAC should be viewed as an adjunct to strong network security, not an independent technology.

Tactical NAC Can't Meet Enterprise Needs

Large organizations need an enterprise NAC strategy that fits with business requirement, security policies, and existing network infrastructure. Unfortunately, most NAC products offered by technology vendors are simple add-on point tools and appliances and not end-to-end solutions. A makeshift response at best, today's tactical NAC solutions can't meet enterprise needs because they (see Table 1):

- **Work in isolation.** Tactical NAC solutions are designed to address isolated problems, not provide a comprehensive NAC infrastructure to address a multitude of needs. A LAN-based NAC appliance may ensure that wired user endpoints are malware-free but works independently from existing SSL VPN and network security equipment. In this scenario, network access control turns into a series of technology islands rather than a cohesive enterprise architecture.
- **Limit global policy definitions and enforcement.** NAC point tools force business and technology managers to map policies to technical capabilities rather than business requirements. For example, if the board decides to restrict access to certain network assets, network administrators may be forced to figure out how to configure multiple NAC appliances as well as Ethernet switches, RADIUS servers, wireless APs, and SSL VPNs to meet these policy requirements. In the end, technology capabilities may limit - or even preclude - certain policies from being implemented at all.
- **Lack central management.** Individual NAC tools must be managed on a one-off basis creating an operational nightmare for organizations with dynamic business needs. NAC management could become a business bottleneck in this case. A line-of-business manager will become exceedingly frustrated when the networking team claims that it may take as long as 3 months to test and implement a NAC solution in order to give a geographically-distributed business partner's employees network access from anywhere in the world.

The constant problems in all of these cases are flexibility, operational overhead and scale. These inadequacies are antithetical to a correctly implemented business focused and strategic NAC initiative.

Table 1. Tactical NAC Solutions Can Lead to Enterprise Problems

Problem With Tactical NAC Solution	IT Implications	Business Ramification
Tactical NAC solutions work in isolation	No integration across the network means purchasing and deploying multiple technologies	Added cost. Business initiatives may be slowed down by IT.
Tactical NAC solutions limit global policy definition and enforcement	NAC rules must be configured and enforced on a technology-by-technology basis	It may be difficult to configure, monitor, and enforce business policies.
Tactical NAC solutions lack central management.	Operations overhead and redundant processes. May also impact security.	Scalability and flexibility issues may limit business opportunities.

NAC Must Be an Enterprise Network Initiative

It's time to set NAC free to meet the strategic business, security, and operational needs of the business! To accomplish this goal, NAC must (see Table 2):

- **Fit in with existing IT infrastructure.** By now it should be clear that NAC is not an independent function but rather an enhancement to existing desktop security, network access controls, and security safeguards. Wired NAC should integrate with wireless and remote NAC through integration with wireless APs and SSL VPNs. Initial desktop health checks should be supported by IDS/IPS devices for ongoing traffic monitoring, filtering, and alerting. Access rules should not be limited to the network edge but enforced throughout the network on a user or group basis. NAC gains strength and value when it is “baked” into the desktop, network, and security infrastructure rather than implemented at limited network access points.
- **Provide for flexible implementation and enforcement.** NAC policies and enforcement will vary greatly by organization. For example, a hospital with shared workstations may focus its effort on user authentication and network authorization while a government agency may want to concentrate on guest user access policies for a large number of contractors. The underlying technology must allow for policy variation with a wide array of enforcement technology options. In other words, technology elements must work together to enforce NAC policies regardless of the location of user, device type, network technology type, or network access method.
- **Support centralized policy and configuration management.** Yes, NAC rules may vary depending upon whether an employee logs onto the network from his or her desktop or a software development contractor in Bangalore enters the network through an SSL VPN. The important thing is that IT administrators can utilize centralized management services to implement policies, configure network elements, monitor behavior, and audit activity. Centralized management is extremely important as it can make NAC efforts scaleable, efficient, and measurable.
- **Scale to meet future needs.** Most NAC implementations start small (a primary reason why there are so many tactical NAC tools) and grow over time. While short term goals are certainly important, NAC must be built for longer term strategic needs.

Think in terms of multiple devices per user, loads of IP application traffic, and granular network authorization enforcement.

- **Provide consistency across any user account, device, or network.** To satisfy NAC requirements without burdening users, NAC must be both ubiquitous and transparent. What does this mean? A common endpoint health policy should be consistent regardless of whether the CFO or a junior administrator signs on to the network. Business rules should be enforceable whether a sales manager logs on using a laptop or an iPhone. Finally, the access experience should be the same whether a user is on a wired desktop, connecting over a wireless AP, or logging on remotely over an SSL VPN.

In this context, NAC should be viewed as an enabling enterprise business technology. This should not be interpreted as “big,” “overbearing,” or “excessively expensive.” NAC doesn’t have to be any of these things as it can be built iteratively in phases over time. Nevertheless, NAC absolutely can not be an independent island. NAC must be integrated with existing business rules, security policies and IT infrastructure for it to reach its true potential.

Table 2. NAC Must Be an Enterprise Initiative

Enterprise NAC Requirement	IT Benefits	Business Benefits
Fit in with existing desktop, network, and security infrastructure	Enables IT to “start small and grow” while building an end-to-end solution	Accelerates business initiatives
Provide for flexible implementation and enforcement	IT is able to react to changing business needs while avoiding the need for new equipment or custom solutions	Business managers can be more creative and experimental knowing that IT can respond to changing needs
Support centralized policy and configuration management	Lower cost of operations and more responsive change management	Aside from speed of implementation, IT can provide better metrics to business manager
Scale to meet future needs	IT can be more responsive to new technologies and business opportunities	Business managers can be more creative and experimental knowing that IT can respond to changing needs
Provide consistency across users, devices, and networks	Policies can be configured once and then enforced across the network infrastructure	Users are provided consistent network access based upon business and security policies, not technology limitations

NAC Implementation Recommendations

Getting the most out of NAC will require lots of planning, testing, and piloting before a full enterprise deployment. This requires a phased approach to NAC implantation that adds incremental value, security, and business flexibility over time. Knowing which pieces of NAC are important, where to start, and how to phase in NAC functionality over time are important parameters toward long term success. ESG recommends that CIOs:

- **Map business requirements to network capabilities.** Who needs access to which network resources? What is the definition of a “healthy” endpoint device? What happens when a device is considered to be out of compliance? These fundamental business and technology questions need to be answered before beginning ANY technology implementation. CIOs should have a firm understanding of their network, desktop and security assets before meeting with business executives to hammer out these policy questions and start building NAC implementation plans.
- **Choose a high value starting point.** Based upon several surveys of security professionals combined with four years of anecdotal evidence, ESG believes that overarching initial projects are often the demise of NAC initiatives. As mentioned before, large organizations should approach NAC with a “start small and grow” mentality by picking a starting point that can reduce risk and deliver immediate value. Many firms choose a specific area of concern like checking the integrity of remote worker PCs or creating stringent guest access policies. Mastering a finite area of NAC will make the next stages of implementation more efficient and productive.
- **Increase functionality over time.** NAC can be completely passive at first, used only to assess and report on endpoint health status. Over time, policy enforcement and remediation can be eased into the process as users and IT get used to NAC in their day-to-day routine. The ultimate NAC goal should be extremely tight policy enforcement. Endpoint configurations should have little variability. Users of non-compliant devices should be guided to intuitive remediation services. Once devices gain network access they should be tightly restricted to assets needed for their job and nothing else and all activities should be closely monitored and audited.
- **Keep an eye on other initiatives along the way.** NAC should never be done in a vacuum, rather network access policies must be integrated into business and IT decisions. Living by this rule will help companies get the most out of their network whether they are adding IP telephony systems, building massive collaboration applications, or complying with new federal government privacy regulations.

While NAC is often equated with security, ESG believes that it should actually be looked at as an intelligent network services embedded in the communications fabric itself. When NAC is deployed as an integral part of the network infrastructure, it adds access control, endpoint health, and authorization to network segmentation, layered security, and traffic management. This combination can provide coordinated policy based management over an enterprise matrix of any endpoint device, IP-based application, and security event (see Table 3).

Table 3. NAC As Part Of The Network Infrastructure

Network Infrastructure Service	NAC Contribution	Benefits of NAC integration into the network infrastructure
Network segmentation	Combines device and user identity with network segmentation services	Can assign a user or device to a VLAN based upon device type, user identity, or network location
Layered security	Combines NAC health check with network firewalls, IDS, and IPS	Pre-admission health checks combined with post admission network threat detection
Traffic management	Combines identity with ACLs and QoS	NAC identity can trigger network authorization, bandwidth throttling, or traffic prioritization

Nortel Is Taking NAC to Enterprise Networks

Even elite IT enterprises won't deploy full NAC capabilities overnight. Rather, they will ease NAC into the enterprise over time by plugging existing vulnerabilities and then adding functionality through implementation phases. Unfortunately, few vendors offer a portfolio of solutions that can address short-term pain points and longer-term business needs.

One exception to this rule is Nortel. Nortel offers its Nortel Secure Network Access (NSNA), an end-to-end portfolio of products and services for endpoint authentication, health checking, network threat assessment, network authorization, quarantine, and remediation. What's more, NSNA can be integrated into the core Nortel network fabric for enhanced value for any user, any device, on any network. With NSNA Nortel provides:

- **A number of starter solutions.** Nortel recognizes that NAC will grow through a phased implementation over time so NSNA can be implemented flexibly and gradually. For example, Nortel offers a stand-alone NAC appliance that integrates into NSNA and can add incremental future value. NSNA appliances can be easily implemented to provide security guest access in conference rooms a common initial implementation model. Over time, NSNA can be extended to internal users through the implementation of Tunnel Guard agents, Nortel Threat Protection, and other infrastructure components. NSNA is a refreshing change from other vendors that require customers to either to rip and replace network infrastructure components or implement appliance solutions that are incompatible with overall NAC architecture.
- **A multitude of NAC enforcement options that extend to layered network security.** NSNA works with agent and agentless clients. Through its Tunnel Guard agent, NSNA meets enterprise scalability and mobility requirements by enforcing common NAC policies across a range of technology options including 802.1X, Ethernet switches (i.e. port blocking, ACLs, bandwidth management, etc.), VLANs, and DHCP. NSNA is also integrated with Nortel Threat Protection to form a defense-in-depth security architecture. Nortel Threat Protection complements NAC by providing post admission security support. If a "healthy" endpoint becomes infected after gaining

network access, Nortel Threat Protection can detect the problem and take immediate actions for quarantine and remediation.

- **Tight integration with IP telephony.** Nortel's strength in voice and data communications is certainly evident here. Nortel 802.1X-enabled IP phones can be authenticated for security while NSNA helps to scale the network by allowing multiple devices to connect to the network over a single Ethernet port. Once authenticated, NSNA places the IP phone in an IP telephony VLAN easing configuration issues for telephony services and even E911. IP telephony VLANs can be instrumented with special ACLs for security and QoS. In this way, NSNA combines NAC benefits with network automation and service management around specific application and traffic.

NSNA is also built with an eye toward future technology changes and industry support. How? NSNA adheres to the Trusted Computing Group (TCG) Trusted Network Connect (TNC) specifications so customers won't be locked into a proprietary architecture (note: Nortel is a contributing member of the TNC and has been working with TNC to draft a requirements document for the IETF Network Endpoint Assessment (NEA) specification). NSNA is not tied to a single subset of antivirus software, personal firewalls, or security applications. Large organizations can customize NSNA to fit their needs across facilities and global locations. NSNA supports third party and legacy Nortel switches to maximize investment protection. Finally, Nortel has a close working relationship with Microsoft and its upcoming Network Access Protection (NAP) technologies. This will be especially important as large organizations upgrade to Vista desktops and Windows Server 2008 (aka Longhorn).

With NSNA, Nortel is demonstrating a keen understanding of enterprise NAC requirements and market realities. NSNA is not overwhelming; rather it can be implemented gracefully over time. Nortel also recognizes that it is not the only NAC "game in town" so it built NSNA to play nicely with others. Finally, Nortel is preparing for the long haul with an NSNA roadmap that extends well into the future.

Clearly NSNA puts Nortel into a small group of top-notch NAC vendors. As such, CIOs should certainly consider speaking with Nortel as part of their NAC planning and vendor selection effort.

Further information on NSNA can be found here: <http://www.nortel.com/snas4050/>

The Bottom Line

It's time to recognize NAC is more than just network access control. NAC is actually a way to add identity into networks making them more productive, secure, and agile for the business.

To maximize the benefits of NAC, CIOs will need to drop their tactical IT-focused mindset and think in terms of a strategic enterprise deployment over time. This should be done by integrating NAC into the existing infrastructure, demanding centralized policy/configuration management, adhering to open standards, and slowly scaling NAC policies, enforcement, and scope over time. NAC should also be viewed as a network service rather than a stand-alone initiative. As such, NAC delivers superior results when it is embedded in the network infrastructure fabric as a counterpart to network segmentation, layered security, and traffic management. When considered in this context, Nortel can be seen as one of few leading vendors.

No, it won't be easy, but ESG believes a phased and intelligent NAC implementation can deliver real value. Smart CIOs should begin a strategic enterprise NAC journey without further hesitation.