

OUTSIDE IN

Novell's Remote Access

by
Linda
Kennard

Solution

Nearly four years ago, Novell IS&T set up a handful of access servers to provide a bigger handful of remote and mobile employees access to the corporate network. To gain this access, employees dialed in to the access servers—initially using a telephone number local to Provo, Utah, and later using a toll-free number. These access servers then passed the employees' authentication information to a BorderManager Authentication Services server using the Remote Authentication Dial-In User Service (RADIUS) protocol. (See Figure 1 on p. 8.)

Assuming that BorderManager Authentication Services cleared the request for authentication, employees gained access to the corporate network. From within Novell's network, employees could access corporate applications and data and read and respond to their e-mail messages. Employees could also access the Internet from the corporate network, enabling them to surf the web.

The problem was that whatever employees downloaded and uploaded or checked and read while on the toll-free line, they did so oblivious to cost. Without a system for billing employees' departments for time spent on the toll-free line, Novell IS&T alone saw and paid the bill for remote access.

News of the convenience of corporate network (plus e-mail and Internet) access over a toll-free line spread faster—and costs climbed higher—than Novell IS&T had anticipated. Admittedly, for remote and mobile employees, the toll-free number was great: This seeming free door to the corporate network enabled them to download the files they needed from anywhere they were within the United States and Canada.

For Novell, however, widespread use of the toll-free number was less than great. Contrary to what many employees seemed to think (and, in their defense, what the word toll-free implies), the toll-free line was not free. Novell was paying for every minute that every one of its employees spent on that line, and remote access costs were getting out of control.

About this time, another problem surfaced. Employees started calling the help desk, excited to report that they had a 1 Mbps or faster connection to the Internet via a Digital Subscriber Line (DSL) or cable modem. These employees called to ask how to use this speedy new connection to access the corporate network and were disappointed to learn that they couldn't. The access servers



supported only dial-up connections from the comparatively sluggish 56 kbps (or slower) modems, and these access servers together represented the single "In" door to Novell's network.

Of course, the majority of Novell employees still had the necessary (albeit slow) equipment, but that equipment didn't guarantee access to the corporate network: For employees who travelled or lived outside the United States and Canada, the toll-free line was unusable. These employees had to pay and request reimbursement for the costly and not-always-reliable toll lines they used to dial in to the Provo-based access servers from across the globe.

Novell needed a new approach to remote access. It needed a solution that could provide access to the corporate network regardless of where employees were or how they connected to the Internet. This solution would have to be easy enough to use for all of Novell's employees—not just the technically sophisticated.

Naturally, Novell demanded a secure solution—one that would ensure that whatever employees were uploading to or downloading from the corporate network would be for their eyes only. Equally important, Novell needed a remote access solution that cost less than the small fortune that it was spending.

THE NOMAD-IC SOLUTION

Novell IS&T met these challenges with a new remote access solution that it started rolling out in pieces two years ago. To come up with a name for this improved approach to remote access, Novell IS&T held a contest within its own department. "The winning name," explains Novell IS&T engineer Lynn Crabb, "was NOMAD, which we later decided should stand for Novell Mobile Access Delivery." Crabb is quick to point out that NOMAD is strictly an internal name for Novell's internal approach to remote access. This umbrella term covers the global Internet Service Provider (ISP) services and all of the Net services software that Novell IS&T has deployed to enable remote access.

Visit our advertiser, Novell eProvisioning, at
www.novell.com/e provisioning

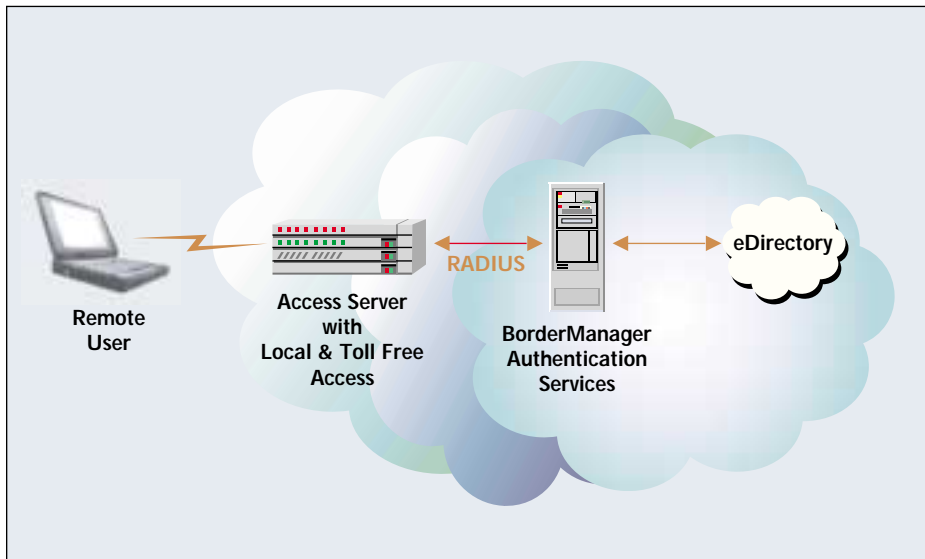


Figure 1. Before NOMAD, Novell employees could access the corporate network only by dialing a local or toll-free number to reach Novell's access servers. This approach to remote access was costly for Novell and sometimes inconvenient for employees, who could use the toll-free number only within North America.

Going Global Without Going Broke

Novell IS&T decided to use a global ISP to solve the toll-free number dilemma—a decision that turned out to be a stroke of genius. Novell IS&T had already determined that a toll-free number was too expensive and too limited, providing access only to employees who had analog modems and were within the United States and Canada.

However, avoiding this expense by setting up local access points at every location from which employees would require access was both costly and impractical. After all, Novell's mobile employees travel from one end of the globe to the other. These "nomads" try to access the corporate network from anywhere: Australia, Venezuela, Finland, Norway, Singapore, Thailand—you name the country, and Novell's wandering workforce has probably been there.

To provide access to the corporate network from virtually anywhere without incurring atrocious toll-free or long-distance fees, Novell contracted with UUNET, a WorldCom company. This leader in Internet communications solutions owns and operates a global network with points of presence (POPs) in thousands of cities throughout North America, South America, Europe, Africa, and Asia Pacific. (For more information, visit www.uu.net.) Along with its gateway partners, UUNET provides the POPs that enable Novell employees to access the Internet from

virtually anywhere in the world using, in many cases, a local telephone number.

Naturally, UUNET is not the sole secret to the success of Novell's remote access solution. Instead, UUNET represents only a convenient and frequently best-cost option for Internet access that Novell IS&T has made available for Novell's remote and mobile employees.

Net Services Software

Another part of NOMAD's secret to success is Novell's Net services software, including Novell Modular Authentication Services (NMAS) 2.0 and BorderManager VPN Services 3.6. (These were the versions in use at the time this article was written. As new versions of these and other products are made available, Novell IS&T upgrades accordingly.)

Essentially, NMAS 2.0 helps Novell employees authenticate to Novell's eDirectory tree using the RADIUS packets received from UUNET servers. (For more information, see the "Minimizing Administrative Overhead" section on p. 10.) NMAS 2.0 thus helps Novell employees get on the Internet by way of Novell's UUNET account.

Of course, Novell remote and mobile employees didn't need Internet access first and foremost; what they needed above all else was convenient access to the corporate network. Enter BorderManager VPN Services 3.6, which enables Novell employees to access the corporate

network from the Internet, regardless of how they connect to the Internet. (For more information, see the "Simple, Secure, Convenient" section on p. 16.)

As Net services software, NMAS 2.0 and BorderManager VPN Services 3.6 are supported, from their foundation up, by eDirectory. Named directory product of the year by Network Magazine, eDirectory is the only directory on the market that runs on all major operating systems including NetWare, Solaris OE, Windows 2000/NT, Linux, Compaq Tru64, UNIX, and soon IBM AIX. In addition to being cross-platform, eDirectory is the most scalable directory available, enabling you to create directory trees that hold up to one billion objects. (For more information about Network Magazine's Products of the Year awards, see www.networkmagazine.com/article/NMG20010413S0005.)

Of course, the fact that eDirectory is multiplatform and scalable sounds great, but what does it mean in this NOMAD-ic context? Basically, eDirectory does for NOMAD what eDirectory does for any networking solution: eDirectory simplifies the complexity of managing users and resources. For example, because Net services software and, consequently, NOMAD are based on eDirectory, Novell IS&T can manage the software underpinnings for Novell's remote access solution from a single, central location.

The Net Result

As Novell demanded and Novell IS&T intended, NOMAD's combination of global ISP services and Novell Net services software enables employees to access corporate data from virtually anywhere in the world. Access to corporate data via NOMAD is simple, fast, and secure.

Also, as Novell hoped and Novell IS&T planned, NOMAD saves Novell a lot of money. In fact, Novell's remote access costs are lower than ever, despite the fact that remote use of its corporate network has significantly increased over the last 2 1/2 years. Prior to NOMAD, Novell spent approximately U.S. \$1.2 million per year on remote access costs. NOMAD has reduced these costs by 70 percent or more.

NOVELL'S SOLUTION IS YOUR SOLUTION

Why should you care that Novell has saved money on an internal solution to its own remote access problem? You

Visit our advertiser, Alexander LAN, at
www.AlexanderLAN.com



Figure 2. When Novell employees launch the NOMAD dialer, it returns a login screen similar to this screen. Unlike this screen, however, Novell employees now log in to NOMAD using their common eDirectory name.

should care because NOMAD is a private but real-life example of what will soon be a public solution: Novell Remote Access. (For more information, see “NOMAD and One Net” on p. 12.)

Available through Novell Sales and Consulting in early 2002, Novell Remote Access “piggy backs off of NOMAD,” says Novell product marketing manager Sherry Bushonville. In other words, NOMAD is basically the prototype for Novell Remote Access. Novell solved its own remote access problem and used its solution to develop a marketable solution for you. As a result, Novell can offer you a complete remote access solution that’s been tested and perfected. (For more information, see “Novell Remote Access” on p. 14.)

As a result, your company could soon be experiencing the same 70 percent or more savings that Novell has realized. You decide: Read how NOMAD works for Novell, and you will be in a position to understand how Novell Remote Access, NOMAD’s progeny, might work for you.

THE ORDER OF ACCESS

The NOMAD-ic concept is simple. The idea is to enable employees to access corporate data no matter how they connect to the Internet and no matter where they are.

Although Novell employees could theoretically access corporate data in dif-

ferent ways, Novell IS&T was determined to keep things simple. To that end, Novell IS&T engineers set up NOMAD such that the service requires two steps that employees always follow in this order:

1. Connect to the Internet.
2. Access the corporate network.

STEP 1: CONNECT TO THE INTERNET

NOMAD does not dictate how Novell employees should access the Internet. Novell employees can access the corporate network (using BorderManager VPN Services) regardless of their method of Internet access—whether it be by way of a 56 kbps, DSL, cable modem, or an Integrated Services Digital Network (ISDN) line. Novell employees may access the Internet using the ISP and method of their choice.

This level of flexibility “fits into our model,” says Crabb. “As long as [employees] choose an access method that’s cost-effective for the company, we don’t really care how they get on.”

However, NOMAD does offer employees the option of accessing the Internet by way of Novell’s UUNET account. To connect to the Internet using NOMAD’s UUNET option, Novell employees need the NOMAD dialer.

The NOMAD dialer is a combination dialer and phone book that simplifies the process of connecting to the Internet. Novell employees can download the NOMAD dialer from the Novell corporate portal (i-Login.net) or from the web site that Novell IS&T created specifically for NOMAD. (As you would expect, Novell makes the NOMAD web site available only to Novell employees.)

After employees download and install the NOMAD dialer, they have a new icon on their desktop. Employees simply double-click this icon to launch the NOMAD dialer, after which they are prompted to log in. (See Figure 2.)

Minimizing Administrative Overhead

To log in to NOMAD or, more specifically, to UUNET via Novell’s account, Novell employees enter their eDirectory username and password. At the time this article was written, employees entered a leading period followed by their complete eDirectory username and context in the Username field. This process will be different by the time you read this article.

As part of its i-Login initiative, Novell IS&T created an eDirectory tree specifi-

cally for authentication purposes. Novell IS&T then used DirXML to link this authentication tree to Novell’s primary eDirectory tree, the Novell—Inc tree. (Just for the record, Novell IS&T has used DirXML to link most of the network directories, applications, and databases on Novell’s network. For more information, see “i-Login: It’s One Net Live From Novell,” *Novell Connection*, Dec. 2000, pp. 6–20. You can download this article from www.ncmag.com/past/.)

This authentication tree has a flat structure that basically includes a Novell Organization container holding only User objects replete with usernames and passwords. The authentication tree speeds authentication by placing all users in one context. This structure eliminates the former need to proxy requests for authentication to various locations based on employees’ eDirectory contexts. The authentication tree also simplifies authentication by enabling employees to log in to NOMAD using their common eDirectory name, such as lkennard.

The first time employees use the NOMAD dialer, they type @novell.com after their common eDirectory name (for example, lkennard@novell.com). Ever after, the dialer remembers this addition, so employees don’t need to enter it again.

When a UUNET (or partner) server detects a Novell username, that server knows where to proxy that request. Using RADIUS, the UUNET (or partner) server forwards this request for authentication to one of NOMAD’s four NMAS 2.0 servers. These servers are physically located within Novell’s corporate network on a rack of about 20 Compaq DL360 servers running NetWare 5.1. (Incidentally, Compaq is Novell’s corporate standard for server hardware.) Novell IS&T will soon upgrade these servers to NetWare 6.

NMAS 2.0 is an authentication service that enables you to centrally manage multiple authentication methods across your network. The authentication modules included with and available for NMAS 2.0 enable login methods based on users submitting something they know (for example, a password), something they have (for example, a smart card), or something they are (for example, a fingerprint).

After you have installed these authentication modules, you can create company-wide authentication policies. Each of these policies indicates a login sequence you will require for authenticating to eDirectory

Visit our advertiser, ACCPAC, at www.faxserve.com

and accessing the network or specific services (such as voice mail). These login sequences may include one or more of the login methods NMAS 2.0 supports.

NMAS 2.0 also supports graded authentication. To set up graded authentication, you create a security policy that grants users access to various resources based on the strength and combination of the login methods they use. (For more information, see "NMAS: It's What Spy Movies Are Made Of," *Novell Connection*, Feb. 2000, pp. 6–21. You can download this article from www.ncmag.com/past. You can also visit Novell's web site at www.novell.com/products/nmas.)

What is more important in this NOMAD-ic context is that NMAS 2.0 includes a RADIUS server. The NMAS 2.0 RADIUS servers enable Novell IS&T to use UUNET services without compromising Novell security.

In the NOMAD-ic solution, the NMAS 2.0 RADIUS servers act essentially like a gateway between UUNET servers and Novell's eDirectory tree. (See Figure 3 on p. 16.) That is, armed with the authentication information from UUNET, NOMAD's NMAS 2.0 servers authenticate Novell employees against Novell's eDirectory tree. Using RADIUS, the NMAS 2.0 servers then return a thumbs up or thumbs down, to accept or reject the authentication requests for access to the Internet on Novell's UUNET account.

Hence, instead of Novell's own access servers sending NMAS 2.0 the authentication requests, UUNET (and its partners) forwards that information. The fact that NMAS 2.0 and UUNET (and partner) servers can exchange authentication information means that Novell IS&T does not have to worry about a separate and remote list of Novell employees on the UUNET network.

If NMAS 2.0 did not support RADIUS and was unable to exchange authentication information with UUNET (and partner) servers, Novell IS&T would have an administrative nightmare: Each time someone joined or left Novell, Novell IS&T would have to contact UUNET to ask them to make the appropriate change. Such a process would be inconvenient at best. New employees may have to wait for Internet access, and departing employees may have time to continue surfing the web on Novell's account.

Not unlike you and your company's IS&T department, Novell IS&T strives to minimize administrative overhead. The exchange of authentication information between UUNET and NMAS 2.0 servers means that from the moment a new Novell employee has an account in eDirectory, he or she also has Internet access. It also means that from the moment an employee's eDirectory account is deleted, that employee loses Internet access via Novell's account with UUNET.

From PAP to CHAP

For remote access authentication purposes, UUNET supports two authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). The essential difference between PAP and CHAP is that PAP sends usernames and passwords from client to server in the clear—that is, unencrypted. CHAP encrypts usernames and passwords before transmitting them.

Until recently, Novell took advantage of UUNET's support for PAP because CHAP poses a technical hurdle that, by the time you read this, Novell IS&T will have cleared (or will soon clear). The problem with CHAP is that its hashed version of a user's password is different than the hashed version of a user's password that is stored in eDirectory. When NMAS 2.0 tries to authenticate a user against eDirectory, the CHAP password does not match the version of that password stored in eDirectory, so the user cannot be authenticated.

To solve this problem with CHAP, Novell IS&T developed a new authentication module for NMAS 2.0 that supports employees logging in to UUNET using a Personal Identification Number (PIN) in lieu of their eDirectory password. NMAS 2.0 stores this PIN encrypted within eDirectory but is able to extract and unencrypt the PIN. After the PIN is unencrypted, NMAS 2.0 can then create a hash of the PIN that should match the hashed PIN that UUNET sends.

In very general terms, the process works like this: UUNET passes a hashed version of an employee's PIN to an NMAS 2.0 server. The RADIUS NetWare Loadable Module (NLM) on this server makes a call to NMAS 2.0, requesting the PIN from eDirectory.

NMAS 2.0 extracts the encrypted PIN from eDirectory, unencrypts it, and then creates a hash of the unencrypted PIN. NMAS 2.0 then passes the hashed PIN back to the RADIUS NLM. The RADIUS NLM compares this NMAS-hashed version of the PIN with the PIN that UUNET sent. If the two match, the employee is cleared for access.

Using a PIN to access the UUNET network rather than using eDirectory passwords also better protects Novell's network. Granted, if someone were to discover a Novell employee's PIN, that person would be able to access the Internet

NOMAD and One Net

NOMAD is part of what Novell calls its i-Login initiative. The i-Login initiative is Novell's attempt to put its own network where its one Net vision is—and to pave the way for you to do the same.

As you may know, the one Net model defines a networking environment that blurs the boundaries between public and private networks. With their boundaries blurred, these networks converge into a single global network, enabling IT professionals like you to more effectively manage and secure all of your company's resources. (For more information about one Net, see www.novell.com/news/onenet.)

With the i-Login initiative, Novell identifies its own problems—problems Novell believes are not unlike your company's problems. Members of Novell IS&T then work with Novell Engineering to develop

and internally deploy solutions to these problems.

As a natural result, Novell's corporate office becomes, in effect, a live testing environment. Novell tests and perfects its solution and, ultimately, makes that solution available to you. (For more information on the i-Login initiative, see "i-Login: It's One Net Live From Novell," *Novell Connection*, Dec. 2000, pp. 6–20. You can download this article from www.ncmag.com/past.)

As part of the i-Login initiative, NOMAD contributes to Novell's one Net, blurring boundaries between the Internet and Novell's corporate network by simplifying, accelerating, and securing access to that network. More important, as part of the i-Login initiative, NOMAD from the outset was slated to be tested, perfected, and made available to you as Novell Remote Access. ●

Visit our advertiser, Novell's NetWare 6, at
www.novell.com/NetWare6

Novell Remote Access

Novell Mobile Access Delivery (NOMAD) is a real-life example of a new Novell solution: Novell Remote Access, which will be available through Novell Sales and Consulting beginning early 2002. Novell Remote Access enables your company's remote and mobile employees to access your company's corporate network from anywhere, at any time, for the lowest possible cost.

Novell Remote Access features all of the Novell Net services software that NOMAD features, including the latest versions of eDirectory, DirXML, Novell Modular Authentication Services (NMAS), and BorderManager VPN Services. In the future, Novell Remote Access will include additional Net services software that will enable wireless remote access.

Novell Remote Access combines Net services software with the services of a global Internet Service Provider (ISP) to ensure that your company's employees have Internet access from wherever they are. Novell Remote Access includes a custom dialer, which employees use to dial either your company's own access servers or the global ISP's points of presence (POPs), typically using a local number. Once connected to the Internet, your employees access your corporate network by using BorderManager VPN Services.

While you use global ISP services, you—not the ISP—maintain your own list of the users who are authorized to access the Internet on your company's account. Novell consultants configure NMAS servers on your network to accept authentication data that the global ISP forwards via the Remote Authentication Dial-In User Service (RADIUS) protocol. NMAS, in turn, authenticates employees against your company's eDirectory tree. Using RADIUS, NMAS then reports whether this employee is permitted or denied access to the Internet on your company's account.

Maintaining your own list of authorized users in your company's eDirectory tree is both more efficient and more secure than attempting to regularly update a separate list maintained by the ISP. For example, because NMAS authenticates remote employees against your company's eDirectory tree, they gain or lose access to

the Internet on your company's account from the moment you create or delete their eDirectory account. In addition, because maintaining your own list of authorized users requires fewer administrative tasks, you save time, and your company saves money.

Novell Remote Access includes a tutorial program that explains to your employees how to use both the custom dialer and the BorderManager VPN Services client software. Among other things, the tutorial program encourages employees to choose one of your company's own access numbers to dial in to the Internet. If such a number is unavailable, the tutorial suggests choosing the nearest global ISP POP.

In this way, the tutorial tries to make employees aware of—and thus reduce—remote access costs. Novell consultants can also help you configure Novell Remote Access to capture accounting information, which you can use to bill employees' departments for the remote access costs these employees incur.

Like NOMAD, Novell Remote Access thus helps simplify, accelerate, and secure remote access to your corporate network for the lowest possible cost. Through its unique approach to the remote access problem, the Novell Remote Access solution offers benefits that include (but are not limited to) the following:

- Reduced monthly remote access costs due to the following:
 - Use of the Internet rather than dedicated lines
 - Elimination of unnecessary modem banks
 - User awareness
- Reduced administrative costs
- Reduced risk of nonproductivity (because users can easily access the data they need from anywhere and at any time)

In addition, because Novell Remote Access is available through a single provider, it is easy to use, centrally managed, and convenient for your company, for your company's users, and for you, the network administrator. Simply put, Novell Remote Access is designed to "make you happy," says Novell product marketing manager Sherry Bushonville. ●

on Novell's account. However, that person would be unable to access Novell's corporate network, which would remain protected from unauthorized users.

Who You Gonna Call?

After Novell employees have entered their authentication information and before they have clicked to connect, they must select the phone number. (Incidentally, the precise steps an employee should take are explained in the Connection Status field on the login screen.) To select a phone number, Novell employees click the Properties button and, from that screen, click Phone Book.

The Phone Book screen prompts Novell employees to enter the type of service they are using to connect to the Internet (that is, modem or ISDN). (See Figure 4 on p. 20.) The Phone Book

screen also prompts employees to enter the country or region from which they're calling and, when applicable, the state or province. The NOMAD dialer then searches for and returns a list of phone numbers that Novell employees can dial given their current location.

NOMAD's phone book may return the following types of access numbers:

- Novell office numbers
- UUNET POP numbers
- UUNET toll-free (also called *freephone*) numbers
- UUNET gateway partners' toll-free numbers

Decisions, Decisions

Novell employees decide which of the displayed numbers they want to dial. They base this decision on which number is the

least expensive. To determine which number is least expensive, employees use common sense and a little math.

Common sense dictates that the least expensive approach, of course, is to dial a local Novell office number. Dialing a local number eliminates toll charges, and because Novell owns and operates the access servers, there is no charge for the access service. Consequently, if a Novell employee is in Provo, Utah, using the server's local Provo number to dial in to Novell's access server is clearly the best choice.

When Novell employees are not in the Provo area, they have to choose the next best option. Generally speaking, the next best option is to call a local UUNET POP. Dialing a local UUNET POP again eliminates toll charges and incurs only the charge for the use of the UUNET POP. In the vast majority of cases, the charge for

using a local UUNET POP is much less expensive than a long-distance call to a Novell office.

Of course, Novell employees may not always have the luxury of dialing a local number. When Novell employees are not conveniently located within local range of a Novell office or UUNET POP, the choices get a bit more complicated. Novell IS&T recommends that Novell employees consider the following options, usually (but not necessarily) in this order:

- Dial a toll-free UUNET (or UUNET partner) POP
- Make a toll call to a Novell office
- Make a toll call to a UUNET POP

As you would expect, dialing a UUNET (or UUNET partner) POP toll-free number costs a bit more than dialing a local UUNET POP. Nevertheless, the cost of dialing a UUNET (or partner) toll-free number is generally better than the price of a long-distance call to a Novell office or a remote UUNET POP. However, which of these options is best in each particular case depends on the "byzantine pricing structure of your local phone company," the *NOMAD User's Guide* explains.

Although Novell employees know or can learn the cost per minute of a long-distance call, how do they know how much UUNET and its partners charge for the use of POPs in various locations? Novell employees can determine how much UUNET and its partners charge per minute (and per hour) by consulting *NOMAD's Rate Table*. Novell IS&T created this Rate Table along with guidelines on how to decide which approach is the best-cost approach in any given circumstance.

Awareness Is Bliss

Of course, Novell employees may decide that using their own ISP and then submitting requests for reimbursement is the least expensive—and easiest—approach of all. In the end, Novell and Novell IS&T don't care how employees get on the Internet, says Crabb. "What we care about is that they're aware of the costs. As long as there's [employee] awareness, everybody's happy," he adds.

If you're wondering why Novell employees would bother to choose the least expensive option, the answer is because the *NOMAD-ic* solution holds employees accountable for the time they spend online. At the time this article was written,

the accounting procedure Novell IS&T was using to bill employees' departments was a bit cumbersome.

Basically, a member of the Novell IS&T department would download accounting information from UUNET. Next, this Novell IS&T member would run an in-house-developed script that was designed to parse relevant data from the UUNET accounting information. The relevant data included employees' usernames and the location, time, and cost of employees' sessions. The Novell IS&T member would then match each session with the employees' cost centers and send bills to employees and their managers. The system worked but was less than ideal and "not duplicatable," says Crabb.

By the time this article goes to press, Novell will be taking an approach to accounting that is both more sophisticated and more practical. Rather than waiting for and downloading accounting information from UUNET, Novell IS&T will use the RADIUS accounting capabilities on its own NMAS 2.0 servers. For each remote access session, the NMAS 2.0 RA-

DIUS server can track and record the employees' username as well as the session time and the number dialed to and from. However, the NMAS 2.0 RADIUS server cannot determine the cost of each session.

As you can guess, the cost of a session depends not only on the session's length, but also on UUNET costs for a given area and on the type of call (local or toll-free). For example, dialing a UUNET POP within the U.S. costs considerably less than dialing a UUNET POP in Belgium.

To determine cost, Novell IS&T will transfer the RADIUS accounting information from their own NMAS 2.0 servers to an Oracle database. Novell IS&T has designed the tables within this database to determine and apply the appropriate UUNET charge.

Employees will soon be able to access reports generated from this Oracle database from Novell's corporate portal, *i-Login.net*. The idea is to heighten employees' awareness of—and hold them accountable for—their remote access costs. Employee awareness and accountability, Novell believes, help reduce costs.

Visit our advertiser,
Biscom, at
www.biscom.com

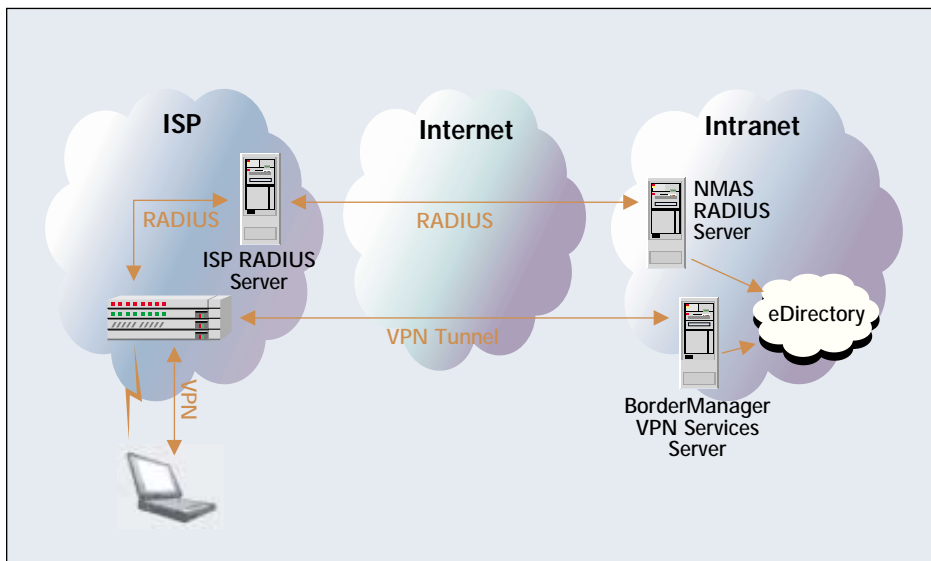


Figure 3. The NOMAD-ic concept is simple and involves only two steps: Connect to the Internet and connect to the corporate network. Employees can connect to the Internet using the ISP and access method of their choice, or they can connect to the Internet on Novell's UUNET account by way of NMAS 2.0 RADIUS servers. Once on the Internet, employees connect to the corporate network using BorderManager VPN Services 3.6.

STEP 2: ACCESS THE CORPORATE NETWORK

When employees select a number for a UUNET (or partner) POP and their authentication information clears, the NOMAD dialer connects them to the Internet—not to the corporate network. Using a browser, employees can then access a few corporate services, such as Group-Wise WebAccess.

Of course, Internet access to a few services cannot compare to the full-fledged network services employees can get when they're actually in the office. (Through its i-Login.net portal, Novell is resolving this problem and working toward achieving a concept it calls the Internet Office. Ultimately, the Internet Office will enable full access to corporate services using nothing more than a browser.) For now, to gain full access to Novell's corporate network from the Internet—regardless of the ISP, modem, or line used to establish the Internet connection—Novell employees use BorderManager VPN Services 3.6.

BorderManager VPN Services 3.6 is a secure, remote connectivity system that enables users to create virtual private networks (VPNs)—as its name clearly suggests. VPNs are encrypted tunnels that pass through the Internet or other public backbones. Each BorderManager VPN Services 3.6 server can support up to 1,000 simultaneous client VPNs over IP.

BorderManager VPN Services 3.6 creates these VPNs using a variety of encryption algorithms, including the following:

- Data Encryption Standard (DES)
- 3DES
- Internet Protocol Security (IPSEC)
- RC2
- RC5
- SKIP

In addition, BorderManager VPN Services 3.6 uses 128-bit encryption whenever doing so is allowed.

BorderManager VPN Services 3.6 enables users to access their corporate network securely regardless of their Internet connection. To be more specific, BorderManager VPN Services 3.6 supports access to corporate network resources via analog, cable, or DSL modems. What is more, BorderManager VPN Services 3.6 can establish a VPN despite an ISP's use of Network Address Translation (NAT), which typically negates the possibility of creating VPNs. (For more information about BorderManager Services 3.6, visit Novell's web site at www.novell.com/products/bordermanager/vpns.)

BorderManager VPN Services 3.6 can be configured to dial a corporate network directly. However, Novell IS&T deployed its BorderManager VPN Services 3.6 clients as LAN-based clients, which means the clients do not dial the network. In-

stead, employees first dial in to the Internet and then access the network through the LAN-based VPN client. This choice supported Novell IS&T's philosophy regarding simplicity: "We wanted [NOMAD's] sequence of steps for accessing the network to be consistent regardless of whether [employees] dial in, use a cable modem, or use an Ethernet network."

Simple, Secure, Convenient

Novell employees can download the BorderManager VPN Services 3.6 client software from i-Login.net or from the NOMAD web site, as they can with the NOMAD dialer. After employees download and install the BorderManager VPN Services 3.6 client software, an icon appears on their desktop. Employees simply double-click the icon to launch the program.

When employees launch the BorderManager VPN Services 3.6 client software, they see the Novell VPN login screen. This screen prompts employees to enter their eDirectory username, password, and context, along with the IP address for one of Novell's two BorderManager VPN Services 3.6 servers. (Employees can find these IP addresses in the *NOMAD User's Guide*.) As with all Novell servers, these BorderManager VPN Services 3.6 servers run on Compaq hardware, in this case Compaq DL360s.

After completing the screen's fields, employees click OK. The first time an employee connects with either of the BorderManager VPN Services 3.6 servers, this server returns some authentication data. (This data looks like a couple of lines of paired numbers and letters.) This authentication data helps employees confirm that they are connecting with an authorized NOMAD BorderManager VPN Services 3.6 server.

Employees need only authenticate this data once for each server. When employees click OK to connect again to the same server, this server does not return the authentication data. Instead, the server authenticates employees against Novell's eDirectory tree. Assuming these employees have the proper credentials and the necessary rights, the server then connects them directly to Novell's network.

At this point, employees have complete access to the corporate network. They can browse InnerWeb (Novell's

Visit our advertiser, Test Out, at
www.testout.com

**Visit our advertiser, Novell eDirectory
Development Partners, at www.novell.com/solutions**

**Visit our advertiser, Novell eDirectory
Development Partners, at www.novell.com/solutions**

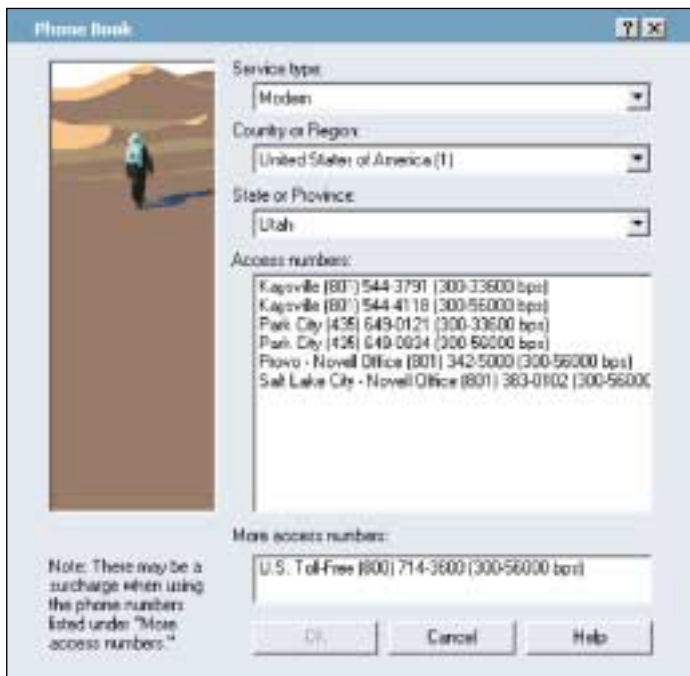


Figure 4. To connect to the Internet using the NOMAD dialer, Novell employees must first choose a number from the Phone Book.

intranet), launch GroupWise to access their e-mail, and map drives to NetWare servers. In other words, using BorderManager VPN Services 3.6, Novell employees can do anything from afar that they can do from within the office, sitting at their own desk.

Split Tunneling

Novell IS&T also makes use of the BorderManager VPN Services 3.6 split tunneling feature. Through split tunneling, Novell IS&T is able to specify with which networks they want the VPN software to exchange encrypted data.

To configure split tunneling, Novell IS&T used the BorderManager VPN Services 3.6 snap-in module for the NetWare Administrator (NWADMIN) utility to create what is called a *protected network list*. In this list, Novell IS&T typed only IP addresses of networks over which they want employees to send encrypted data. Ever after, the VPN client software encrypts data only when exchanging data with servers that are within this list of protected networks.

For example, suppose a Novell employee has accessed the corporate network via the BorderManager VPN Services 3.6 client software. Further suppose that he is accessing several InnerWeb servers, the data for which the VPN client encrypts. When this employee enters

the address for the Compaq web site, www.compaq.com, however, the VPN client does not encrypt the exchanges of data between this client and the Compaq web servers.

Minimizing the amount of data encrypted conserves battery power and minimizes traffic on Novell's corporate network. If data exchanged between remote clients and public Internet sites, such as www.compaq.com, were encrypted, the traffic generated by that exchange would go

through the VPN, out Novell's Internet connection, and back again through the VPN tunnel. This configuration would generate an unnecessary amount of traffic on Novell's network. Whenever possible, Novell prefers "to keep that traffic off of its network," says Crabb. The split tunneling feature in BorderManager VPN Services 3.6 enables Novell IS&T to do just that.

The VPN Jackpot

BorderManager VPN Services 3.6 has saved Novell a significant amount of money in terms of its remote access costs. Without BorderManager VPN Services 3.6, Novell employees squeezed through only one figurative door to the corporate network: the local or toll-free number to the Novell office access servers.

BorderManager VPN Services 3.6 opens several more doors to the network. Rather than entering the corporate network exclusively through the costly toll-free number, Novell's remote and mobile employees now enter the network in any number of ways—by way of a UUNET (or partner) POP; by way of their own ISP; by way of a cable or DSL modem or an ISDN line; and, of course, by way of the Novell office access servers. Employees can now choose not only the most efficient method of access but also the least costly method of access.

NOMAD SIMPLIFIES, SECURES, ACCELERATES—AND SAVES

As yet another example of a real-life solution that realizes Novell's one Net vision, NOMAD simplifies, accelerates, and secures access to the Novell corporate network from virtually anywhere in the world. NOMAD simplifies access by making the order of access consistent for employees: Internet first, corporate network second. NOMAD further simplifies access through the user-friendly interfaces you find in the NOMAD dialer and BorderManager VPN Services 3.6 client software.

NOMAD accelerates access by enabling Novell employees to use the access method of their choice. When employees have broadband access to the Internet, they can use it—and gain broadband access to the corporate network.

NOMAD also accelerates access for employees by enabling Novell IS&T to provide Internet and remote corporate network access simply by creating eDirectory accounts for Novell employees. As a result, Novell employees can access the Novell corporate network from their first day on the job. Likewise, when an employee leaves the company, Novell IS&T simply deletes that employee's eDirectory account and, immediately, that employee loses Internet access (via Novell's UUNET account) and corporate network access.

NOMAD further secures access through its use of an NMAS 2.0 PIN method of authentication to the network. This PIN method reduces the risk of exposing eDirectory passwords to unauthorized users.

The most obvious example of NOMAD securing access to the Novell corporate network is through its use of BorderManager VPN Services 3.6, which encrypts data exchanged between remote Novell employees and the corporate network over the Internet.

Through its use of NOMAD, Novell is experiencing all of these benefits—plus a significant cost savings of 70 percent or more in remote access costs. By using the NOMAD offshoot, Novell Remote Access, your company could experience similar benefits and cost savings.

Linda Kennard is a regular contributor to Novell Connection. Kennard works for Niche Associates, an agency that specializes in writing and editing technical documents. Niche Associate is located in Sandy, Utah. ●