Novell Network Services 4.1 for AIX

By Denise Genty and Rakesh Sharma

Novell Network Services 4.1 for AIX is a NetWare Server based on Novell's Cross-Platform Services 4.10b. Novell Network Services (NNS) is enterprise network operating software that enables a workstation to share files, printers, applications, and other resources among client PCs running operating systems like OS/2® and Windows. NNS is a Licensed Program Product (LPP) that operates on AIX Version 4.2.1 or 4.3.

Novell® Network Services includes Novell Directory Services (NDS), which provides a global naming services that is distributed across the entire NetWare® network. NNS places NetWare Services on an AIX® computer, turning AIX into a non-dedicated NetWare server that provides both host operating and application services and NetWare Services. NetWare Services runs transparently on AIX, so clients are not aware whether the server is a native Novell NetWare server or an AIX NetWare server.

NNS integrates the AIX computer world with the networked PC world. It also solves the need for access to company-wide applications, such as databases or schedules, that run on host systems. Users can write reports and track data using PC desktop applications while having access to the AIX system resources.

NNS Features

NNS provides file and print system services to PC clients. The security model that it supports prevents unauthorized access to network resources. For network management, NNS includes statistical utilities, Simple Network Management Protocol (SNMP), and AIX System Management Interface Tool (SMIT) menus. With NDS, users can log in to the network rather than to an individual server. For application developers who develop applications for NetWare, NNS includes the NetWare application programming interface (API) and APIs for the NetWare IPX, SPX, and SAP protocols.

It includes new features of a Lightweight Directory Access Protocol (LDAP) server, IP tunneling, and licensing models, which are described below.

Novell Directory Services

Novell Directory Services has a global naming service that is distributed across the entire NetWare network with a single point of server administration. NetWare users can login to the Directory tree and, with appropriate rights, access any resource on the network, regardless of physical location.

NDS provides the following features:

- Serves as a distributed information service that stores many types of data

Denise Genty

Rakesh Sharma

- Provides scalability and reliability through its ability to be partitioned and replicated
- Provides a single point of identification to the network with its single sign-on authentication methods
- Uses access control lists (ACLs) to access services
- Enables application developers to customize the information contained in the Directory with its extensible schema
- Uses X.500 as its model

NDS replaces the NetWare bindery found in NetWare Versions 2.0 and 3.0. It allows users to login to the network rather than to an individual server. Its flexibility enables it to work well in both small workgroups with a few servers and corporate organizations with hundreds of servers.

NDS also includes time synchronization. This means that all servers within the same tree report the same time and make automatic adjustments, even when they are located in different time zones.

Other services include the following:

File System Services: Supports multiple name spaces and a multilevel file access system. The namespace feature allows users to view filenames in the naming conventions of their workstation's operating system. Trustee assignments control file access to users and groups, inherited rights, and file attributes, which can restrict rights to specific files.

Print Services: Allows NetWare clients to access printing resources on both NetWare and AIX printers. AIX can be used as a print server and NNS can be used as a print queue server to Novell NetWare network printers. NNS supports all NetWare printing protocols.

Security Services: Provides secure NDS authentication with private-key/public-key encryption login restrictions. The keys are strings of numbers used in mathematical functions. The client workstation uses a private key to encode messages sent to the NetWare server. The server uses a public key to decode the messages. Neither of the two keys nor the user's password are sent across the network.

Online Publications

Fifteen publications are shipped with NNS. One book, *Quick Beginnings*, is shipped with NNS as a hardcopy publication. After installing the `ncps.html.en_US` image, the books are available in PDF format in the `/usr/share/man/info/en_US/a_doc_lib/nns` directory. They can be viewed online using Adobe Acrobat® Reader. You can use a Web browser at the following URL to view a directory page from which you can access the PDF documentation: *file:///usr/share/man/info/en_US/a_doc_lib/nns/nnsnav/topnam.htm*.

Figure 1 shows the NNS documentation home page.

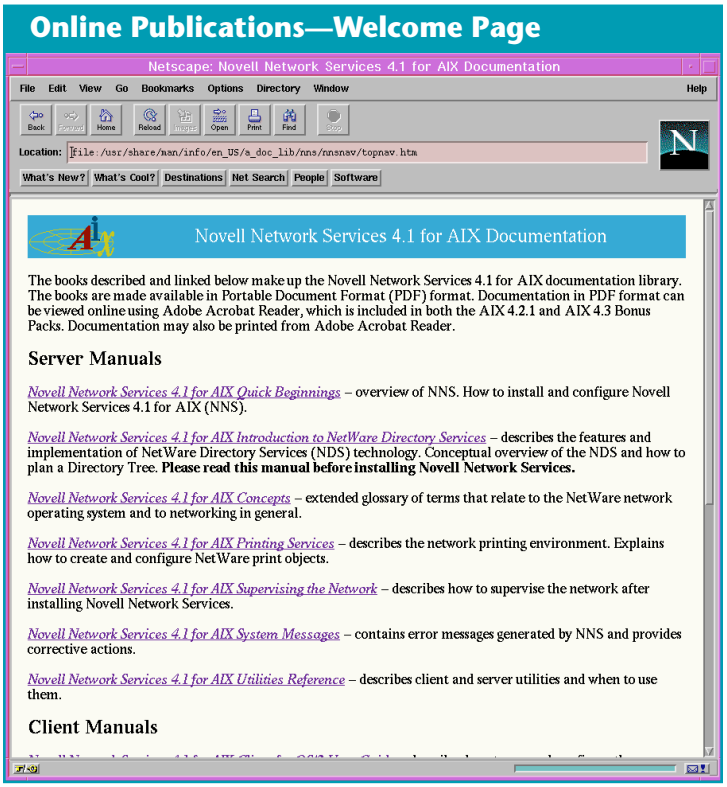

Figure 1. Welcome page for Online Publications

Communications Protocols

NNS supports IPX and IP tunneling transports. NNS supports IPX packet-bursts (as opposed to NCP request responses for every request). This improves file-server data transfer performance.

NNS IPX/SPX includes support for SPX II in addition to SPX protocol support. SPX II delivers much higher performance than SPX I for connection-oriented transport. Since protocol dialect is negotiated at connection time, NNS IPX/SPX will interoperate only with the clients supporting SPX I.

NNS supports IP tunneling for IPX, a feature that provides IP protocol capability to NNS 4.1. IPX packets are sent over an IP network encapsulated in a User Datagram Protocol (UDP). This feature requires both Domain Name Server (DNS), which is part of AIX, and Domain SAP/RIP Service (DSS). The tunneled IPX network requires DSS.

NetWare IP requires its own domain, but AIX supports IP Security to complement NetWare IP. IP Security allows secure IPX tunneling across the Internet.

API Support

The NetWare API for C is the interface to the C programming libraries for workstation applications. These libraries enable applications to interact with the NetWare server and access NDS.

LDAP Server

Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs over TCP/IP. It is used primarily to search for information in the directory, where the directory service protects the data and provides the security for the data.

NNS LDAP support is compatible with LDAP Version 2. NNS 4.1 LDAP is compatible with AIX LDAP Client support, which includes the Java™ Class Library and an AIX shared library. In addition to the AIX client, NDS/LDAP is compatible with any client that supports LDAP Version 2 protocol.

An example of the use of the NNS LDAP server would be to obtain NDS users' information, such as e-mail addresses, using an LDAP-enabled Web browser.

Licensing Models

NNS uses a client/server licensing model. Specifically, it uses the License User Management System, based on the iFOR/LS management system. This iFOR/LS server-based licensing scheme consists of a license server that maintains a license database. This database contains the availability of NNS licenses and maintains a usage count of the product.

> ***NDS flexibility enables it to work well in both small workgroups with a few servers and corporate organizations with hundreds of servers.***

Two types of licenses can be purchased for NNS: SCALE server license and user licenses. If you do not purchase any licenses, you may configure a SANDS mode server, which has a default of two user licenses.

A SANDS tree can be installed and configured on a single server. No other servers can be added to the Directory, and the NDS database cannot be partitioned or distributed. A SCALE server license is used when installing and configuring the NDS tree. A SCALE tree allows server database replication to multiple servers, and the NDS database can be partitioned and distributed. The directory tree can be shared with other servers.

Minimum Server Configuration

After the license server is configured, it takes four steps to configure the AIX NetWare server. The first step is to configure the maximum number of user licenses. Using the SMIT tool, enter the maximum number of licensed connections, as shown in Figure 2. Next, configure the server name and unique IPX internal address on the Minimum Configuration screen, shown in Figure 3. Verify that the IPX LAN interface data is correct on the Change/Show a LAN Interface screen as shown in Figure 4.

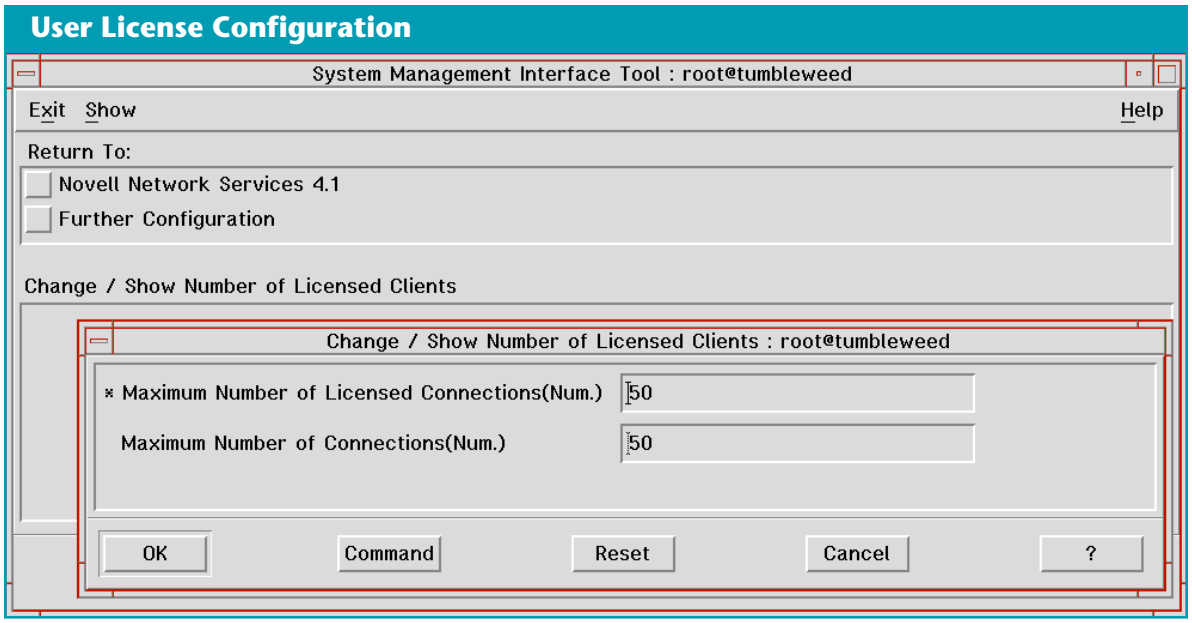

Figure 2. Configuration of user licenses

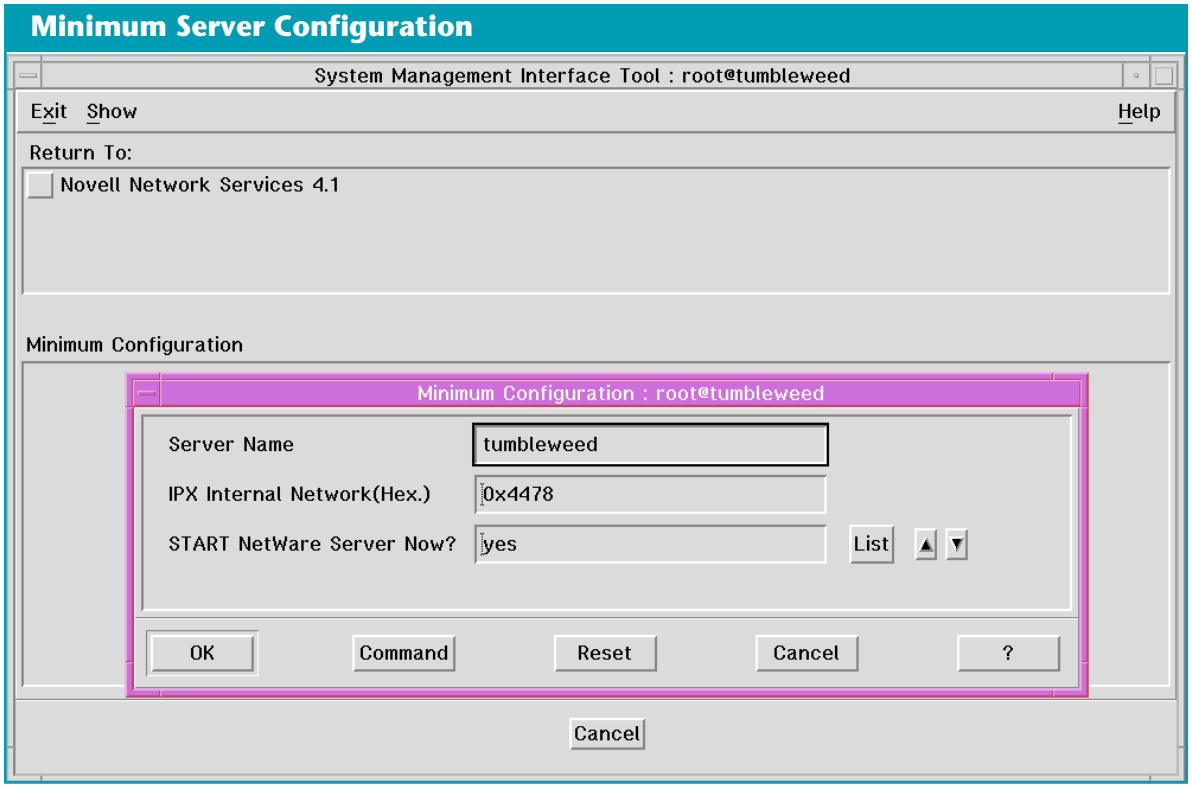

Figure 3. Minimum server configuration

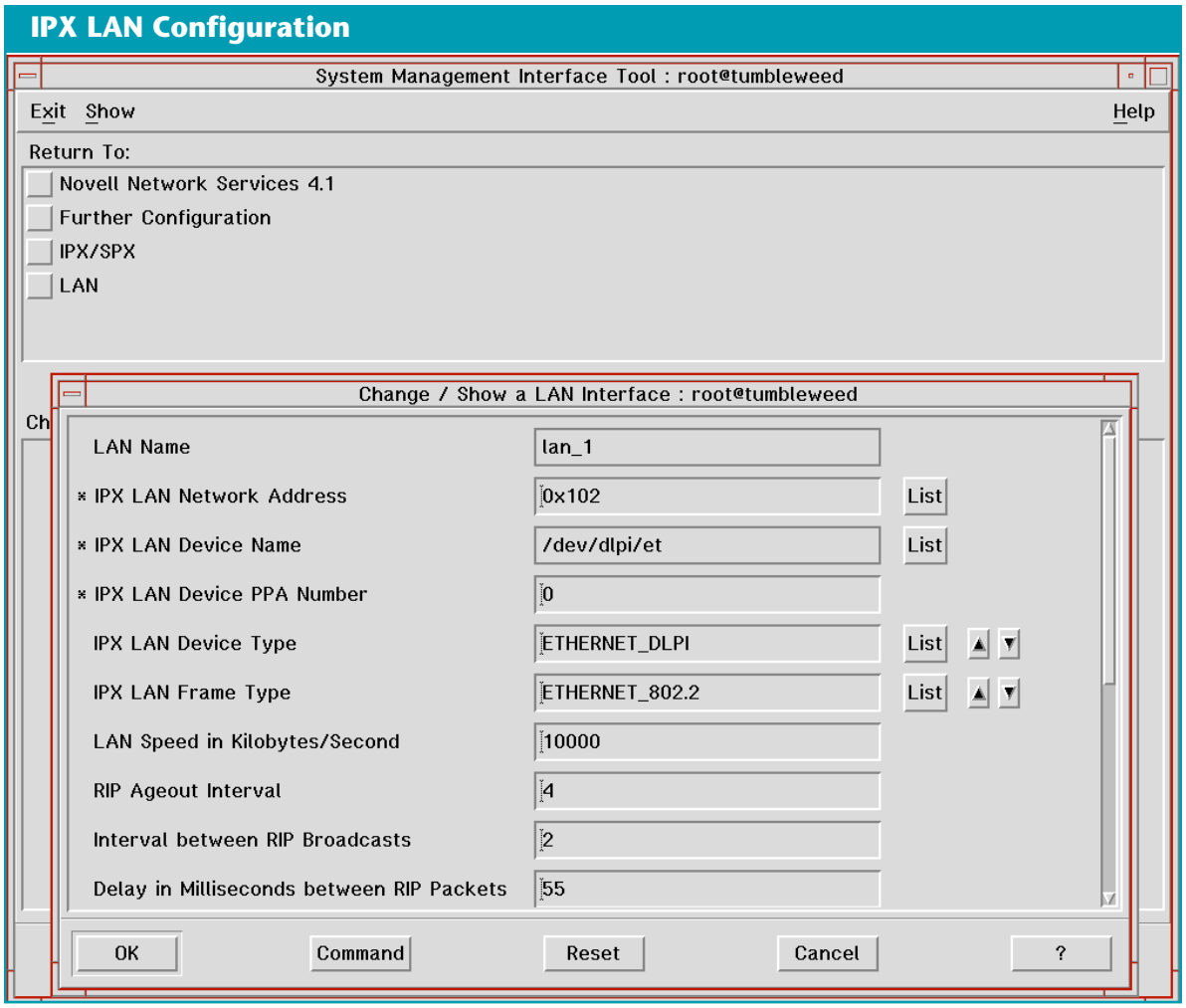

Figure 4. IPX LAN configuration

Finally, install the NDS tree and configure the tree name, context, and administration user password using the `SMIT` option; then configure Network Directory Services using `dsinstall`. The AIX NetWare server is now ready for operation with one volume (`SYS:`) and one user (`admin`) created.

The Structure of NNS

Figure 5 shows the overall architecture of NNS. Modules within the dark box are available only when the NetWare server is up. Modules outside the box are either required by the NetWare protocol stack or run on the stack independent of NNS. The ovals represent daemons or AIX processes. The rectangles represent kernel drivers. The lines, which represent the significant paths of communication, are not meant to be inclusive. When daemons overlap (as the SAP and Diagnostic daemons in Figure 5), the daemon in the back has direct lines of communication to the same drivers as the daemon in front. For example, the Diagnostic daemon has lines of communication to the IPX, RIPX, and SPX II drivers.

NNS uses two key daemons to initialize NetWare Services:

- NPS daemon is primarily responsible for linking kernel drivers and spawning daemons required to set up IPX communication services.
- NetWare daemon is responsible for linking kernel drivers and spawning daemons required to set up NNS services.

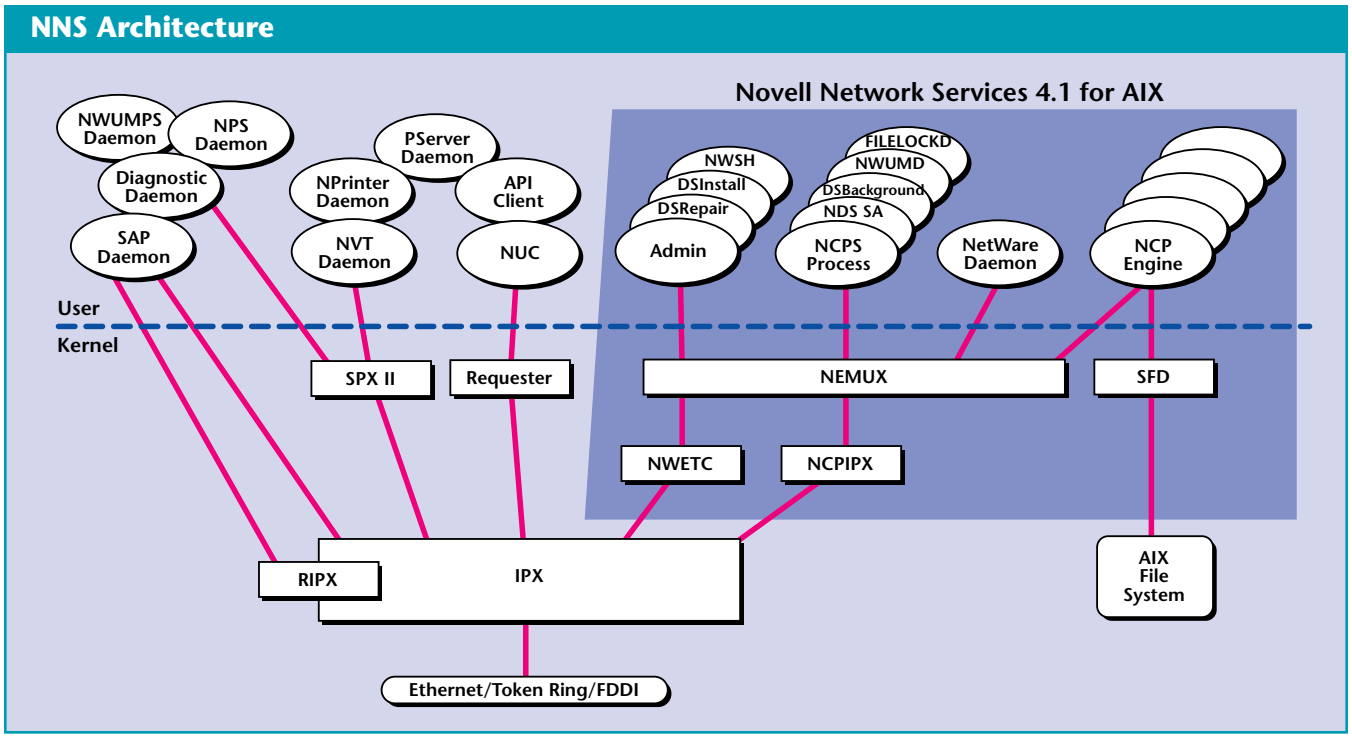

Figure 5. NNS architecture

NDS Example Configuration

A NetWare server can be configured to have multiple volumes in addition to the SYS volume; NDS can be configured so that a business' network has one or multiple directory trees. Companies with centralized management usually prefer a single tree. Businesses with decentralized management may prefer multiple trees if there is little interaction between groups, or a single tree if there is much interaction between groups. Figure 6 shows an example of a directory tree and its objects.

In the tree example in Figure 6, the NDS tree contains a top-most organization named

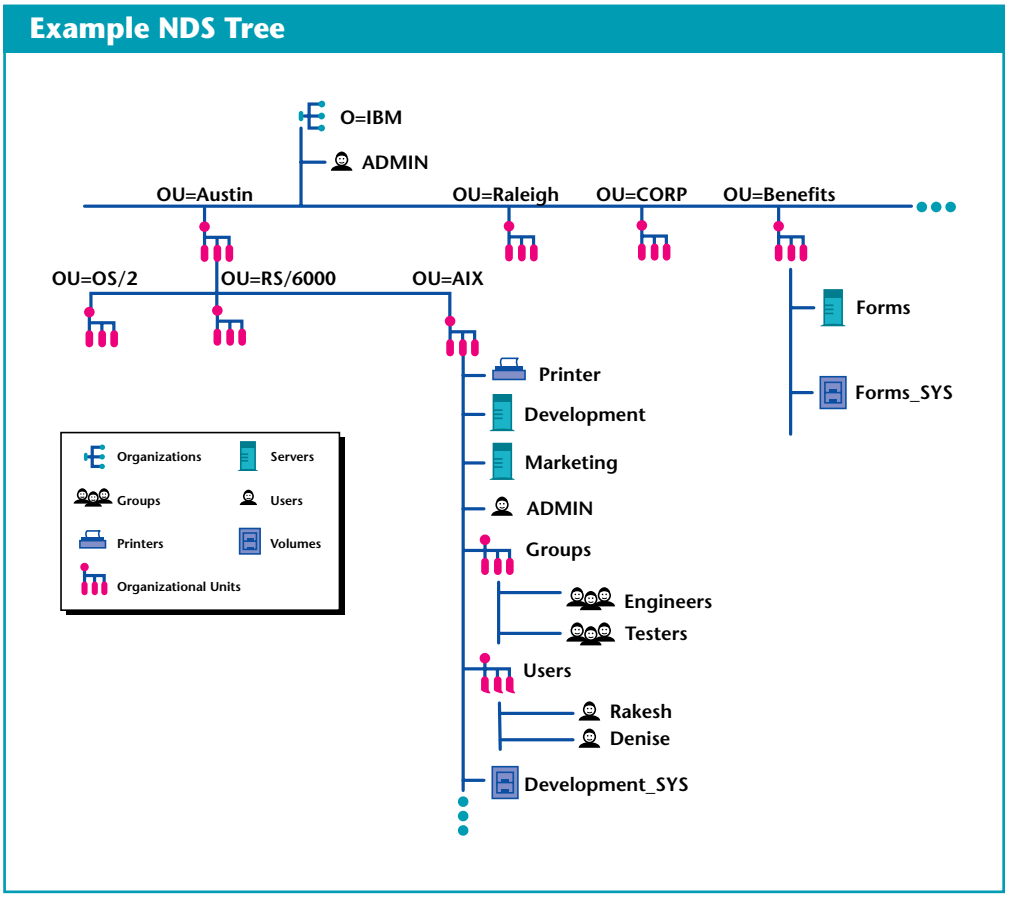

Figure 6. Directory tree and its objects

"IBM." There is one user, ADMIN, which has been given all rights to the tree. Those rights flow down to the organizations of Austin, Raleigh, Corporate, and Benefits. Company-wide resources can be accessed and administered, even if the resource is in a different geographical location. End users have access to their organizational unit or other units without requiring logins to individual servers.

This tree is divided by geographic locations and divisional functions. There is a logical organization for the Austin and Raleigh IBM sites, and organizations for corporate headquarters and the benefits organization. To restrict access, the Austin organizational unit has three different divisions: OS/2, RS/6000, and AIX. In this example, a second ADMIN user is defined in the AIX organization. ADMIN, the administrator for the organization, has all rights to the volumes and servers in AIX. This ADMIN user can administer the day-to-day operations of the AIX organization.

The AIX organization has defined one NetWare printer, two servers, and a volume named `Development_SYS`. The Development and Marketing organizations each have one server primarily for their use. There are groups defined for engineers and testers. The Users group contains users named Rakesh and Denise, who have access to the AIX printer and the two servers.

Groups are a beneficial NDS feature because the administrator can assign users to a group, then, with just one trustee assignment, grant access to all the users who belong to the group. In this example, the Benefits organizational unit has a server that contains all benefit claim forms for the IBM company. On the `Forms_SYS` volume, a user such as Denise in the AIX organization could be given access rights to the volume to print necessary claim forms.

***Denise M. Genty**, IBM Corporation, 11400 Burnet Road, Austin, TX 78758. Ms. Genty is a staff software engineer in the RS/6000 Division. She has worked in IBM RS/6000 hardware and AIX software development for seven years. She has concentrated on AIX device system configuration and communications applications, and currently works on NetWare for AIX. Ms. Genty has a BS in Computer Science from Texas A&M University.*

***Rakesh Sharma**, IBM Corporation, 11400 Burnet Road, Austin, TX 78758. Mr. Sharma is senior software engineer with a specialty in networking protocols, TCP/IP, and UNIX® interoperability with PCs. He is currently working with Windows NT/PC interoperability for AIX. He has a BS in Electrical Engineering from ITT Kanpur in India and an MS in Computer Science from North Dakota State University.*