

# LDAP and NDS

## A Relationship You Can Count On

Cheryl Walton

When you want to find the telephone number for a local company, you probably look for that company's name in the white pages of your local telephone directory. Similarly, when you want to locate a particular resource on your company's network, you might look for that resource's name in the network directory. In fact, directories are so ubiquitous that it is easy to take them for granted—until you require a directory and that directory is either difficult to access or nonexistent.

Any number of factors can make a directory difficult to access, including poorly organized information. For example, can you imagine how difficult it would be to find a company's telephone number if the entries in a telephone directory were organized by telephone numbers rather than by subscriber names? (If you can't imagine this, consider how difficult it is for the protagonist in Chuck Berry's song "Memphis Tennessee" to find his daughter's telephone number. You can view the lyrics to this song at [http://lyrics.natalnet.com.br/html/english/chuck\\_berry/great/summer.htm](http://lyrics.natalnet.com.br/html/english/chuck_berry/great/summer.htm).) Fortunately, telephone companies avoid creating such directory access problems by organizing subscriber names in a standardized way—that is, in alphabetical order.

Network information can be difficult to access if that information resides in a number of different electronic directories, each of which uses a different access protocol. For example, suppose that your company's network included five LAN segments and each of these segments had a different directory. Furthermore, suppose that each directory contained only information about the LAN segment on which it resides. How difficult would it be to locate a particular user if you did not know which directory to use?

How do you, as a network administrator, avoid such directory access problems on your company's network? The most logical way to avoid these problems is to deploy directories that—like telephone directories—are based on standards. Specifically, you can avoid directory access problems on your company's network by deploying directories and applications that are based on the Lightweight Directory Access Protocol (LDAP) standard.

### WHAT IS LDAP?

LDAP is a standardized protocol for accessing X.500 directories. X.500 is a joint International Organization for Standardization (ISO) and International Telecommunications Union-Telecommunication Standardization Sector (ITU-T) standard



for creating electronic directories that can function as part of a global directory. The X.500 standard also defines the Directory Access Protocol (DAP), a protocol for accessing X.500 directories. As the modifying term *lightweight* implies, LDAP is a version of DAP that contains less code than DAP contains. The Internet Engineering Task Force (IETF) approved LDAP 2 (actually the first version of LDAP) as a proposed standard in 1993 and as a draft standard in 1995. (To view or download this draft standard—Request for Comments [RFC] 1777—visit <http://www.ietf.org/rfc/rfc1777.txt>.)

LDAP's original purpose was to provide PCs with TCP/IP access to X.500 directories. X.500 directories originally ran on large UNIX computers, and DAP access to these directories was a resource-intensive process that ran over all seven layers of the Open Systems Interconnection (OSI) model. However, LDAP 3 has since evolved to become more than an access protocol: LDAP 3 defines an extensible schema for a directory and for a protocol that can access LDAP 3-compliant directories. (A directory schema defines the object classes—or types of objects—that can be stored in the directory. LDAP 3's extensible schema allows directory vendors to add object classes to the core schema defined in LDAP 3.)

Although LDAP and X.500 directories are different from one another, these directories share a common naming protocol for directory information and a common directory structure. (For more information about the advantages and disadvantages of LDAP and X.500 directories, see "LDAP: Use as Directed," *Data Communications*, Feb. 7, 1999. You can download this article at <http://www.data.com/issue/990207/ldap.html>.) The LDAP naming protocol defines LDAP entries as the basic units of directory information. An LDAP entry is a particular instance of an object class and the attributes that comprise that object class. (In Novell Directory Services [NDS] 8, which is LDAP 3 compliant, entries are often referred to as objects—User objects or container objects, for example.)

Attributes, on the other hand, define the types of information that can be stored as part of a particular object class. For

example, the LDAP 3 schema defines an object class called *organizationalUnit*. This class might include the following two LDAP 3-defined attributes and the corresponding values of these attributes: ou=Accounting and facsimile TelephoneNumber=801-555-8645.

LDAP and X.500 directories have a tree structure that begins at the root entry and then branches out to other entries, which in turn branch out to still other entries. (For an example of the LDAP and X.500 directory structure, see Figure 1.) However, LDAP 3 defines more than a useful schema for directories. LDAP 3 also defines the actions that LDAP 3-compliant directories and client applications can take to meet your company's directory requirements.

## LDAP VERBS

What can LDAP 3-compliant directories and applications do? The following verbs—or operations—define the actions LDAP 3-compliant applications and directories can take to provide you with the directory services you need:

- **Bind.** The Bind operation establishes an LDAP 3 session between a client application and an LDAP 3 server. This operation also allows an LDAP 3 client application to pass authentication information to an LDAP 3 server.
- **Unbind.** The Unbind operation terminates an LDAP 3 session between a client application and the LDAP 3 server.
- **Search.** The search operation allows an LDAP 3-enabled client application to request lookup services from an LDAP 3 server. Depending on the parameters listed in the client application's search request, the server will return selected information from a single entry, from all of the entries below a particular entry on the directory tree, or from an entire branch of the directory tree.

In addition to allowing client applications to define the scope of a particular search, LDAP 3 parameters allow a client application to define search filters, a size limit for the number of entries returned, and a time limit within which the search should be performed. A client application can also specify whether or not it wants to know what type of information is defined for a particular entry—that is, the entry's attributes—or the actual values of those attributes. For example, a search may

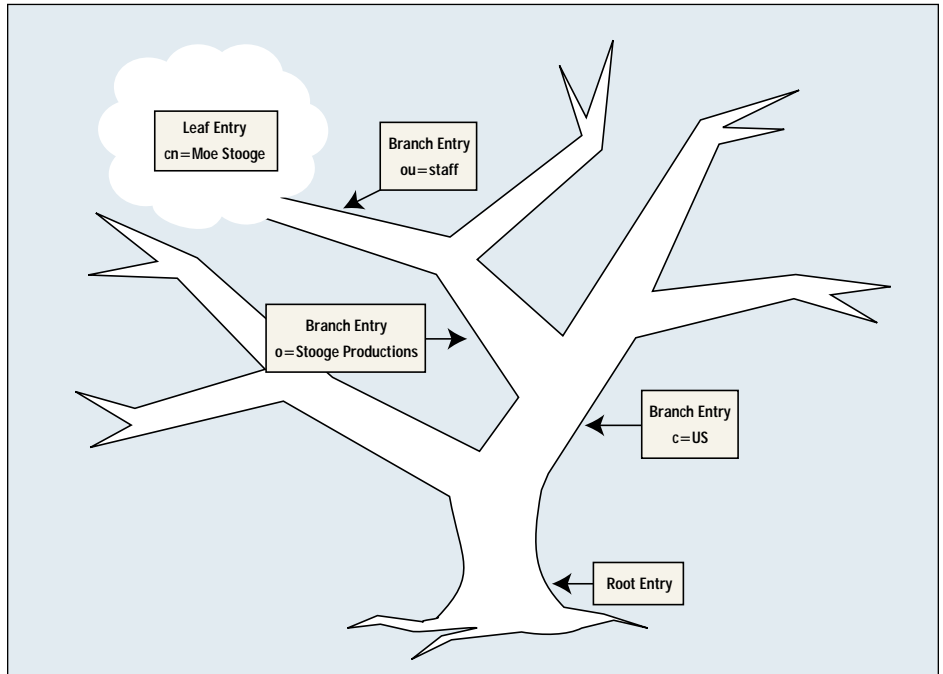


Figure 1. The LDAP directory structure is based on the X.500 standard—the same standard upon which NDS is modeled.

- return one of the following results: The entry for a particular person contains that person's given name, or the given name of that person is Moe Stooge.
- **Modify.** The modify operation allows a client application to modify the value of an attribute for a particular entry. Parameters of the modify operation allow a client application to add values for attributes, to delete values for attributes, and to change values for attributes. For example, a client application might request one of the following operations:
  - A telephone number is added to the telephoneNumber attribute of a particular user entry.
  - A telephone number is deleted from the attribute.
  - An old telephone number is replaced with a new telephone number.
- **Modify Distinguished Name (DN).** The modify DN operation allows a client application to change an entry's distinguished name by changing the leftmost element of that name. An entry's distinguished name is unique within a particular directory tree and identifies the entry's location in that directory tree.

An entry's distinguished name begins with the attribute that names that particular entry, followed by an equal sign, followed by the value of that naming attribute. For example, the distinguished

name of a user entry might begin with the following: cn=Moe Stooge. (In this example, cn [common name] is the attribute that names LDAP 3 user entries.) The distinguished name for this user entry would also include a concatenation of the naming attribute and attribute value pairs that lead from cn=Moe Stooge to the root of the directory tree.

For example, the distinguished name for this entry could be the following: cn=Moe Stooge, ou=staff, o=Stooge Productions, c=US. (In this example ou is the attribute that names LDAP 3 organizational unit entries, o is the attribute that names organization entries, and c is the attribute that names country entries.)

A client application could use the modify DN operation to change cn=Moe Stooge (the leftmost element of this distinguished name) to cn=Moe Whosit. The distinguished name of this entry would then be cn=Moe Whosit, ou=staff, o=Stooge Productions, c=US.

The modify DN operation also includes parameters that allow a client application to move leaf entries to other branches of an LDAP 3 directory tree.

- **Add.** The add operation allows a client application to add a new entry into a directory. In contrast, the modify

## Directories R Us

The following companies are founding members of the Directory Interoperability Forum (DIF). (Companies that distribute directory server software are eligible for DIF membership.)

Novell Inc.  
IBM Corp.  
Oracle Corp.  
Data Connection Ltd. (DCL)  
Lotus Development Corp.  
ISOCOR

The following companies endorse Lightweight Directory Access Protocol (LDAP) 3 standards and have agreed to support DIF objectives:

Allot Communications Inc.  
Alteon WebSystems Inc.  
Altiris Inc.  
AT&T  
Aventail Corp.  
AXENT Technologies Inc.

Bow Street Software Inc.  
Cisco Systems Inc.  
Citrix Systems Inc.  
DASCOM Inc.  
enCommerce Inc.  
Entrust Technologies Ltd.  
Evergreen Internet Inc.  
Food.com  
HAHT Software Inc.  
Lucent Technologies Inc.  
Netegrity Inc.  
NetPro Computing Inc.  
NetObjects Inc.  
NetVision Inc.  
Network Associates Inc.  
OBLIX Inc.  
Orbital Software Group Ltd.  
Process Software Corp.  
Proginet Corp.  
Protek Inc.  
Protocom Development Systems Ltd.  
Red Hat Inc.  
The Open Group  
Triangulum Software Inc.  
VeriSign Inc.  
webMethods Inc. ●

operation allows a client application to add attributes to an existing entry.

- **Delete.** The delete operation allows a client application to delete an entry from a directory.
- **Compare.** The compare operation allows a client application to compare a stated attribute value with the value of an attribute in a particular entry. For example, a client application might verify a particular user's password using the compare operation.
- **Abandon.** The abandon operation allows a client application to abandon an operation that has not yet been completed.
- **Extended.** The extended operation allows LDAP 3 servers to define services that are not available through the operations listed above. The IETF can standardize extended operations through RFCs that act as adjuncts to RFC 2251, which is the RFC that defines LDAP 3. (To view RFC 2251, visit <http://www.ietf.org/rfc/rfc2251.txt>.) However, the LDAP 3 specification does not require application vendors to propose their extended operations as IETF standards.

LDAP 3 also defines a means by which a directory can refer a client

application to another LDAP 3 directory. For example, suppose a client application requested information about a particular entry from an LDAP 3 directory, but the LDAP 3 directory could not find the requested entry. If this LDAP 3 directory knew another LDAP 3 directory that might contain the entry, the first LDAP 3 directory could refer the client application to the other directory.

In addition, LDAP 3 application and directory vendors can define controls that extend a particular operation's capabilities. Although vendors are not required to propose these controls as IETF standards, some controls have already been submitted. For example, the server side sort control allows a client application to specify that requested data be returned in a particular order, such as alphabetical order. The virtual list view control allows a client application to scroll through entries returned as the result of a search. (For more information about the server side sort control, visit <http://www.ietf.org/internet-drafts/draft-ietf-ldapext-sorting-02.txt>. For more information about the virtual list view control, visit <http://www.ietf.org/internet-drafts/draft-ietf-ldapext-ldapv3-ylv-03.txt>.)

## LDAP'S TO DO LIST

Although LDAP 3 provides many of the features and services your company requires from a directory, LDAP 3 will probably not meet all of your company's directory needs. Specifically, LDAP 3 fails to meet the requirements of most companies in the following three areas:

- Replication
- Mandatory authentication
- Access control

### Repeat That, Please

LDAP 3 defines a master-slave model for directory replication. Unfortunately, for many companies, this model is impractical at best and unworkable at worst. In the master-slave model, the master server is responsible for replicating its information on one or more servers that function as subordinates, or slaves. (See Figure 2 on p. 24.)

For medium and large companies, the master-slave replication model quickly becomes unworkable since all of the changes to the directory must be administered by the master server. For example, suppose a company has its headquarters in New York and has 49 branch offices, one in each of the remaining states in the United States. If this company implements a directory that uses master-slave replication, all branch administrators must send directory changes to the network administrator at the corporate office. This administrator must then make all of these changes—such as adding entries for new hires and deleting entries for terminated personnel—on the master server.

Making all of a company's directory changes on one server is "a big problem," observes Michael Simpson, director of strategic market planning for Novell. "In fact, it's impossible to do that in a global organization."

### Not a Knock Knock Joke

LDAP 3 defines two methods by which LDAP 3 client applications can authenticate to LDAP 3 servers: simple authentication and Simple Authentication and Security Layers (SASL). Simple authentication requires authentication by a username and a clear-text password. SASL requires authentication by one of the mechanisms defined in RFC 2222. (To view this document, visit <http://www.ietf.org/rfc/rfc2222.txt>.) SASL mechanisms include Kerberos 4 and Generic Security

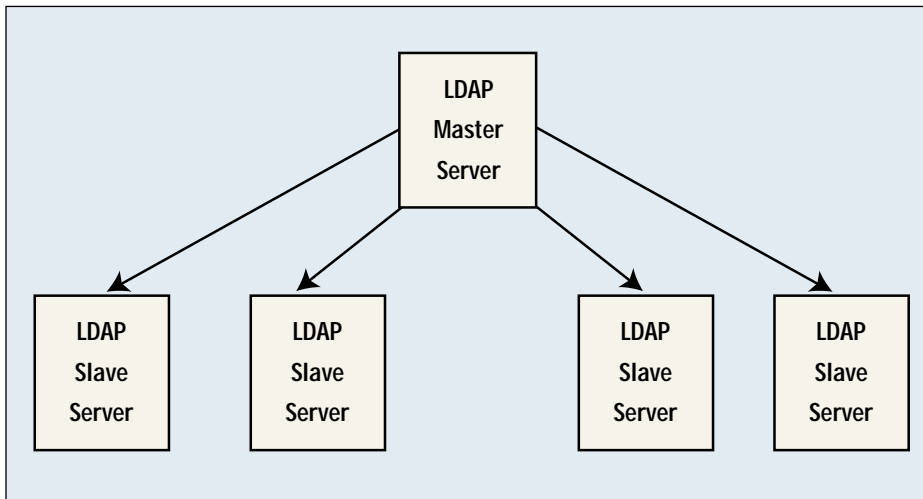


Figure 2. In a master-slave replication model, the master server is responsible for replicating information on one or more servers one level down.

Service Application Program Interface 2 (GSSAPI 2). Kerberos 4 is a security mechanism that uses a ticket—an encryption key partially based on a user's password—to authenticate that user. GSSAPI 2 is a mechanism that passes tokens—messages that contain authentication information such as private key-public key encryption data—between a requesting user and an authenticating LDAP 3 server. (You can view or download more information about GSSAPI 2 at <http://www.ietf.org/rfc/rfc2078.txt>.)

Many directory vendors, including Novell and Netscape, currently use LDAP 3 simple authentication over a Secure Sockets Layer (SSL) connection to provide a secure authentication mechanism. SSL uses the public key-private key encryption of the Rivest, Shamir, Adleman Algorithm (RSA) to transport information—such as usernames and passwords—securely between SSL connections. (SSL 3.0 is a proposed IETF standard. To view this Internet draft, visit <http://home.netscape.com/eng/ssl3/draft302.txt>.)

Although LDAP 3 allows client applications to use either of these security mechanisms to authenticate to LDAP 3 servers, it does not require them to do so. Recognizing the security deficiencies of LDAP 3, the IETF recommends that you not allow LDAP 3 client applications to modify your company's directory until the IETF adopts mandatory standards for authentication. (See RFC 2251, p. 1.)

#### Access Denied

In addition to providing insufficient replication and security services, LDAP

3 does not require access controls. Without access controls, any user who can authenticate to an LDAP 3 directory can access any service that particular directory provides. For example, a newly hired employee might have access to modify DN operations that would wreak havoc on the structure of your company's directory tree.

#### WHY LDAP?

With all of LDAP 3's deficiencies, you may wonder how LDAP 3-compliant directories and applications can possibly meet your company's directory requirements. The answer is simple: Most directory vendors use their own technologies to overcome the deficiencies of LDAP 3. As a result, most LDAP 3-compliant directories can meet your company's replication, authentication, and access control requirements.

You may also wonder which directory vendors support this unfinished protocol. Surprisingly enough, some of the biggest names in the industry—Novell, IBM Corp., Oracle Corp., and Netscape, for example—support LDAP 3. Furthermore, Novell has promised to support future LDAP 3 standards as well, even if support entails making drastic changes to its products. Why?

As Simpson explains, directory vendors such as Novell support standards—even immature standards such as LDAP 3—for several reasons. For example, complying with standards makes it easier for these companies to recruit software developers to write client applications that add value to their products.

In addition, creating standards-based products “removes the barrier in some customers' minds that arises from the fear of vendor lock-in,” Simpson says. Simpson defines the fear of vendor lock-in as the fear of getting caught in a technology trap: “If I buy a vendor's technology because it's the best today, what if it's not the best five years from now, and I want to switch to something else? Am I trapped?”

Also, standards are the only real hope of providing cross-vendor application interoperability. A customer's ability to manage and access his or her company's network should not depend on the relationship of the customer's vendors.

#### In for a Penny, In for a Pound

Supporting LDAP 3 also enables companies such as Novell to be involved in the standards-making process, thereby shaping those standards. For example, to address LDAP 3's replication deficiencies, Novell, Oracle, and Netscape have proposed a companion standard to LDAP 3 called Lightweight Directory Update Protocol (LDUP). LDUP proposes the following enhancements to LDAP 3:

- LDAP 3 directories could be partitioned.
- LDAP 3 servers could use server-to-server replication, rather than master-slave replication.

NDS 8, which is LDAP 3 compliant, uses server-to-server replication and thus will be LDUP-compliant if the IETF ratifies this proposal. (To view the LDUP Internet draft, visit <http://www.ietf.org/internet-drafts/draft-ietf-ldup-model-01.txt>.)

Novell has also teamed with IBM to formulate a proposal that would address LDAP 3's lack of access controls. Like the proposed standard for directory replication, this jointly proposed standard for access control is modeled on NDS 8. More specifically, this proposed standard is based on dynamic inheritance, the directory access control method that NDS 8 uses.

Dynamic inheritance allows you to control directory access hierarchically—that is, based on various levels of the directory tree. For example, with dynamic inheritance, you can establish certain access rights—such as the ability to access the Internet—that apply to everyone in the directory tree, from the

root entry to leaf entries. You can also establish rights that apply to branch entries, such as dial-in rights, as well as rights to certain leaf entries, such as rights to modify the directory. (To view this Internet draft, visit <http://www.ietf.org/internet-drafts/draft-ietf-ldapext-acl-model-04.txt>.)

Of course, Novell is not the only directory vendor that recognizes the value of proposing standards based on the way its products function. Microsoft Corp. has also proposed an access control standard that is based on static inheritance—the access control method that Active Directory will use. With static inheritance, all access rights are written to individual user entries, rather than to a hierarchical level of a directory tree.

For example, if you want to add dial-in access rights to a branch of the directory tree and that branch contains 10,000 user entries, you must add that right to all 10,000 user entries in that branch. Furthermore, if you then want to move a particular user entry from that branch of the directory tree and place the user entry in another branch, you must also manually revoke the dial-in access right.

In contrast, with the dynamic inheritance model, you can grant the dial-in access right to the branch of the directory tree. All of the user entries in that branch are then automatically granted the dial-in right. Furthermore, if you move a user entry from that branch of the directory tree, that user entry automatically loses the dial-in right. Naturally, Novell believes that the LDAP 3 standard should not adopt the static inheritance model—a model that produces what Simpson calls “object bloat.”

#### What's the DIF?

Even if all of the standards Novell proposes are ratified by the IETF, making NDS 8 ipso facto compliant with those standards, there is still no guarantee that third-party applications will have easy access to NDS 8 (or any other LDAP 3-compliant directory). The reason for this seeming contradiction is that IETF standards leave room for interpretation.

To address this problem, Novell and five other directory vendors—IBM, Oracle, Data Connection Ltd., Lotus Development Corp., and ISOCOR—cofounded the Directory Interoperability Forum (DIF). DIF is an organization that fosters the development of applications that are

based on the LDAP 3 standard and that operate consistently with various LDAP-3 compliant directories. DIF consists of five working groups, each of which is charged with a specific task.

For example, each member of the Software Developer Kit (SDK) working group is charged with the task of providing an SDK for his or her specific directory that implements all current LDAP 3 standards and proposed draft standards. These SDKs must also include extended operations and controls—server side sort, for example—that have been developed

*Naturally, Novell believes that the LDAP 3 standard should not adopt the static inheritance model—a model that produces what Simpson calls “object bloat.”*

by DIF members and supporters. (For a list of DIF members and supporters, see “Directories R Us” on p. 22.) In addition, each SDK must be written to a common Application Program Interface (API). (Two LDAP 3 APIs exist as Internet drafts: an API for the C programming language and an API for the Java programming language.)

Eventually, these vendor-specific SDKs will evolve into a single LDAP 3 SDK that developers can then use to write client applications that will perform consistently with any LDAP 3-compliant directory.

DIF's objectives—promoting LDAP 3 standards and interoperability—benefit vendors and consumers alike. The more directories that a given application can access, the greater the number of consumers who can use that application. Likewise, the more applications that can access a given directory, the greater the value of that directory. Finally, the more applications and directories consumers can choose from, the greater the prob-

ability that consumers can find the right products to meet their needs.

#### HERE TODAY, HERE TOMORROW

For vendors, the greatest benefits of participating in various LDAP 3 working groups will probably occur in the future, when LDAP 3 evolves into a mature standard. However, consumers can reap the benefits of deploying LDAP 3-compliant directories now. Applications that allow users to access LDAP 3-compliant directories via their browsers are available today. (To view a list of LDAP 3-compliant applications that are also Novell Yes, Tested and Approved, visit the *NetWare Connection* web site [<http://www.nwconnection.com>].)

In addition, many of the LDAP 3-compliant directories that are available today make up for what LDAP 3 lacks in the areas of replication, security, and access control. For example, Novell currently has the following two products that comply with LDAP 3 but offer features that LDAP 3 lacks:

- NDS 8
- digitalme

#### The Big 8

How does NDS 8 deliver the best of both the standard and nonstandard worlds of directory services? In a nutshell, NDS 8 uses LDAP 3 on the front end and NDS on the back end. That is, Novell uses the same protocol to provide strong authentication, server-to-server replication, and dynamic inheritance access control that it has used since NDS began shipping in April 1993. (The NDS access protocol is based on DAP, the X.500 access protocol that is a superset of LDAP.)

Users can access NDS 8 via NDS applications such as the NetWare Administrator (NWADMIN) utility or via third-party LDAP 3 client applications such as Corporate Services Automation Solution (CSA) 3.6 from OBLIX Inc. (CSA 3.6 is a web-based application that allows you to publish information contained in NDS 8 to the web and allows you to manage information contained in NDS 8. For more information about CSA 3.6, visit <http://developer.novell.com/yes/52297.htm> or <http://www.oblix.com>.)

By default, NDS 8 listens for Protocol Data Unit (PDU) communications from third-party applications on two ports: 389 and 636 (for SSL transmissions).

(You can also configure other ports to listen for PDU communications.) PDU is a standard method for transporting LDAP messages over TCP/IP.

In most cases, NDS 8 passes any PDU requests it receives through one of these ports straight to the NDS back end, which accesses the requested information and returns it to the LDAP 3 front end. The LDAP 3 front end then passes the information to the requesting application.

In some cases, however, NDS 8 must map LDAP 3 object classes to NDS object classes. For example, NDS 8 maps the LDAP 3 `inetOrgPerson` object class to the NDS User object class. (To view the LDAP 3 object classes that are mapped to NDS 8 objects, click the LDAP group object in the NWADMIN utility. This group object is located near the root of the NDS 8 tree.)

As Mark Meredith, senior software engineer for Novell, explains: "We do a little bit of the name mapping stuff to make sure that what we're looking for is the right thing, but we basically just pass PDU requests straight through to NDS 8."

Third-party LDAP 3 client applications, such as CSA 3.6, make it possible to access NDS 8 information without having to use a computer that is running NetWare client software. For example, many third-party client applications—including CSA 3.6—give users browser access to NDS from remote locations. However, since each third-party client application interprets LDAP 3 standards differently (because a common SDK is still not available), you may need to extend the NDS 8 schema to accommodate some of the extended object classes these applications use.

How many schema extensions does it take to run a third-party client application with NDS 8? The answer to this question depends on the particular application you have in mind. However, as a general rule, you will have to make fewer adjustments to the NDS 8 schema if the LDAP 3 client application you choose is Novell Yes, Tested and Approved. For example, CSA 3.6 comes with a batch file that makes the necessary NDS 8 schema extensions for you. (For information about how you can use SCHMAP, a Novell utility to help you extend the NDS schema and map extended object classes to NDS, see "SCHMAP: NDS Schema Extension and LDAP-to-NDS Mapping Utility," *Novell Developer Notes*,

Sept. 1999. You can view this document at <http://developer.novell.com/research/devnotes/1999/septembe/a4frame.htm>.)

If a third-party client application uses SSL to provide secure transmissions, you will also need to set up a certificate authority for the application. A certificate authority issues and manages security information, such as public keys for RSA encryption.

#### Between You and digitalme

digitalme uses NDS 8 to help Internet users manage their digital identity. With digitalme, users can control the information a company gathers about them when they visit that company's web site. (For more information about how digitalme can help you protect your privacy over the Internet, see "The Human Face of NDS," *NetWare Connection*, Aug. 1999, pp. 22–31. You can download this article at <http://www.nwconnection.com/past>.)

digitalme users access directory information via a browser-based client application that Novell created expressly for this purpose. Through this browser-based client application, "digitalme users can access LDAP 3-compliant directories on the Internet to find friends from high school and to look up local restaurants," Eric O. Anderson, a product manager for Novell, explains. In other words, digitalme uses LDAP 3-compliant directories much as you might use the white and yellow pages of a telephone directory.

The LDAP 3 services currently available through digitalme are limited to lookup services because LDAP 3 lacks the ability for users to fine-tune the access rights that are the hallmark of the digitalme technology. Since NDS 8 provides the access control that LDAP 3 lacks, digitalme uses NDS 8 to allow its users to specify what information a particular contact is allowed to access or change. However, as LDAP 3 matures, NDS 8 will continue to evolve to support changes to the LDAP 3 standard, and digitalme will use LDAP 3 services more extensively.

#### The Future

In the meantime, Novell will continue to help you to increase the value of NDS 8 and other LDAP 3-compliant directories. For example, Novell recently announced the upcoming release of a new product, DirXML, that uses LDAP 3 and Extensible Markup Language (XML) to present in-

formation from network directories and other network resources, such as databases, in a single view. XML is a web-based language that contains symbols describing the format of data in a web page.

DirXML uses the LDAP 3 protocol to talk to network directories, and XML provides the style sheet that formats the data LDAP 3 delivers as a result of that conversation. "XML is the middle guy that processes the data and delivers it to me the way I want to see it," Brian Six, a senior systems engineer for Novell, explains. "DirXML allows differing systems to have conversations by breaking the entire translation and data presentation barrier."

#### CONCLUSION

If you have decided that deploying several directories is the best option for your company's network, the advantages of deploying LDAP 3-compliant directories are obvious: If you choose LDAP 3-compliant directories, chances are that you will be able to manage all of those directories via a single LDAP 3-compliant application. You will also be able to choose from a variety of LDAP 3-compliant applications through which users can access information from all of the directories on your company's network.

Even if deploying only one directory is the best option for your company's network, that network will be better served if you deploy an LDAP 3-compliant directory, such as NDS 8. Choosing an LDAP 3-compliant directory will allow you to access that directory via any LDAP 3-compliant application that meets your company's needs. In contrast, if you choose a directory that is not based on LDAP 3 standards, your access to that directory will be limited to the applications the vendor of that directory offers or to applications offered by business partners of that directory vendor.

Choosing an LDAP 3-compliant directory for your company's network also means that you won't be stuck with a particular directory vendor's technology in the future, when directory technologies change. In other words, even though the LDAP 3 standard is still under construction, products based on that standard will probably go further toward meeting your company's directory needs than proprietary directory products will.

*Cheryl Walton works for Niche Associates, a firm that specializes in writing and editing technical documents. ●*