Remote Connectivity @ Novell
A Beigepaper

by Grettir Asmundarson (grettir@neticus.com)
Last Revised: June 30, 1999

A Service Of Novell's Information Services & Technology Global Technical Architecture Group

About The "@ Novell" Series

Most documentation starts as hastily scrawled notes from sleep-deprived developers who weren't necessarily hired for their keen communication skills. Those notes are then fleshed out by recently graduated English majors who have spent their last four years immersed in works of fiction. The results are then passed on to the marketing department whose job it is to make sure that no word or phrase, even if it's true, will reflect unfavorably on the product ("I don't think that the word 'Basic' properly communicates the exciting nature of the product. Why don't we call it 'Visual Zesty!?!'"). It is then beset by lawyers who finish the job by making sure that they haven't explicitly promised that the product will actually do anything.

By the time the documentation gets into your hands, it has been so sanitized for your protection and generalized beyond recognition that you usually have to go out and buy a 3rd-party manual (that was, more likely than not, written by the same non-technical technical writer who wrote the original documentation) in a vain attempt to get an unbiased, unexpurgated, and/or unfiltered view of just how you're really supposed to use the stuff.

That's where the "@ Novell" series comes in. Rather than the vague, generalized, and wholly fictional examples found in most documentation, we're going to tell you exactly how we use our own products to run our own company. After all, we are not a small, tidy computing environment suitable for documentation. We are a big, sprawling, untidy environment made up of over 500 production servers and 20,000 workstations in 130 locations throughout the world. In other words, we're probably an awful lot like you.

And it's not that we're necessarily any smarter than you are, we just have a distinct advantage. By the time you get your hands on one of our released products, we've already been using it to run our business for quite some time. For instance, a month before NetWare 5 shipped, well over half of our 500 production file servers had already been upgraded to NetWare 5. (Keep in mind that these were production servers. These were not test servers that we had safely tucked away in antiseptic labs. These were real-world servers in a real-world environment solving real-world problems.) And two months before NetWare 5 shipped, we'd already converted one of our buildings to IP Only. That means that we've probably gained some insights into implementing our products in a big, sprawling, untidy environment, and this paper is an attempt to share those big, sprawling, untidy insights with our customers.

But keep in mind that this document may be a little rough. It wasn't conceived by a committee, written by a committee, or approved by a committee, so it hasn't been edited, re-edited, tidied up, sanitized, and whitewashed. Don't think of this as an official whitepaper. It's more like a beigepaper.

Universal Connectivity…Period

I'll tell you right now, I hate the title of this beigepaper. Why? Well, for one thing, I think that there is still a lot of baggage associated with the term "remote connectivity." I remember (years

ago, mind you) having to tell users, "Well, you'll be able to dial in to the corporate system, but you'll need to use this special client to do it, and you'll only be able to download your e-mail if you're using this particular e-mail client, and you won't be able to get to any files unless you previously copied them up to this FTP server…" It was an embarrassment. I don't even think that it could be referred to as "connectivity." It was more like accessing remote floppy disks.

But, more importantly, I think we've reached a point where we need to stop differentiating between different kinds of connectivity and say that we provide universal connectivity…period. It should no longer matter how I'm connecting to the corporate intranet, I should have access to the exact same resources in exactly the same way whether I'm connected to a 100Mb Ethernet port at corporate headquarters or dialing in from Beijing. Anything less is just accessing remote floppy disks.

Exploiting The Proletariat…Wherever & Whenever They Might Want To Be Exploited

Our chief motivating factor in providing universal connectivity is entirely selfish. We want employees to be able to get work done no matter where they are and whenever they might want to do it. Whether they are at work, at home, in a hotel room, at a customer site, or at their grandmother's house, we want them to be able to get work done. Whether they are a workaholic, an insomniac, in bed with the flu, or just plain bored and can't bear to watch their *Austin Powers* DVD for the 67th time, we want them to be able to get work done.

And yet we, as an industry, have a rich history of putting up every roadblock imaginable to getting work done when people aren't physically at the office. "What? You're at a customer site and need to download a 120MB file from the corporate Intranet? Sorry, you can't get here from there. No, I'm sorry, you can't use their multiple T-3s to the Internet. You're outside our firewall. You'll need to find an analog line, dial in, and download the file that way. Call me if you still haven't been able to do it by next Friday."

Thankfully, technology and our own cultural mindset have converged to the point where we can now provide universal access to data no matter where you are, no matter how you want to connect to us, and whenever you might need it.

Finally Resolving Your Dial-Up Issues

Historically, "remote connectivity" was provided solely through modems and telephone lines, and it was always an administrative nightmare. These dial-up solutions usually required you to manage your dial-up accounts separately from your regular network accounts, and keeping those

accounts in sync was next to impossible.[1] And then you had the issue of users who didn't live within local calling distance of the office? Do you make them pay long-distance charges just for doing you the favor of doing work at home?[2] Or do you set up a toll-free line for them to use, which works great until your V.P. wants to know why the department's phone bill would come close to covering Brazil's debt load? You could try to outsource your problems away and have some ISP handle your entire dial-up infrastructure, but then problems with administration became even more pronounced. And getting data from your corporate intranet to the ISP and back again *securely* was a thorny issue, too.

That's why BorderManager Authentication Services was such a godsend. BMAS (as the marketing department likes to refer to it, because it sounds rather butch) allowed us to use RADIUS and NDS to authenticate users. We no longer had two points of administration. All dial-up authentication and access could be controlled via NDS…which is as it should be. We've even taken care of our long-distance issues by having UUNET[3] to act as our RADIUS proxy. Our users can dial in to any of UUNET's 1,000 worldwide POPs and their remote access servers will hand off the authentication requests to our own RADIUS server. It's a win-win situation. UUNET loves it because they don't have to worry about any sort of account management or access control, and we love it because all we have to worry about is account management and access control.

Moving Beyond Dial-Up

But providing an adequate dial-up solution is no longer adequate. What about users who are at a customer site that already has a fast connection to the Internet? You're not going to make them dial in using a paltry 56k (hah!) modem are you? What about users who have DSL connections or cable modems? And what about users who already have an account with a much more technologically hip ISP and who find your corporate dial-up system antiquated, bourgeois and jejune.

Well, you can meet those ostentatiously literate whiners' needs by using BorderManager's VPN Services and providing the pretentious little gits with a VPN client.[4] This allows anyone who

---

[1] To highlight what can happen when the two systems aren't in sync, I remember an incident where a gentleman called in to complain about unreliable dial-up connectivity. Things had been working fine for him up until that day. As we were trying to diagnose his problem, it dawned on us that the gentleman in question had been fired three months previous. (That's like to calling up technical support when your pirated software isn't living up to your expectations.)

[2] You could have them submit an expense report and be reimbursed for the long distance charges, but getting the Accounting department involved in any financial process is never a good idea.

[3] UUNET is obviously not the only company that can provide this type of service. Most of the larger ISPs can provide this same sort of service on either a national or international scale.

[4] Here @ Novell, users can install the VPN client via ZENworks when they are at the office. But if they find themselves in a hotel in Baltimore, slapping themselves on the forehead because they (once again) forgot to install the tools that they were going to need on the road before they actually went on the road, it is mercifully available for

already has access to the Internet to gain secure access to your corporate data easily and (this is where the accountants wake up) *at absolutely no cost to you*. That's one thing that people forget about using a VPN solution. You no longer have to worry about *how* the user is going to connect to you. You let them connect to whomever, however they would like. You only have to maintain a single, secure gateway from the Internet to your corporate intranet.

There are other advantages to using a VPN solution. A lot of our developers probably have more than one computer at home, and considering the nature of our business, those computers are probably networked together. If we want those developers to have high-speed access to corporate data (so they can work whenever/wherever they want to), we could get them a DSL connection to their house and have that DSL connection terminate inside our corporate firewall. The problem with that is that now the whole family, including 14-year-old Johnny[5] who might be a little too inquisitive, has direct access to corporate data from any of those workstations at home.

But what are you going to tell them? "We've given you a high-speed connection, but no one else is allowed to use it. Your husband, wife, kids, domestic partner, and/or domestic cat can't use your network connection to access the Internet. They'll have to dial in to another ISP instead." That seems both improbable and impractical.

Instead, we're routing all of our incoming DSL connections to Neticus, our external corporate ISP. That way the family, etc. can surf the Internet any time they want, completely separate from the corporate system. But, when the developer needs to access corporate data, they can simply fire up the VPN client and have instant access to the data they need.

When Remote Access Isn't Enough

We've run into a few instances where simply providing remote access to a resource isn't enough. Database front-ends are a good example of this. We have a few database front-ends that experience some performance degradation unless the user has a four-processor workstation, 1GB of RAM, and a direct gigabit connection to the database server. At least that's what I think the developers must have had in mind when they developed the product, because performance is pretty pathetic on anything less.

People trying to access these databases across a less-than-stellar WAN link (let alone a modem connection) were finding that they could start a query, go have lunch, come back from lunch, visit with friends, finish the work day, go home, have dinner, pack their bags, go visit relatives for a fortnight, and return to the office just in time to see their query results displayed on the screen. In cases like this, remote *access* wasn't enough…we had to resort to remote *control*.

---

download on the Novell Web site (http://support.novell.com/products/bmee35/patches.htm, as of this writing).

[5] …and 14-year-old Johnny's 14-year-old friend who goes by the alias "Lord HackMaster…"

We used Citrix to give these users access to a beefy Windows NT box that had a zippy connection to the database servers. They could then perform their queries in a reasonable amount of time no matter what kind of workstation or network connection they had. The only problem was that Citrix relies on Windows NT accounts/domains for user administration. In a rather brilliant display of IT ingenuity, we were able to get around this by using a "dynamic local user policy" in ZENworks which would dynamically create Windows NT accounts on the Citrix server whenever an authorized user logged in.

Where We're Going From Here

As far as future directions are concerned, we're in the process of testing the use of token cards and smart cards in association with RADIUS. The nice thing about token/smart cards is that they provide you with another layer of security, above and beyond the security provided by NDS. And almost all of the solutions that we've seen allow you to manage the associations between the card and the user via NDS. We are also exploring ways that we can securely provide even more of our services outside of the firewall, obviating the need for any type of VPN client.

Conclusion

We don't pretend to have all of the answers, but we think we're much closer to providing true universal connectivity to users than we've ever been before. We have solutions in place that allow people to get their jobs done no matter where they might be and no matter how they want to connect to us.

As a review, here's a list of our current solutions:

Connection Type	Users can…	…or alternately, they can…
Local Dial-Up Connection	Dial in to the corporate remote access system.	Connect to the ISP of their choice and then use the VPN client to gain access to corporate data.
Non-Local Dial-Up Connection	Dial in to one of UUNET's 1,000 POPs and then use the VPN client to gain access to corporate data.	Connect to the ISP of their choice and then use the VPN client to gain access to corporate data.
ISDN	Dial in to the corporate remote access system.	Connect to the ISP of their choice and then use the VPN client to gain access to corporate data.
DSL	Have their connections routed to Neticus, Novell's external corporate ISP, and then use	Connect to the ISP of their choice and then use the VPN client to gain access to

	the VPN client to gain access to corporate data.	corporate data.

Cable Modem	Connect to the ISP of their choice (if they have a choice) and then use the VPN client to gain access to corporate data.	
Customer Site w/Direct Internet Connection	Connect directly to Novell using the VPN client.[6]	
Slow Connection To An Overly-Demanding Database	Use Citrix to access a Windows NT box with a zippier connection, using ZENworks for dynamic account creation.	Have a lovely vacation.

Acknowledgments

Nothing in this beigepaper represents original thought on my part. I couldn't have written a word without the generous help and input from everyone in Novell's IS&T Global Technical Architecture group. (I'd name them all individually but they'd probably get spammed.)

Send all comments, questions, corrections, and/or complaints to:

grettir@neticus.com

Tasty baked goods can be sent to:

Grettir Asmundarson
PRV-C-122
122 E. 1700 S.
Provo, UT 84606

And please note that Grettir Asmundarson is just a ridiculous pseudonym, so don't bother trying to call. You'll only confuse our receptionist.

[6] Providing that the overzealous Router Czar's at the customer site aren't filtering the ports that the VPN client uses.