

Understanding NDS

NDS™ 7

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 1993-2000 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent Nos. 4,555,775; 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,594,863; 5,608,903; 5,633,931; 5,652,854; 5,671,414; 5,677,851; 5,692,129; 5,758,069; 5,758,344; 5,761,499; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,275; 5,832,483; 5,832,487; 5,859,978; 5,870,739; 5,873,079; 5,878,415; 5,884,304; 5,893,118; 5,903,650; 5,905,860; 5,913,025; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,467; 5,956,718; 5,974,474. U.S. and Foreign Patents Pending.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

www.novell.com

Understanding NDS
January 2000
104-001265-001

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

For a list of Novell trademarks, see the final appendix of this book.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

Understanding NDS	9
1 Understanding NDS	11
What Is the NDS Directory?	11
NDS Ease of Management.	12
Powerful Tree Structure	12
Container Objects	13
Inheritance	15
Integrated Management Utility	16
Single Login and Authentication	17
Replicas: Keeping NDS Running.	17
Replica Types	18
Context and Naming	20
Complete Name	21
Typeful Name.	21
Name Resolution	21
Current (Workstation) Context	21
Leading Period	22
Relative Naming	22
Trailing Periods.	23
Partitions: Helping NDS Perform Well	24
Creating a New Partition	25
Distributing Replicas for Performance	25
Partitioning and WAN Links	26
Single Partition Solution	26
Two-Partition Solution	27
Object Classes and Properties.	28
Container Object Classes	29
Leaf Object Classes	29
NDS Rights.	30
NDS Rights Concepts	30
Synchronizing Servers in the Replica Ring	31
If Your Network Needs a Bindery	31
The Importance of Synchronizing Time	32

2	Planning Your NDS Tree	33
	Start with the Defaults	33
	Accommodate Slow or Unreliable WAN Links	35
	Avoiding a Flat Tree	36
	Restrict Partitions to 1,000 Objects	38
	Plan Workgroup Containers and Leaf Objects	39
	Workgroup Exceptions	40
	Standardize Property Values	40
3	Objects and Rights	43
	List of Objects	43
	[Root]	46
	What [Root] Represents	46
	Usage	46
	Important Properties	47
	Organization	47
	What an Organization Object Represents	47
	Usage	47
	Important Properties	48
	Organizational Unit (OU)	49
	What an Organizational Unit Object Represents	49
	Usage	49
	Important Properties	49
	Country	50
	What a Country Object Represents	50
	Usage	51
	Important Properties	51
	NetWare Server	51
	What a NetWare Server Object Represents	51
	Usage	51
	Important Properties	51
	Volume	52
	What a Volume Object Represents	52
	Usage	52
	Important Properties	52
	User	53
	What a User Object Represents	53
	Usage	53
	Important Properties	54
	Group	56
	What a Group Object Represents	56
	Usage	56
	Important Properties	56

Alias	57
What an Alias Object Represents	57
Usage.	57
Important Properties	59
Directory Map	59
What a Directory Map Object Represents	59
Usage.	59
Important Properties	60
Profile	61
What a Profile Object Represents	61
Usage.	61
Important Properties	61
Trustee Assignments and Targets	62
Public Trustee	63
Object Rights.	63
Property Rights.	64
Effective Rights.	66
Security Equivalence.	67
Access Control List (ACL)	67
Inherited Rights Filter (IRF)	68
Default Rights for a New NetWare Server	69
Delegated Administration	70
4 Terms	71
NDS Server	71
Replica Synchronization	71
Schema Synchronization.	72
Limber	72
Backlink	72
Connection Management	73
A Novell Trademarks.	75

Understanding NDS

NDS™ is Novell's reliable, proven architecture for network management. This section introduces you to the basics of NDS and provides you helpful planning information for creating an NDS tree.

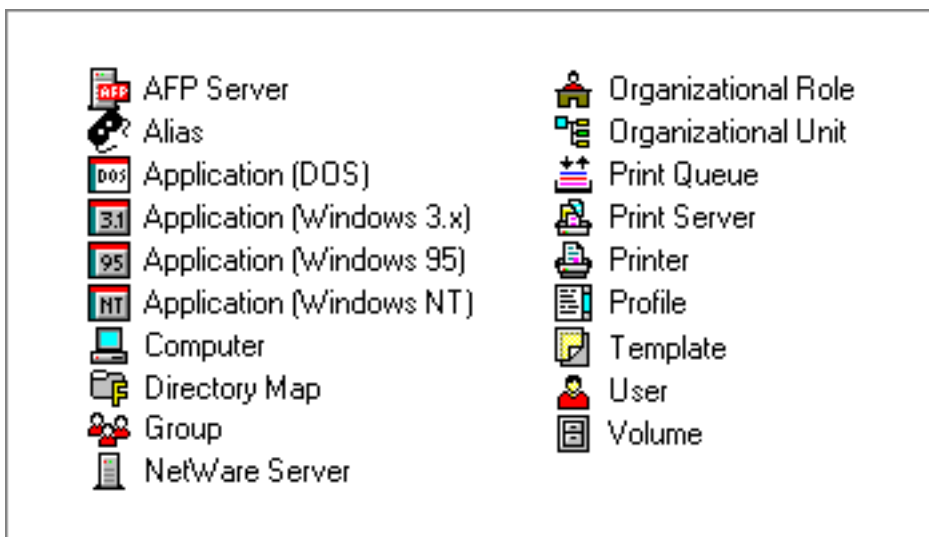
1

Understanding NDS

This section gives you the general knowledge about NDS™ that you'll need to administer an NDS-based network.

What Is the NDS Directory?

In simplest terms, the NDS Directory is a list of objects that represent network resources, such as network users, servers, printers, print queues, and applications. The figure below shows a few of the objects as viewed in the NWAdmin management utility.



NOTE: Some object classes may not be available, depending on the operating system of the NDS server.

For more information on NDS objects, see “Object Classes and Properties” on page 28.

The NDS Directory is physically stored as a set of database files on a server. If the server hosts file system volumes, these files are on volume SYS. If no volumes are present, the Directory is stored on the server’s local drive in a subdirectory of the NDS installation directory.

If you have more than one NDS server on the network, the NDS Directory can be replicated on multiple servers.

NDS Ease of Management

The NDS™ Directory allows for easy, powerful, and flexible management of network resources. It also serves as a repository of user information for groupware and other applications. These applications access your NDS Directory through the industry-standard Lightweight Directory Access Protocol (LDAP).

NDS ease-of-management features include a powerful tree structure, an integrated management utility, and single login and authentication.

Powerful Tree Structure

NDS organizes objects in a tree structure, beginning with an object called [Root].

Whether your NDS servers are running NetWare, UNIX*, or Windows NT*, all resources can be kept in the same NDS tree. You won’t need to access a specific server or domain to create objects, grant rights, change passwords, or manage applications.

The hierarchical structure of the NDS tree gives you great management flexibility and power. These benefits are primarily the result of two features: container objects and inheritance.

Container Objects

Container objects allow you to manage other objects in sets, rather than individually. There are three common classes of container objects:



 *[Root]* is the first container object in the tree. It usually contains your company's *Organization* object.

 *Organization* is normally the first container class under *[Root]*. The *Organization* object is typically named after your company. Small companies keep management simple by having all other objects directly under the *Organization* object.

 *Organizational Unit* objects can be created under the *Organization* to represent distinct geographical regions, network campuses, or individual departments. You can also create *Organizational Units* under other *Organizational Units* to further subdivide the tree.

A fourth class of container object is the *Country* object, which is seldom used.

You can perform one task on the container object that applies to all objects within the container. Suppose you want to give Amy complete management control over all objects in the *Accounting* container.

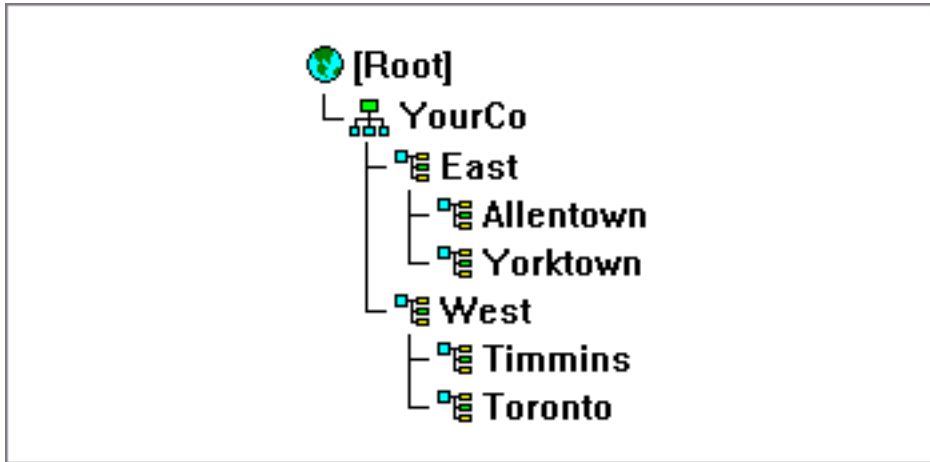


All you need to do is drag the User object named Amy onto the Organizational Unit object named Accounting. Then you select the rights you want Amy to have and click OK. Now Amy has rights to manage the Database application, the Bookkeepers group, the LaserPrinter printer, and the User objects Amy, Bill, and Bob.

For more information on NDS objects, see “Object Classes and Properties” on page 28.

Inheritance

Another powerful feature of NDS is rights inheritance. Inheritance means that rights 'flow down' to all containers in the NDS tree. This allows you to grant NDS rights with very few rights assignments. For example, suppose you want to grant management rights to the NDS objects shown below:



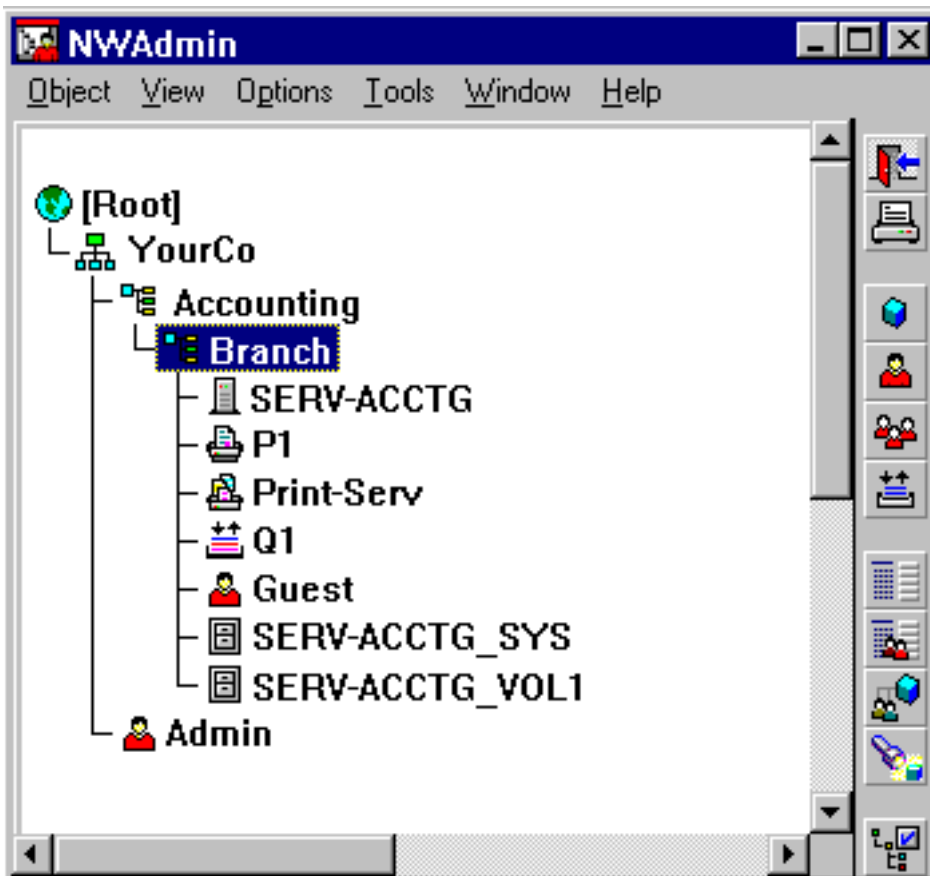
You could make any of the following assignments:

- ♦ If you grant a user rights to Allentown, the user can only manage objects in the Allentown container.
- ♦ If you grant a user rights to East, the user can manage objects in the East, Allentown, and Yorktown containers.
- ♦ If you grant a user rights to YourCo, the user can manage any objects in any of the containers shown.

For more information on assigning rights, see “NDS Rights” on page 30.

Integrated Management Utility

NWAdmin (shown below) is the management console for the entire network.



- ♦ From a workstation running Windows 3.1x, Windows 95, or Windows NT, you can use NWAdmin to perform the following supervisory tasks:
- ♦ Create and delete NDS* objects
- ♦ Move and rename NDS objects
- ♦ Assign rights in the NDS tree and in the NetWare file system
- ♦ Set up print services
- ♦ Set up licensing services

NOTE: NWAdmin incorporates all the functions available in Novell's DOS command line utilities FILER, NETADMIN, PARTMGR, and PCONSOLE.

Single Login and Authentication

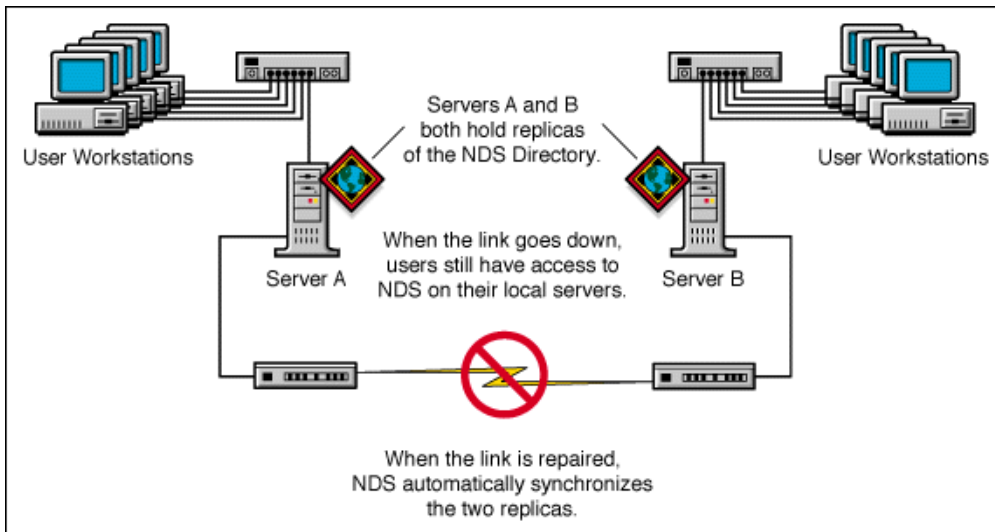
Users log in to a global directory, so you don't need to manage multiple server or domain accounts for each user, and you don't need to manage trust relationships or pass-through authentication among domains.

A security feature of the Directory is authentication of users. Before a user logs in, a User object must be created in the Directory. The User object has certain properties, such as a name and password.

When the user logs in, NDS checks the password against the one stored in the Directory for that user and grants access if they match.

Replicas: Keeping NDS Running

If you have more than one NDS server on your network, you can keep multiple replicas (copies) of the NDS Directory. That way, if one server or a network link to it should fail, users can still log in and use the remaining network resources.



We recommend that you keep three replicas for fault-tolerance of NDS (assuming you have three NDS servers to store them on). A single server can hold replicas of multiple partitions.

NOTE: NDS replication does not provide fault tolerance for the file system. Only information about NDS objects is replicated. You can get fault tolerance for file systems by using the Transaction Tracking System* (TTS*), disk mirroring/duplexing, RAID, or Novell Replication Services* (NRS).

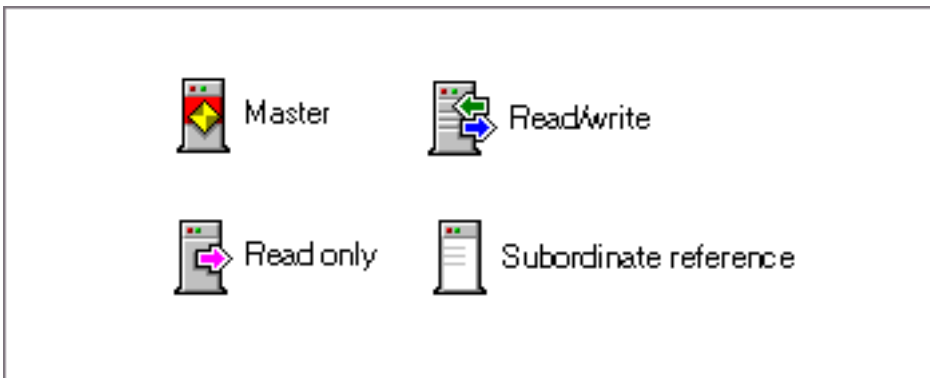
For servers before NetWare 5 that provide bindery services, a master or read/write replica is required.

If users regularly access NDS information across a WAN link, you can decrease access time and WAN traffic by placing a replica containing the needed information on a server that users can access locally.

The same is true to a lesser extent on a LAN. Distributing replicas among servers on the network means information is usually retrieved from the nearest available server.

Replica Types

Four types of replicas are available, as shown below with their corresponding icons.



Master Replica

By default, the first NDS server on your network holds the master replica. There is only one master replica for each partition at a time. If other replicas are created, they are read/write replicas by default. For more information on partitions, see “Partitions: Helping NDS Perform Well” on page 24.

If you're going to bring down the server holding a master replica for longer than a day or two, you can make one of the read/write replicas the master. The original master replica automatically becomes read/write.

A master replica must be available on the network for NDS to perform operations such as creating a new replica or creating a new partition.

Read/Write Replica

NDS can access and change object information in a read/write replica as well as the master replica. All changes are then automatically propagated to all replicas.

If NDS responds slowly to users because of delays in the network infrastructure (such as slow WAN links or busy routers), you can create a read/write replica closer to the users who need it. You can have as many read/write replicas as you have servers to hold them, although more replicas cause more traffic to keep them synchronized with each other.

Read-Only Replica

The read-only replica has been devised for future implementations of NDS. Read-only replicas receive synchronization updates from master and read/write replicas but don't receive changes directly from clients.

Subordinate Reference Replica

Subordinate reference replicas are special system-generated replicas that don't contain all the object data of a master or a read/write replica. Subordinate reference replicas therefore don't provide fault tolerance. They only contain enough information for NDS to resolve names across partition boundaries.

You can't delete a subordinate reference replica; NDS deletes it automatically when it is not needed. Subordinate reference replicas are only created on servers that hold a replica of a parent partition but no replicas of its child partitions.

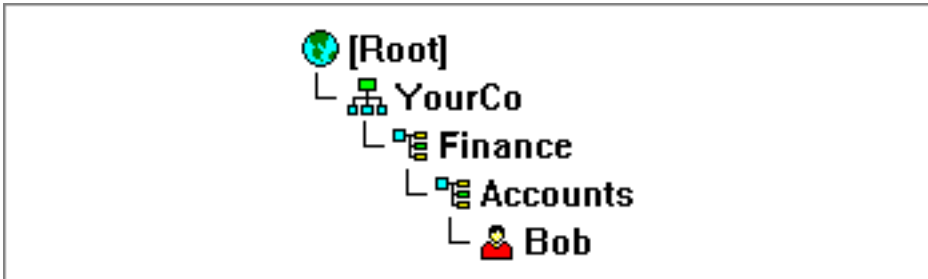
If a replica of the child partition is copied to a server holding the replica of the parent, the subordinate reference replica is automatically deleted.

Context and Naming

The context of an object is its position in the NDS tree.

In NWAdmin, the position of the object is shown in the graphic layout.

You can see in the picture below, for instance, that User Bob is in Organizational Unit Accounts, which is in Organizational Unit Finance, which is in Organization YourCo.



Sometimes, however, you need to express the context of an object in an NDS utility. For example, you could be setting up Bob's workstation and need to supply a name context, as shown below.

Client 32	Login	Default Capture	Advanced Settings
Preferred server:	AppServer		
Preferred tree:	YourTree		
Name context:	Accounts.Finance>YourCo		
First network drive:	F v		

The context is specified as a list of containers separated by periods, between the object in question and the [Root]. In the example above, the User object

Bob is in the container Accounts, which is in the container Finance, which is in the container YourCo. (You don't list the container [Root].)

Notice that if you say the context, replacing the periods with the words 'which is in,' the context seems logical.

Complete Name

The complete name of an object is its object name with the context appended. For example, the complete name of User object Bob is Bob.Accounts.Finance.YourCo.

Typeful Name

Sometimes typeful names are displayed in NDS utilities. Typeful names include the object type abbreviations from the list below:

<i>Object Class</i>	<i>Type</i>	<i>Abbreviation</i>
All leaf object classes	Common Name	CN
Organization	Organization	O
Organizational Unit	Organizational Unit	OU
Country	Country	C

In creating a typeful name, NDS uses the type abbreviation, an equal sign, and the object's name. For instance, Bob's partial typeful name is CN=Bob. Bob's complete typeful name is CN=Bob.OU=Accounts.OU=Finance.O=YourCo. You can use typeful names interchangeably with typeless names in NDS utilities.

Name Resolution

The process NDS uses to find an object's location in the Directory tree is called name resolution. When you use object names in NDS utilities, NDS resolves the names relative to either the current context or the [Root].

Current (Workstation) Context

Workstations have a context set when the networking software runs. For instance, Bob's workstation would be set to the current context as follows:

Accounts.Finance.YourCo

Current context is a key to understanding the use of leading periods, relative naming, and trailing periods.

Leading Period

Use a leading period to resolve the name from [Root], no matter where the current context has been previously set. In the example below, the leading period tells the CX (Change Context) utility to resolve the name relative to the [Root].

CX.Finance.YourCo

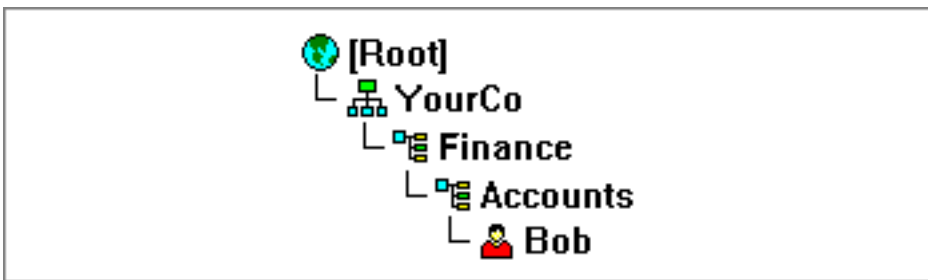
NDS interprets the command as 'Change context to the Finance container, which is in the YourCo container, resolved from [Root].'

The workstation's current context changes to the Finance container, which is in the YourCo container.

Relative Naming

Relative naming means that names are resolved relative to the workstation's current context, rather than [Root]. Relative naming never involves a leading period, since a leading period indicates resolution from [Root].

Suppose a workstation's current context is set to Finance.



The relative object name of Bob is

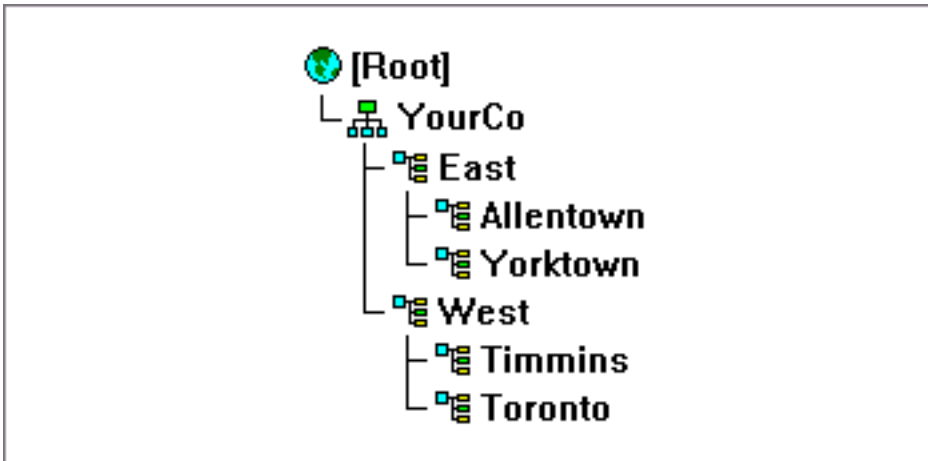
Bob.Accounts

NDS interprets the name as 'Bob, which is in Accounts, resolved from the current context, which is Finance.'

Trailing Periods

Trailing periods can only be used in relative naming. Therefore, you can't use both a leading period and a trailing period. A trailing period changes the container from which NDS resolves the name.

Each trailing period changes the resolution point one container toward the [Root]. Suppose you want to change your workstation's current context from Timmins to Allentown in the example below.



The proper CX command uses relative naming with trailing periods:

`CX Allentown.East..`

NDS interprets the command as 'Change the context to Allentown, which is in East, resolved from two containers up the tree from the current context.'

Similarly, if Bob is in the Allentown container and your workstation's current context is Timmins, Bob's relative name is

`Bob.Allentown.East..`

Partitions: Helping NDS Perform Well

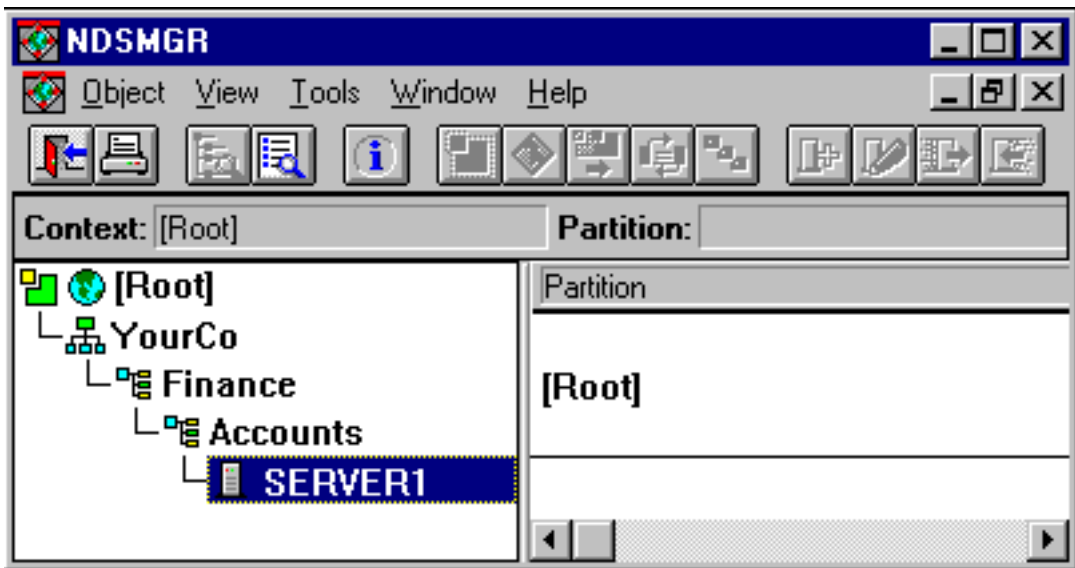
If you have more than 1,000 objects in your NDS tree, or slow or unreliable WAN links, you should consider partitioning (dividing) the NDS Directory.

Partitioning allows you to take part of the Directory off one server and put it on another server.

A partition is a logical division of the NDS database. A Directory partition forms a distinct unit of data in the NDS tree that stores Directory information.

Each Directory partition consists of a set of container objects, all objects contained in them, and data about those objects. NDS partitions don't include any information about the file system or the directories and files contained there.

Partitioning is done with the NDS Manager utility, which you can access from NWAdmin or run independently. A sample NDS Manager screen is shown below.



Partitions are identified in NDS Manager by the partition icon: 

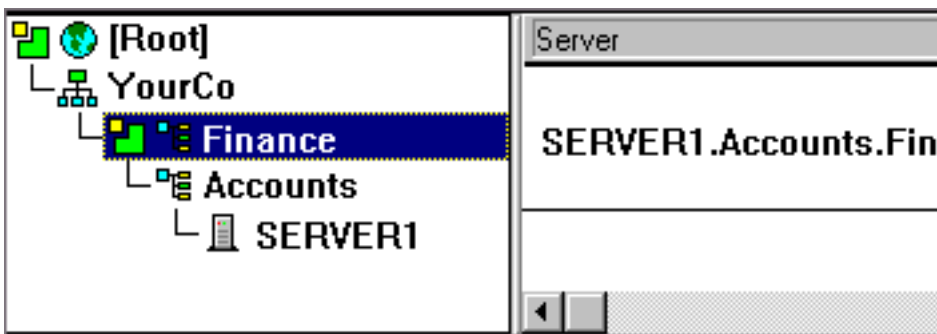
In the example, the partition icon is next to [Root]. This means [Root] is the topmost container in the partition. No partitions are shown by any other containers, so the [Root] partition is the only one.

This is the default partitioning for NDS, keeping the entire Directory together in one partition.

Notice in the screen that server SERVER1 is highlighted. When you highlight a server in NDS Manager, any replicas held on that server are shown on the right. In this case, SERVER1 holds a replica of the [Root] partition. See also “Replicas: Keeping NDS Running” on page 17.

Creating a New Partition

Partitions are named by their topmost container. In the example below there are two partitions, named [Root] and Finance. Finance is called a child partition of [Root], since it was split off from [Root]. [Root] is called the parent partition of Finance.



You might create such a partition because the Directory has so many objects that the server is overwhelmed and access to NDS is slow. Creating the new partition allows you to split the database and pass the objects in that branch to a different server.

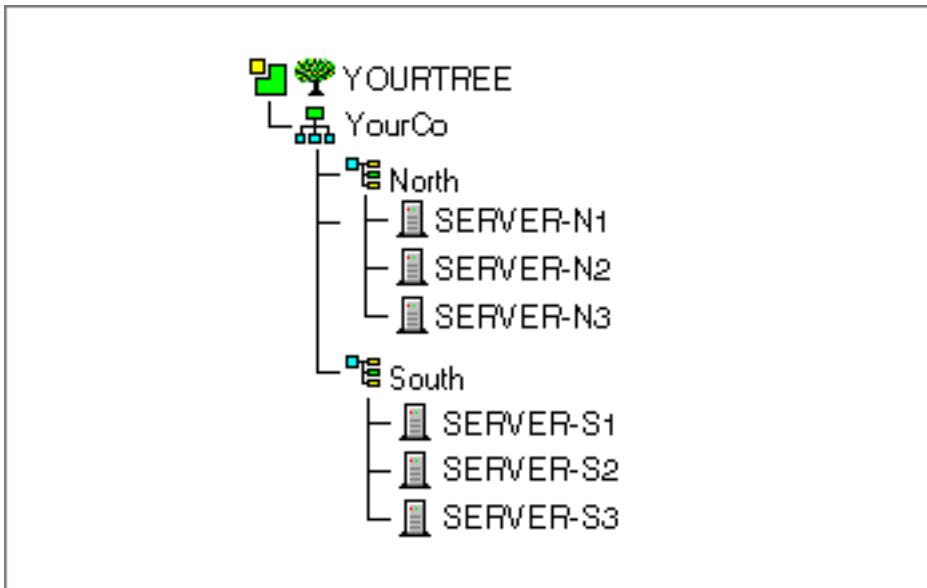
Distributing Replicas for Performance

In the example above, suppose that server SERVER1 holds replicas of both the [Root] partition and the Finance partition. At this point, you haven't gained any performance advantage from NDS since SERVER1 still holds the entire Directory (replicas of both partitions).

To gain the desired performance advantage, you need to move one of the replicas to a different server. For instance, if you move the [Root] partition to SERVER2, then SERVER2 holds all objects in the [Root] and YourCo containers. SERVER1 only holds objects in the Finance and Accounts containers. The load on both SERVER1 and SERVER2 is less than it would be with no partitioning.

Partitioning and WAN Links

Suppose your network spans two sites, a North site and a South Site, separated by a WAN link. Three servers are at each site.



NDS performs faster and more reliably in this scenario if the Directory is divided in two partitions. The following explanation tells why.

Single Partition Solution

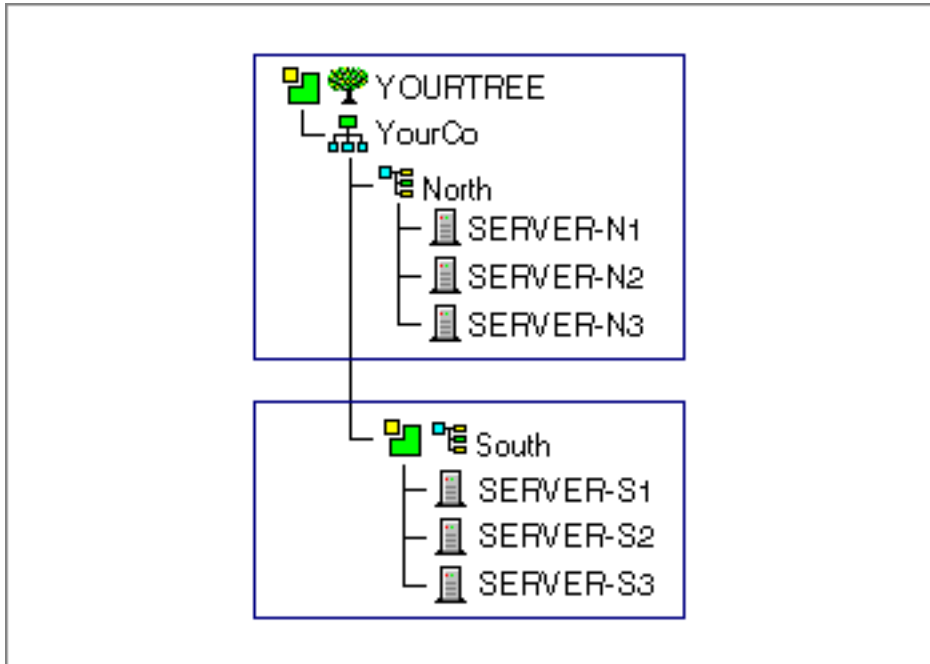
With a single partition, the replicas are either kept at one site or distributed between the two sites. This proves unwieldy for two reasons:

- ♦ If all replicas are kept on servers at the North site, for instance, users at the South site encounter delays when logging in or accessing resources. If the link goes down, users at the South site can't log in or access resources at all.

- ♦ If replicas are distributed between sites, users can access the Directory locally. However, server-to-server synchronization of replicas happens over the WAN link, so there can be NDS errors if the link is unreliable. Any changes to the Directory are slow to propagate across the WAN link.

Two-Partition Solution

The two-partition solution shown below solves performance and reliability problems over the WAN link.



Replicas of the [Root] partition are kept on servers at the North site. Replicas of the South partition are kept on servers at the South site, as shown below.

Partition	Server	Replica Type
 [Root]	 SERVER-N1	 Master
	 SERVER-N2	 Read/write
	 SERVER-N3	 Read/write
 South	 SERVER-S1	 Master
	 SERVER-S2	 Read/write
	 SERVER-S3	 Read/write

For each site, the objects that represent local resources are kept locally. Synchronization traffic among servers also happens locally over the LAN, rather than over the slow, unreliable WAN link.

NDS traffic is generated over the WAN link, however, when a user or administrator accesses objects at a different site.

Object Classes and Properties

Each type of NDS object is called an object class. For instance, User and Organization are object classes. Each class of object has certain properties. A User object, for example, has Login Name, Password, Last Name, and many other properties.

A set of rules called the schema defines the object classes and properties, along with the rules of containment (what containers can contain which

objects). NDS ships with a base schema that you, or the applications you use, can extend.

Container objects contain other objects and are used to divide the tree into branches, while leaf objects represent network resources. The object classes listed below don't constitute an exhaustive list. These are only some often-used classes. For more information, click on an object or its icon below. For classes not shown, see "List of Objects" on page 43.

Container Object Classes

[Root]



Organization



Organizational Unit



Country



Leaf Object Classes

NetWare Server



Volume



User



Group



Alias



Directory Map



Profile



NDS Rights

When you create an NDS tree, the default rights assignments give your network generalized access and security. Some of the default assignments are as follows:

- ♦ User Admin has the Supervisor right to [Root], giving Admin complete control over the entire Directory. Admin also has the Supervisor right to the NetWare* Server object, giving complete control over any volumes on that server.
- ♦ [Public] has the Browse right to [Root], giving any user the right to view any objects in the NDS tree.
- ♦ Objects created through an upgrade process such as a NetWare migration, printing upgrade, or Windows NT** user migration receive NDS trustee assignments appropriate for most situations.

For an explanation of trustees and target objects, see “Trustee Assignments and Targets” on page 62.

NDS Rights Concepts

Following is a list of concepts that will help you understand NDS rights.

“Inheritance” on page 15

“Object Rights” on page 63

“Property Rights” on page 64

“Effective Rights” on page 66

“Security Equivalence” on page 67

“Access Control List (ACL)” on page 67

“Inherited Rights Filter (IRF)” on page 68

“Default Rights for a New NetWare Server” on page 69

“Delegated Administration” on page 70

Synchronizing Servers in the Replica Ring

When multiple servers hold replicas of the same partition, those servers are considered a replica ring. NDS automatically keeps those servers synchronized, so the object data is consistent on all replicas.

The following NDS processes keep servers in the replica ring synchronized.

- ♦ Replica synchronization
- ♦ Schema synchronization
- ♦ Limber
- ♦ Backlink
- ♦ Connection management

If Your Network Needs a Bindery

Many applications, such as print servers and backup software, were written for NetWare* versions previous to NetWare 4. These applications used the NetWare bindery instead of NDS for network access and object manipulation.

The bindery is a flat database of objects such as Users, Groups, and Volumes known to a given server. The bindery is server-specific and server-centric.

Older NetWare client software (such as the NETX bindery shell) used a bindery login procedure in which a user logged in to a specific server only. Access to multiple servers required multiple logins using multiple user accounts.

NDS allows applications written for a bindery to function using bindery services. Bindery services allows you to set a context or a number of contexts as a server's virtual bindery. The context you set is called a server's bindery context.

Following are some important facts about bindery services:

- ♦ To use bindery services, you must set a bindery context for the server.
- ♦ Not all NDS objects map to bindery objects. Many NDS objects, such as Alias objects, do not have a bindery equivalent.
- ♦ Most bindery applications have been upgraded to work with NDS. Check with your application vendor to get the newest version.
- ♦ Each server (before NetWare 5) with a bindery context must hold a master or read/write replica of the partition that includes the bindery context.

The Importance of Synchronizing Time

In a single server environment, the server's internal clock is adequate to maintain a common and consistent time source for the network.

For a multiple-server network, NDS (like many applications that use time stamps) requires that servers agree on time.

Time synchronization offers three benefits:

- ♦ Applications that run on your server provide accurate time stamps to events. Messaging and collaboration applications and databases all benefit from synchronized time.
- ♦ Workstations can be configured to get their time from servers, taking synchronized time benefits to locally-run applications.
- ♦ NDS applies correct time stamps to NDS events.

When changes are made to NDS objects, the changes can be made to different replicas on different servers. These changes must be enacted in the order in which they were requested.

An example of this would be one administrator renaming an object and another moving the object. If these events were applied out of sequence, the object might not be renamed because it would not exist in the original context.

NDS records the time of each event with a time stamp. When NDS actually modifies the database, the particular event occurs in the time and order that it was intended. NDS also uses time stamps to record time values for the network and set expiration dates.

2

Planning Your NDS Tree

This section gives you planning information for creating an NDS™ tree. It will help you decide whether to accept the default tree when installing your first NDS server and give you recommended solutions for networks that are large, complex, or that span multiple campuses.

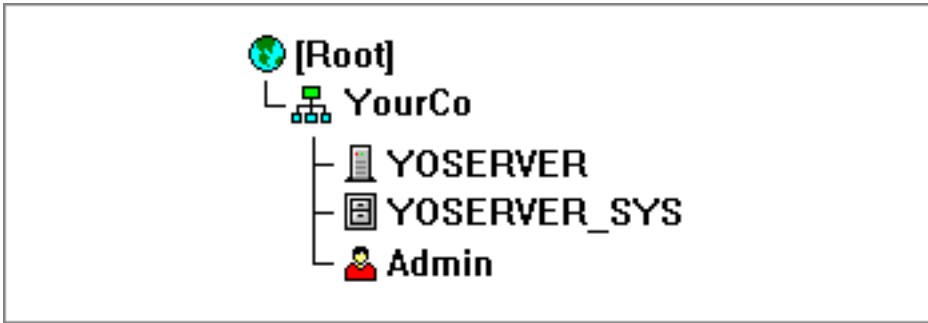
Start with the Defaults

Does your network have fewer than 1,000 objects (users and resources)? Are all servers connected by reliable LAN links? If the answer to both questions is yes, then you have a small network in NDS terms.

For small networks, you don't need to use the more advanced features of NDS (although understanding them can help). NDS takes care of itself with its default settings. Some of these defaults are as follows:

- ♦ NDS keeps the Directory in one partition, without dividing it.
- ♦ NDS replicates the Directory to the first three NDS servers on the network. Those replicas are kept synchronized automatically.
- ♦ One NDS tree is created, rather than multiple trees.
- ♦ A single Organization object is created and named after your company.
- ♦ The Admin User object is created in the Organization container, as are the NetWare™ Server and Volume objects.

The picture below shows the default NDS tree for a small network. It has the required [Root] object, an Organization named after your company, a server (named YOSERVER in this example), a volume (named YOSERVER_SYS in this example), and a User object named Admin.



NOTE: Networks with only a Windows NT* server running NDS will have no Volume objects.

Users are added individually using NWAdmin, or in batches through a migration, upgrade, or import utility. The default NDS tree has a single container: an Organization object named after your company (YourCo in the example).

For small networks, this configuration is adequate; you can add new User objects, Application objects, printing-related objects, and other useful objects to the YourCo container.

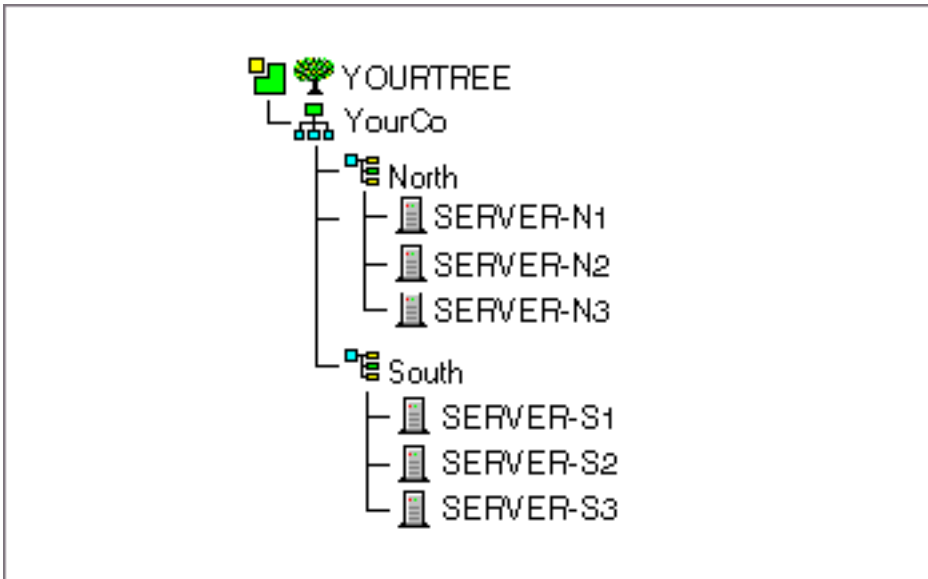
You may want to plan new container objects in the upper levels of the tree for either or both of the reasons listed below.

- ♦ Your network has slow or unreliable WAN links
- ♦ Your network has more than 1,000 users

After designing of the upper levels of the tree, you should plan workgroup containers and leaf objects.

Accommodate Slow or Unreliable WAN Links

Slow or unreliable WAN links affect your NDS tree design. You should create containers for each site separated by such links, placing each NetWare Server object in its local container.

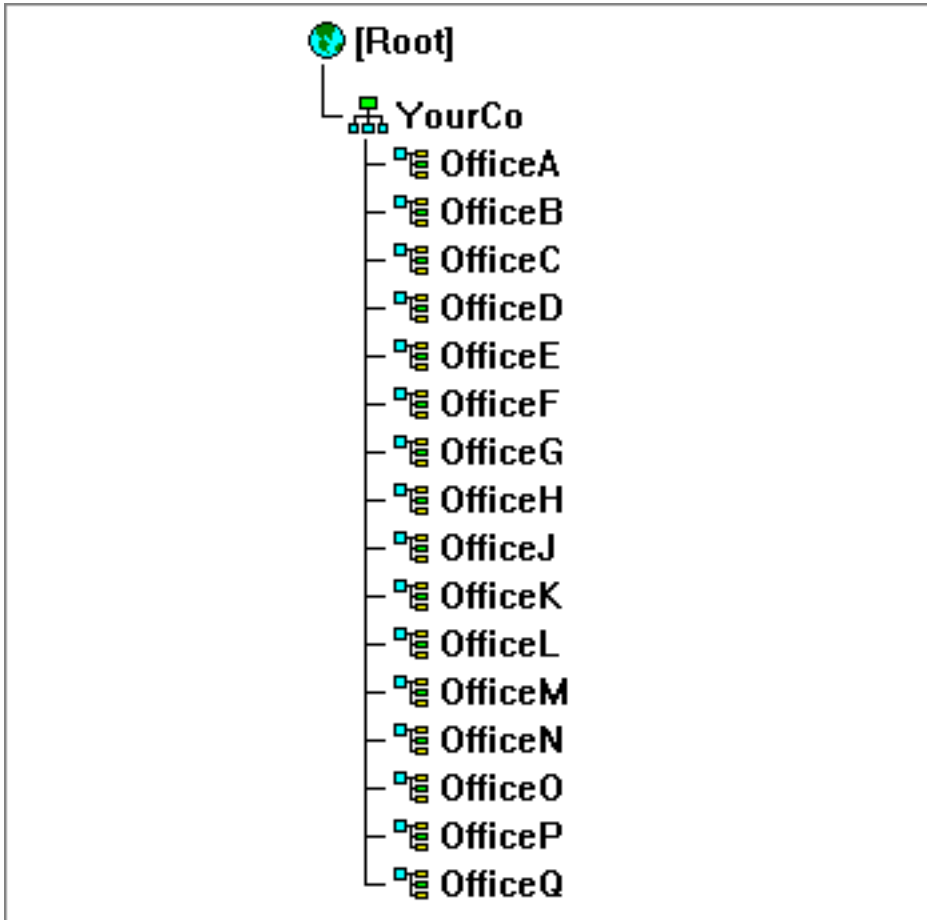


The advantage of this level of site containers is partitioning. Objects representing local resources can be kept on a local partition, eliminating synchronization traffic over the WAN.

Another benefit is that resources and volumes are kept in a branch of the tree in common with the users that access them. This simplifies administration of NDS rights and login scripts.

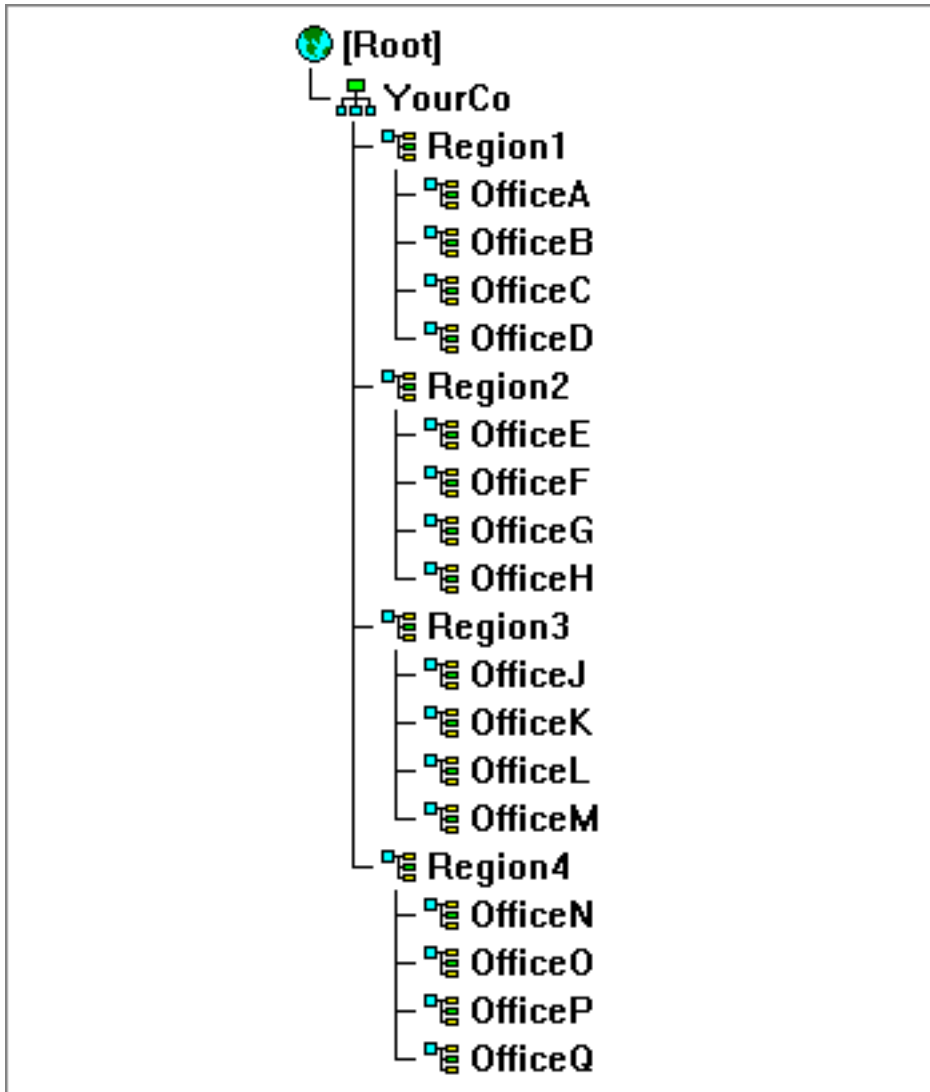
Avoiding a Flat Tree

In organizations with numerous branch offices, you might naturally create a flat tree, with numerous Organizational Units under the Organization. A sample flat tree is shown below.



A flat tree produces inefficiencies that have to be overcome by NDS processes. These inefficiencies can lead to poor performance and a less user-friendly environment for users and administrators.

To avoid the inefficiencies of a flat tree, create intermediate containers that subdivide the tree, usually into regions, as shown below.



You may need to further subdivide the tree to restrict partitions to about 1,000 objects. After designing of the upper levels of the tree, plan workgroup containers and leaf objects.

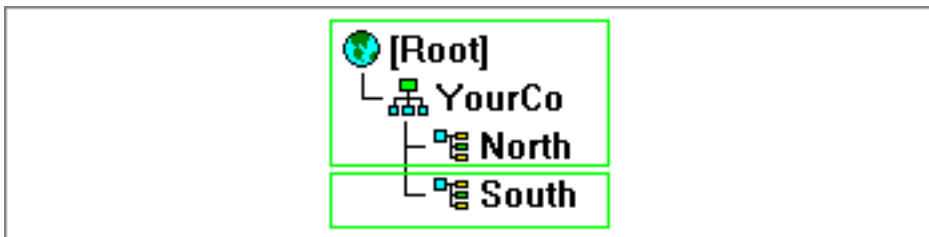
Restrict Partitions to 1,000 Objects

NDS performs best with about 1,000 objects or fewer per partition. This number is approximate, since other variables also affect performance, such as:

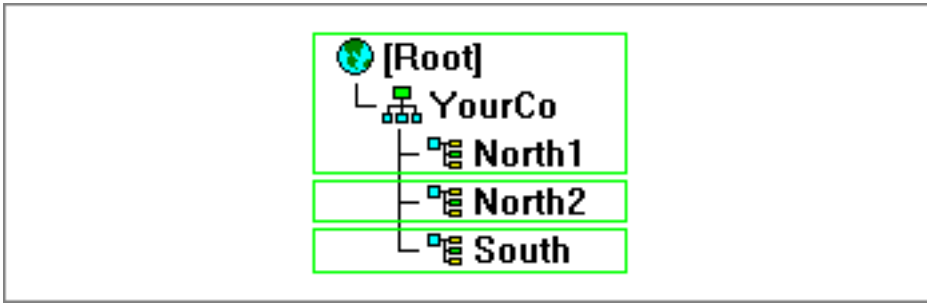
- ♦ The number and speed of servers
- ♦ The speed of network infrastructure, such as network adapters, hubs, and routers
- ♦ The amount of network traffic

Since you create partitions based on container objects, the upper levels of your NDS tree should reflect your partitioning strategy.

Suppose, for instance, that you have already planned Organizational Units (and partitions) for your company's North and South sites. Your plan for the NDS tree, with partitions shown in green, might look like the example below:



This is a good start for designing the upper levels of the tree. At this point, though, you should consider the number of objects per partition. For example, if you project 1,500 objects at the North site and 500 objects at the South site, you will want an additional Organizational Unit (and partition) at the North site. See the example below.



The additional Organizational Unit and partition should represent a distinct division of the LAN topology, such as the physical network in one building or one floor of a building.

Whenever you plan a new partition, you should also plan enough servers to hold replicas of that partition. Three replicas are recommended per partition, hosted on different NDS servers. In the example above, you would need nine NDS servers.

After designing of the upper levels of the tree, you should plan workgroup containers and leaf objects.

Plan Workgroup Containers and Leaf Objects

After designing the upper layers of the NDS tree for an efficient partitioning strategy, you can add workgroup containers and leaf objects to the lower layers.

Create workgroup Organizational Units for sets of users that generally have common resource requirements, such as printers, file systems, and applications. If workgroups tend to have hundreds of User objects and more than one network administrator, you can subdivide workgroups around management responsibilities.

Planning an Organizational Unit for each workgroup lets you make a common trustee assignment and login script for the User objects in that workgroup. It also simplifies naming in the common context.

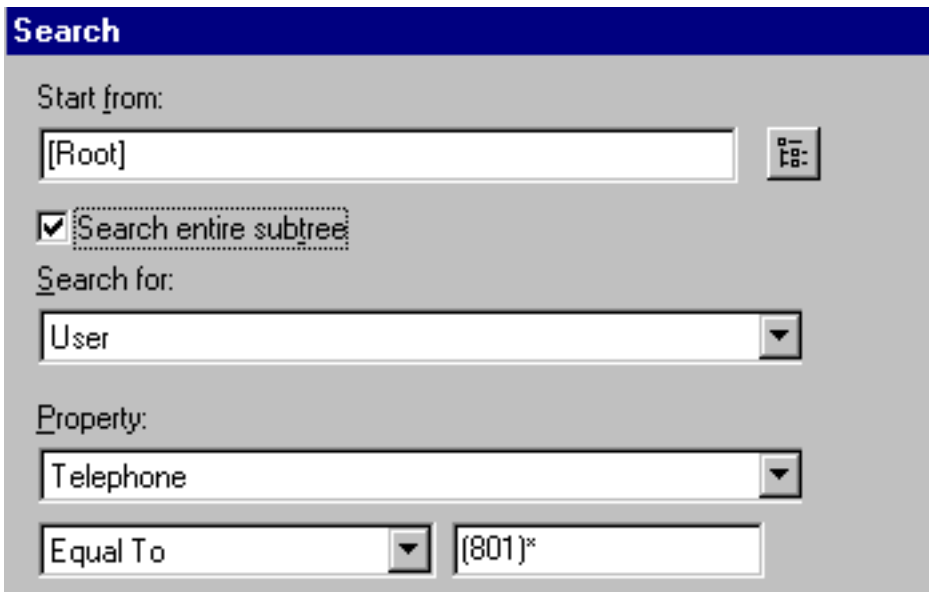
Workgroup Exceptions

Exceptions to general workgroup boundaries are not hard to manage. If two workgroups use a common printer, for instance, you can create an Alias to the printer in one of the workgroups. You can create Group objects to manage some User objects within a workgroup or User objects across multiple workgroups. You can create Profile objects for subsets of users with unique login script requirements.

Standardize Property Values

Using standard property values such as object names makes your network more intuitive to both users and administrators. Written standards can also specify how administrators set other property values, such as telephone numbers and addresses.

Searching and browsing the Directory rely greatly on the consistency of property values. For instance, the NWAdmin Search window below shows a search for User objects with a telephone number beginning with '(801).'



The screenshot shows the 'Search' window in NWAdmin. It has a blue title bar with the word 'Search'. Below the title bar, there are several fields and controls:

- 'Start from:' label followed by a text box containing '[Root]' and a small square icon with a tree structure.
- A checked checkbox labeled 'Search entire subtree'.
- 'Search for:' label followed by a dropdown menu showing 'User'.
- 'Property:' label followed by a dropdown menu showing 'Telephone'.
- 'Equal To' label followed by a dropdown menu and a text box containing '(801)*'.

If some of the values for the Telephone property were entered beginning with 1-801, the search returns an incomplete list of results.

Following is a sample document containing standards for some of the most often used properties. Of course, you only need to have standards for those properties you use. You should distribute the standards document to all administrators responsible for creating or modifying objects.

<i>Object Class Property</i>	<i>Standard</i>	<i>Examples</i>	<i>Rationale</i>
User Login name	First initial, middle initial (if applicable), last name (all lowercase), 8 characters maximum. All common names are unique in the company	msmith, bgashler	Using unique names company-wide is not required by NDS but helps avoid conflicts within the same context (or bindery context).
User Last name	Last name (normal capitalization)	Van Pelt	Used for generation of mailing labels.
Telephone and fax numbers	Numbers separated by dashes	US: 123-456-7890 Other: 44-344-123456	Used by autodialing software.
Multiple classes Location	Two-letter location code (uppercase), dash, mail stop	BA-C23	Used by interoffice mail carriers.
Organization Name	YourCo for all trees.	YourCo	If you have separate trees, a standard Organization name allows for future merging of trees.
Organizational Unit Name (based on location)	Two or three-letter location code, all uppercase	ATL, CHI, CUP, LA, BAT, BOS, DAL	
Organizational Unit Name (based on department)	Department name or abbreviation	Sales, Eng	Short, standard names are used for efficient searching.
Group Name	Descriptive name	Project Managers	
Directory Map Name	Contents of the directory indicated by the Directory Map	DOSAPPS	

Profile Name	Purpose of the profile	MobileUser	
NetWare Server Name	SERV, dash, department, dash, unique number	SERV-Eng-1	NDS requires server names to be unique in the tree

3

Objects and Rights

This section contains a list of NDS object classes, a description of each container object, and information on each object’s usage. It also gives you information to help you assign NDS rights, set up default rights for a new NetWare server, and delegate administration.

List of Objects

The following tables list NDS™ object classes. Note that added services can create new object classes in NDS that are not listed below. Also, all classes may not be available on all server operating systems hosting NDS.

<i>Container Object (Abbreviation)</i>	<i>Description</i>
[Root]	Represents the beginning of your NDS tree.
	
Country (C)	Designates the countries where your network resides; also organizes other Directory objects within the country. See also “Country” on page 50.
	

Licensed Product (LP) 	Created automatically when you install a license certificate or create a metering certificate using Novell Licensing Services (NLS) technology. When an NLS-enabled application is installed, it adds a Licensed Product container object to the NDS tree and a License Certificate leaf object to that container.
Organization (O) 	Helps you organize other objects in the Directory. The Organization object is a level below the Country object (if you use the Country object). See also “Organization” on page 47.
Organizational Unit (OU) 	Helps you to further organize other objects in the Directory. The Organizational Unit object is a level below the Organization object. See also “Organizational Unit (OU)” on page 49.
<i>Leaf Object</i>	<i>Description</i>
AFP Server 	Represents an AppleTalk Filing Protocol server that operates as a node on your NDS network. It usually also acts as a NetWare router to, and the AppleTalk server for, several Macintosh* computers.
Alias 	Points to the actual location of an object in the Directory. Any Directory object located in one place in the Directory can also appear to be in another place in the Directory by using an Alias. See also “Alias” on page 57.
Application 	Represents a network application. Application objects simplify administrative tasks such as assigning rights, customizing login scripts, and launching applications.
Computer 	Represents a computer on the network.

Directory Map	Refers to a directory in the file system. See also "Directory Map" on page 59.
	
Group	Assigns a name to a list of User objects in the Directory. You can assign rights to the group instead of to each user, then the rights transfer to each user in the group. See also "Group" on page 56.
	
License Certificate	Used with Novell Licensing Services (NLS) technology to install product license certificates as objects in the NDS database. License Certificate objects are added to the Licensed Product container when an NLS-aware application is installed.
	
NetWare Server	Represents a server running any version of NDS. See also "NetWare Server" on page 51.
	
Organizational Role	Defines a position or role within an organization.
	
Print Queue	Represents a network print queue.
	
Print Server	Represents a network print server.
	
Printer	Represents a network printing device.
	

Profile	Represents a login script used by a group of users who need to share common login script commands. The users don't have to be in the same container in the NDS tree. See also "Profile" on page 61.
	
Template	Represents standard User object properties that can be applied to new User objects.
	
User	Represents the people who use your network. See also "User" on page 53.
	
Unknown	Represents an NDS object that has been corrupted and can't be identified as belonging to any of the other object classes.
	
Volume	Represents a physical volume on the network. See also "Volume" on page 52.
	

[Root]

The [Root] container is created when you first install NDS on a server in your network. As the topmost container, it usually holds Organization objects, Country objects, or Alias objects.

What [Root] Represents

[Root] represents the beginning of your NDS tree.

Usage

[Root] is used to make universal rights assignments. Because of inheritance, any rights assignments you make to [Root] as the target apply to all objects in

the tree. The [Public] trustee has the Browse right and Admin has the Supervisor right to [Root] by default.

Important Properties

The [Root] object has a Name property, which is the tree name you supplied when installing the first server. The tree name is shown in the title bar of NWAdmin.

Organization

An Organization container object is created when you first install NDS on a server in your network. As the topmost container under [Root], it usually holds Organizational Unit objects and leaf objects.

The User object named Admin is created by default in your first Organization container.

What an Organization Object Represents

Normally the Organization object represents your company, although you can create additional Organization objects under [Root]. This is typically done for networks with distinct geographical districts or for companies with separate NDS trees that have merged.

Usage

The way you use Organization objects in your tree depends on the size and structure of your network. If the network is small, you should keep all leaf objects under one Organization object.

For larger networks, you can create Organizational Unit objects under the Organization to make resources easier to locate and manage. For instance, you could create Organizational Units for each department or division in your company.

For networks with multiple sites, you should create an Organizational Unit for each site under the Organization object. That way, if you have (or will have) enough servers to partition the Directory, you can do so logically along site boundaries.

For easy sharing of company-wide resources, such as printers, volumes, or applications, create corresponding Printer, Volume, or Application objects under the Organization.

Important Properties

The following properties (and many more) are available for the Organization object. Only the Name property is required. For a complete list of properties, select an Organization object in NWAdmin, then choose Object > Details. To display a description for each page of properties, click Help.

Name

Typically, the Name property is the same as your company's name. Of course, you can shorten it for simplicity. For instance, if the name of your company is Your Shoe Company, you might use YourCo.

The Organization name becomes part of the context for all objects created under it.

Login Script

The Login Script property contains commands that are executed by any User objects directly under the Organization. These commands are run when a user logs in.

Applications

The Applications property lists all applications you have set up for this context. Users view and work with applications via the Novell® Application Launcher (NAL) Window and NAL Explorer desktop software.

Applications are associated with an Organization from the Application object's Associations property page. When an application is associated with an Organization object, User objects in that Organization are (by default) presented the application through the NAL Window.

Launcher Configuration

Use the Launcher Configuration properties to specify how users view and work with the Novell Application Launcher (NAL) Window and NAL Explorer desktop software. Use this property to allow users to inherit applications through multiple levels of the NDS tree.

Organizational Unit (OU)

You can create Organizational Unit (OU) container objects to subdivide the NDS tree. Organizational Units are created with NWAdmin under an Organization, Country, or another Organizational Unit object.

Organizational Units can contain other Organizational Units and leaf objects such as User and Application objects.

What an Organizational Unit Object Represents

Normally the Organizational Unit object represents a department, which holds a set of objects that commonly need access to each other. A typical example is a set of Users, along with the Printers, Volumes, and Applications that those Users need.

At the highest level of Organizational Unit objects, each Organizational Unit can represent each site (separated by WAN links) in the network.

Usage

The way you use Organizational Unit objects in your tree depends on the size and structure of your network. If the network is small, you probably don't need any Organizational Units.

For larger networks, you can create Organizational Unit objects under the Organization to make resources easier to locate and manage. For instance, you could create Organizational Units for each department or division in your company. Remember that administration is easiest when you keep User objects together in the Organizational Unit with the resources they use most frequently.

For networks with multiple sites, you should create an Organizational Unit for each site under the Organization object. That way, if you have (or will have) enough servers to partition the Directory, you can do so logically along site boundaries.

Important Properties

The following properties (and many more) are available for the Organizational Unit object. Only the Name property is required. For a complete list of properties, select an Organizational Unit object in NWAdmin, then choose Object > Details. To display a description for each page of properties, click Help.

Name

Typically, the Name property is the same as the department name. Of course, you can shorten it for simplicity. For instance, if the name of your department is Accounts Payable, you can shorten it to AP.

The Organizational Unit name becomes part of the context for all objects created under it.

Login Script

The Login Script property contains commands that are executed by any User objects directly under the Organizational Unit. These commands are run when a user logs in.

Applications

The Applications property lists all applications you have set up for this context. Users view and work with applications via the Novell Application Launcher (NAL) Window and NAL Explorer desktop software.

Applications are associated with an Organizational Unit from the Application object's Associations property page. When an application is associated with an Organization object, User objects in that Organization are (by default) presented the application through the NAL Window.

Launcher Configuration

Use the Launcher Configuration properties to specify how users view and work with the Novell Application Launcher (NAL) Window and NAL Explorer desktop software. Use this property to allow users to inherit applications through multiple levels of the NDS tree.

Country

You can create Country objects directly under [Root] using NWAdmin. Country objects are optional and only required for connection to certain X.500 global directories.

What a Country Object Represents

The Country object represents the political identity of its branch of the tree.

Usage

Most administrators do not create a Country object, even if the network spans countries, since the Country object only adds an unnecessary level to the NDS tree. You can create one or many Country objects under [Root], depending on the multinational nature of your network. Country objects can only contain Organization objects.

If you do not create a Country object and find that you need one later, you can always modify the tree to add one.

Important Properties

The Country object has a two-letter Name property.

Name

Country objects are named with a standard two-letter code such as US, UK, or DE. For a list of standard abbreviations, see also Naming Countries.

NetWare Server

A NetWare[®] Server object is created in the NDS tree automatically whenever you install NDS on a server. Although the object class is called a *NetWare* Server, it can be an IntranetWare[™], UNIX*, or other server running NDS.

You can also create a NetWare Server object to represent a NetWare 2 or NetWare 3 bindery server.

What a NetWare Server Object Represents

The NetWare Server object represents a server running NDS, or a bindery-based (NetWare 2 or NetWare 3) server.

Usage

The NetWare Server object serves as a reference point for replication operations. A NetWare Server object that represents a bindery-based server allows you to manage the server's volumes with NWAdmin.

Important Properties

The NetWare Server object has a Network Address property, among others. For a complete list of properties, select a NetWare Server object in NWAdmin,

then choose Object > Details. To display a description for each page of properties, click Help.

Network Address

The network address property displays the protocol and address number for the server. This is useful for troubleshooting at the packet level.

Volume

When you create a physical volume on a server, a Volume object is automatically created in the NDS tree. By default, the name of the Volume object is the server's name with an underscore and the physical volume's name appended (example: YOSERVER_SYS).

What a Volume Object Represents

A Volume object represents a physical volume on a server, whether it is a writable disk, a CD-ROM, or other storage medium. The Volume object in NDS does not contain information about the files and directories on that volume, though you can access that information through NWAdmin. File and directory information is retained in the file system itself.

Usage

Using NWAdmin, you can click the Volume icon to manage files and directories on that volume. NWAdmin provides information about the volume's free disk space, directory entry space, and compression statistics.

You can also create Volume objects in the NDS tree for NetWare 2 and NetWare 3 volumes.

Important Properties

In addition to the required Name and Host Volume properties, there are other important Volume properties.

Name

This is the name of the Volume object in the NDS tree. By default, this name derives from the name of the physical volume, though you can change the object name.

Host Server

This is the server on which the volume resides.

Version

The Version property gives the NetWare or NDS version of the server hosting the volume.

Host Volume

This is the physical volume name. Since the actual Volume object name does not need to reflect the physical volume name, this property is necessary to associate the Volume object with the physical volume.

User

A User object is required for logging in. When you install the first server into an NDS tree, a User object named Admin is created. The first time you log in, you will use the Admin account.

You can create User objects with NWAdmin, or import them automatically from Windows NT* domains using NDS for NT. You can also import User objects in batches from database files. Additionally, NetWare upgrade utilities import Users from existing bindery servers.

What a User Object Represents

A User object represents a person who uses the network.

Usage

You should create User objects for all users who need to use the network. Although you can manage User objects individually, you'll save time by

- ♦ Using Template objects to set default properties for most User objects. The Template applies automatically to new Users you create (not to already-existing ones).
- ♦ Creating Group objects to manage sets of Users.
- ♦ Assigning rights using the container objects as trustees when you want that assignment to apply to all User objects in the container.

- ♦ Selecting multiple Users. When you do (with standard Windows* shift-clicking or control-clicking), you can change property values for all selected User objects.

Important Properties

User objects have over 80 properties. For a complete list of properties, select a User object in NWAdmin, then choose Object > Details. To display a description for each page of properties, click Help.

The Login Name and Last Name properties are required. These and some of the most useful properties are listed below.

Account Expiration Date

This property lets you limit the life of a user account. After the expiration date, the account is locked so the user cannot log in.

Account Disabled

This property has a system-generated value that indicates a lock on the account so the user cannot log in. The lock might occur if the account has expired or because the user has given too many incorrect passwords in succession.

Force Periodic Password Changes

This property allows you to enhance security by requiring the user to change passwords after a specified interval.

Group Membership

This property lists all the Group Objects that include the User as a member.

Home Directory

The Home Directory property refers to a NetWare volume and file system path for the user's own files. Most administrators like to create such a directory so that a user's working files can be kept on the network.

The directory referred to in this property can be created automatically when you create the User object.

Last Login

This is a system-generated property that lists the date and time that the user last logged in.

Last Name

The Last Name property, though required, is not used directly by NDS. Applications that take advantage of the NDS name base can use this property, along with other identification properties such as Given Name, Title, Location, and Fax Number.

Limit Concurrent Connections

This property allows you to set the maximum number of sessions a user can have on the network at any given time.

Login Name

This is the name shown in NWAdmin by the User icon. It is also the name supplied by the user when logging in.

NDS does not require that login names be unique throughout the network, only in each container. However, you may want to keep login names unique across the company to simplify administration.

Typically, login names are a combination of first and last names, such as JOHNT or JTHOMAS for John Thomas.

Login Script

The Login Script property allows you to create specific login commands for a User. When a user logs in, the container login script runs first. Then a profile login script runs if the User has been added to the membership list of a Profile object. Finally, the user login script runs (if one exists).

You should put most of the login commands in container login scripts to save administrative time. The User login script can be edited to manage unique exceptions to common needs.

Login Time Restrictions

This property allows you to set times and days when the user can log in.

Network Addresses

This property contains system-generated values that list all the IPX and/or IP addresses from which the User is logged in. These values are useful for troubleshooting network problems at the packet level.

Require a Password

This property allows you to control whether the user must use a password. Other related properties let you set common password constraints such as password length.

Rights to Files and Directories

This property lists all rights assignments made for this user to the NetWare file system. Using NWAdmin, you can also check a user's effective rights to files and directories, which include those inherited from other objects.

Group

You can create Group objects in NWAdmin to help you manage sets of User objects.

What a Group Object Represents

A Group object represents a set of User objects.

Usage

While container objects let you manage all User objects in that container, Group objects are for subsets within a container or in multiple containers.

Group objects have two main purposes:

- ♦ They allow you to grant rights to a number of User objects at once.
- ♦ They allow you to specify login script commands using 'IF MEMBER OF...' syntax.

Important Properties

The most important properties of the Group object are Members and Rights to Files and Directories. For a complete list of properties, select a Group object in NWAdmin, then choose Object > Details. To display a description for each page of properties, click Help.

Members

This property lists all User objects in the group. Rights assignments made to the Group object apply to all members of that group.

Rights to Files and Directories

This property lists all trustee assignments made for this Group to the NetWare file system.

Alias

You can create an Alias object that points to another object in the NDS tree. Alias objects are most commonly used to give users a local name for an object that lies outside their container.

When you rename a container, you have the option of creating an alias in the former container's place that points to the new name. Workstations and login script commands that reference objects in the container can still access the objects without having the container name updated.

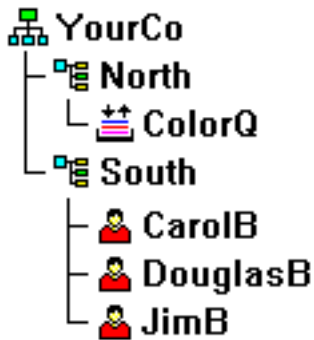
What an Alias Object Represents

An Alias object represents another object, which can be a container, User, or any other object in the tree. An Alias object does not carry trustee rights of its own. Any trustee authority you grant to the Alias object applies to the object it represents. The Alias can be a target of a trustee assignment, though.

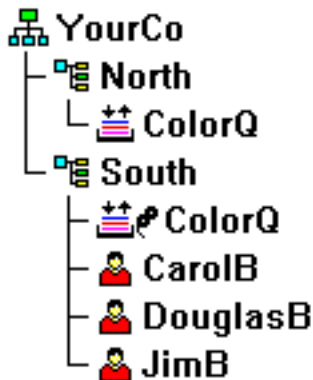
Usage

Create an Alias object to make name resolution easier. Since object naming is simplest for objects in the current context, you should create Alias objects there that point to any resources outside the current context.

For example, suppose users log in and establish a current context in the South container as shown below, but need access to the Print Queue object named ColorQ in the North container.



You can create an Alias object (shown with the icon below) in the South container.



The Alias points to the original ColorQ object, so setting up printing for the users involves a 'local' object.

Important Properties

Alias objects have an Aliased Object property, which associates the Alias with the original object.

Directory Map

A Directory Map object is a pointer to a path in the NetWare file system. It allows you to make simpler references to directories.

If your network has no NetWare volumes, you cannot create Directory Map objects.

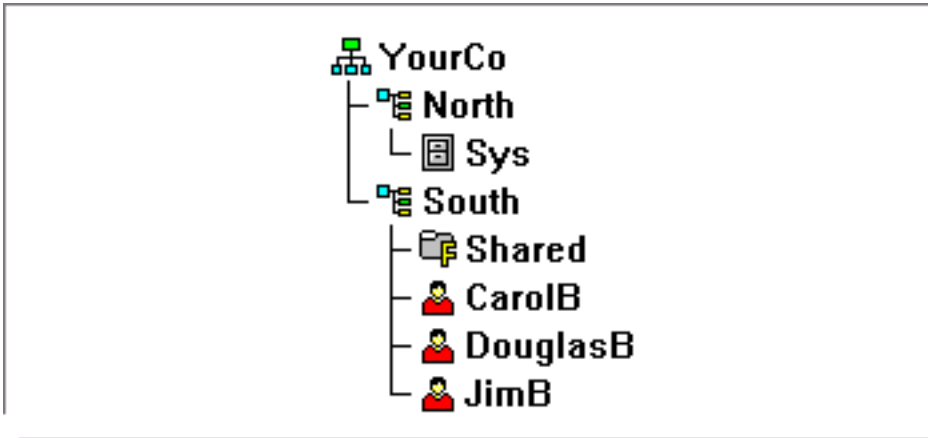
What a Directory Map Object Represents

A Directory Map object represents a directory on a NetWare volume. (An Alias, on the other hand, represents an NDS object.)

Usage

Create a Directory Map object to make drive mapping simpler, particularly in login scripts. Using a Directory Map object allows you to reduce complex file system paths to a single name.

Also, when you change the location of a file, you don't need to change login scripts and batch files to reference the new location. You only need to edit the Directory Map object. For example, suppose you were editing the login script for the container South, shown below.



A command mapping drives to the SHARED directory on volume SYS would look like the following:

MAP N:=SYS.North.:Shared

If you created the Shared Directory Map object, the map command would be much simpler:

MAP N:=Shared

Important Properties

The Directory Map object has Name, Volume, and Path properties.

Name

The Name property identifies the object in the Directory (for example, Shared), and is used in MAP commands.

Volume

The Volume property contains the name of the Volume object that the Directory Map object references, such as Sys.North.YourCo.

Path

The Path property specifies the directory as a path from the root of the volume, such as PUBLIC\WIN95\NLS\ENGLISH.

Profile

Profile objects help you manage login scripts.

What a Profile Object Represents

A Profile object represents a login script which runs after the container login script and before the user login script.

Usage

Create a Profile object if you want login script commands to run for only selected users. The User objects can exist in the same container or be in different containers. Once you have created the Profile, you add the commands to its Login Script property. Then make the User objects trustees of the Profile and add the Profile to their Profile Membership property.

Important Properties

The Profile object has two important properties, as explained below: Login Script and Rights to Files and Directories.

Login Script

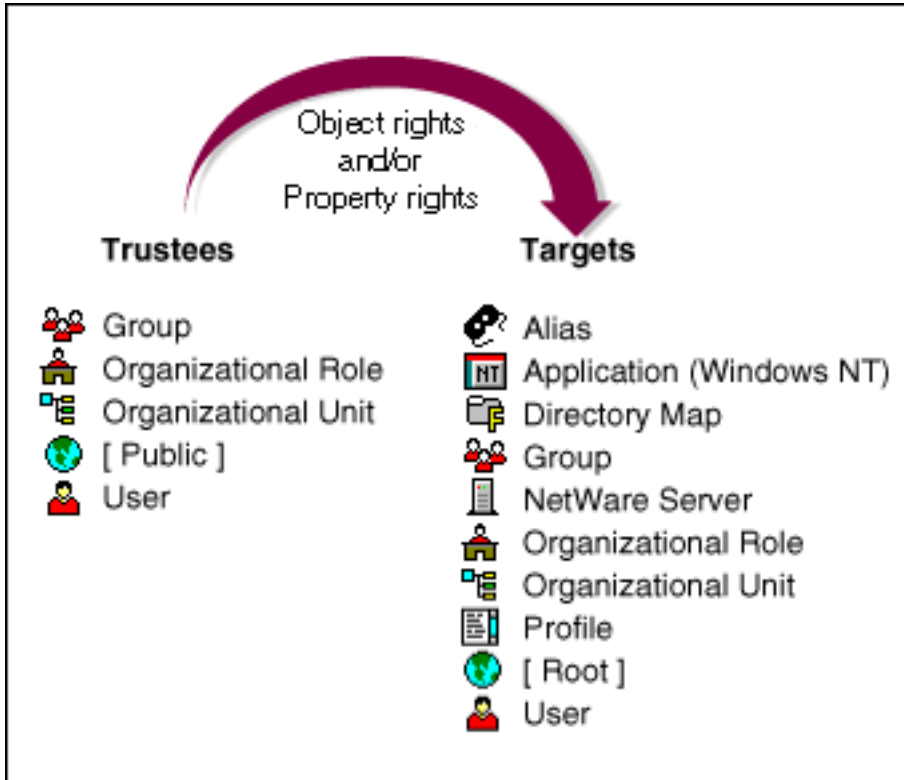
The login script property contains the commands you want to run for users of the Profile.

Rights to Files and Directories

If you have INCLUDE statements in the login script, you need to give the Profile object rights to the files included. This is done with the Rights to Files and Directories property. For more information on INCLUDE statements and other login script commands, see Login Script.

Trustee Assignments and Targets

The assignment of NDS rights involves a trustee and a target object. The trustee represents the user or set of users which are receiving the authority. The target represents those network resources the users have authority over. Although any object can be either a trustee or target, objects used in typical trustee assignments are illustrated below.



NOTE: If you make an Alias a trustee, the rights apply only to the object it represents. The Alias object can be an explicit target, however.

A file or directory in the NetWare file system can also be a target, although file system rights are stored in the file system itself, not in NDS.

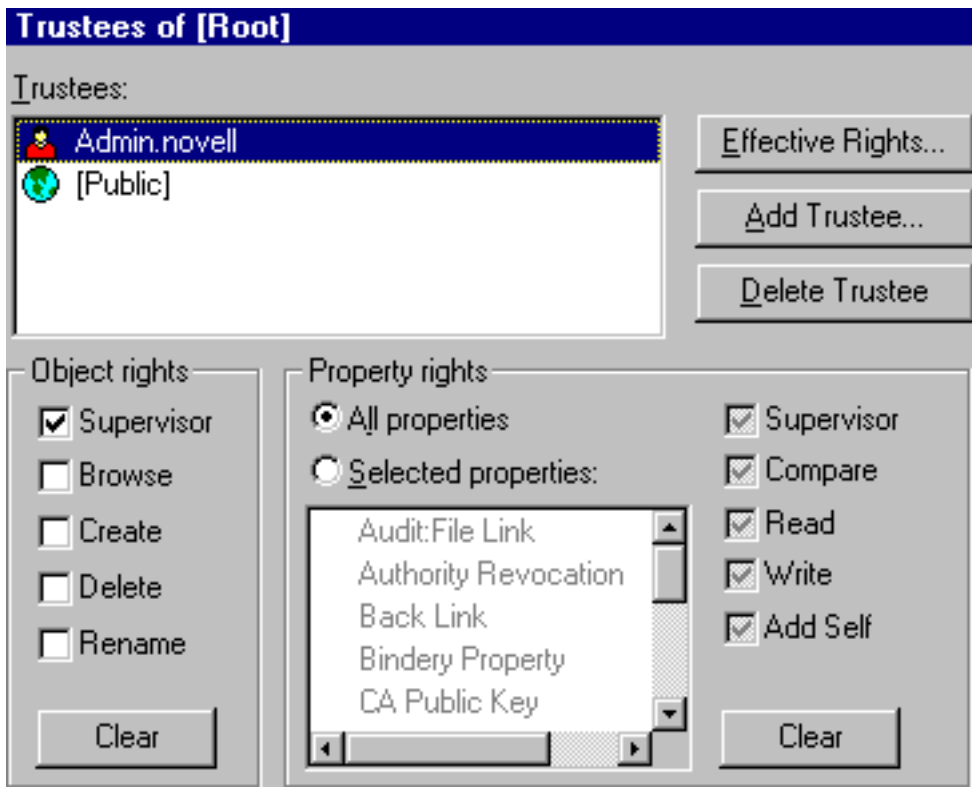
Public Trustee

The [Public] trustee is not an object. It is a specialized trustee that represents any network user, logged in or not, for rights assignment purposes.

Object Rights

When you make a trustee assignment, you can grant object rights and/or property rights. Object rights apply to manipulation of the entire object, while property rights only apply to certain object properties.

Object rights are shown in the left-hand side of the NWAdmin Trustees dialog. A description of each right follows.



Supervisor includes all rights to the object and all of its specific properties.

Browse enables the trustee to see the object in the tree. It does not include the right to see an object's specific properties.

Create only applies when the target object is a container. The target in the example above is [Root], shown in the window's title bar. Create allows the trustee to create new objects below the container, and also includes the Browse right.

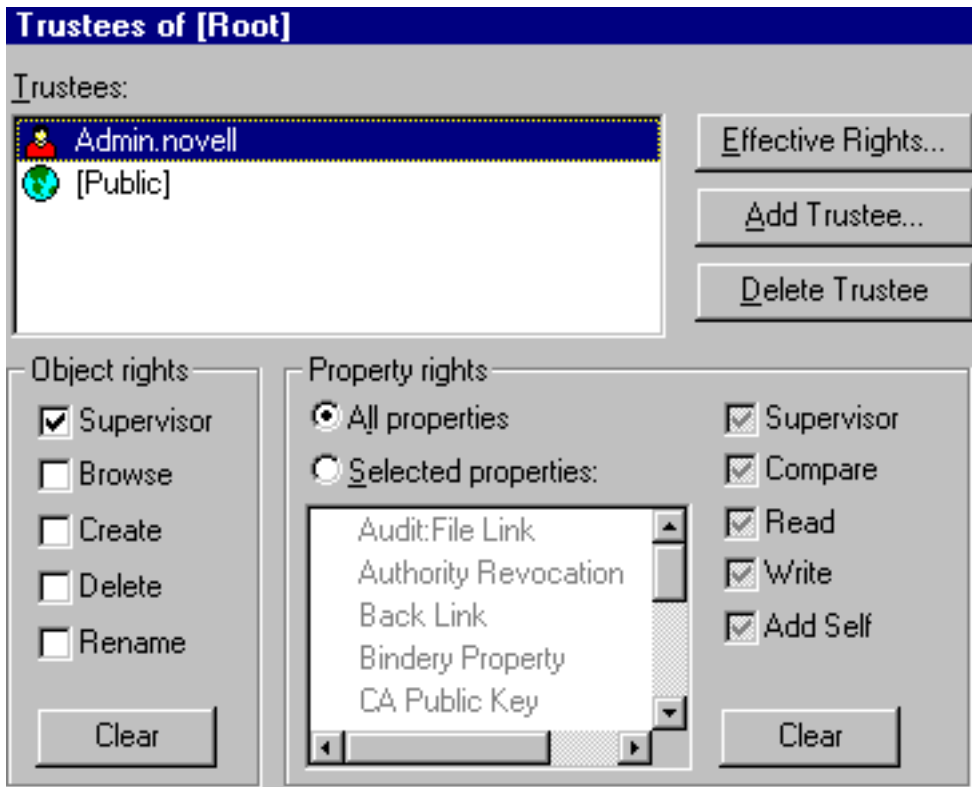
Delete allows the trustee to delete the target from the Directory.

Rename allows the trustee to change the name of the target.

Property Rights

When you make a trustee assignment, you can grant object rights and/or property rights. Object rights apply to manipulation of the entire object, while property rights only apply to certain object properties.

Property rights are shown in the lower right pane of the NWAdmin Trustees dialog below.



NWAdmin gives you two options for managing property rights:

- ♦ You can manage all properties at once when the All Properties radio button is selected.
- ♦ You can manage one or more individual properties when the Selected Properties radio button is selected.

Following is a description of each property right.

Supervisor allows the trustee complete power over the property.

Compare enables the trustee to compare the value of a property to a given value. This right allows searching, and only returns a true or false result. It does not allow the trustee to actually see the value of the property.

Read allows the trustee to see the values of a property. It includes the Compare right.

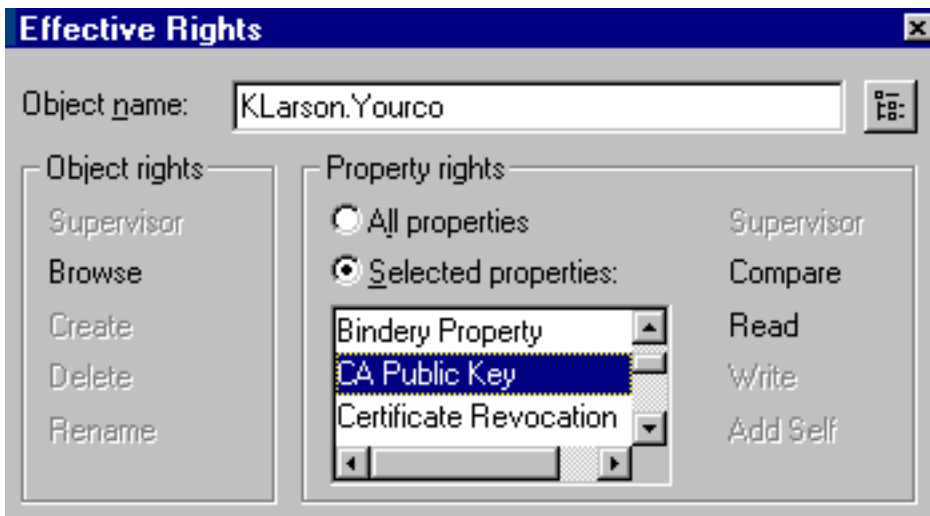
Write allows the trustee to create, change, and delete the values of a property.

Add Self allows the trustee to add or remove itself as a property value. It only applies to properties with object names as values, such as membership lists or Access Control Lists (ACLs).

Effective Rights

Users can receive rights in a number of ways, such as explicit trustee assignments, inheritance, and security equivalence. Rights can also be limited by IRFs and changed or revoked by subsequent trustee assignments. The net result of all these actions--the rights a user can employ--are called effective rights.

A user's effective rights to an NDS object are calculated each time the user attempts an action. NWAdmin checks the effective rights of any object and displays them for you, as shown below.



The effective rights displayed for User KLarson are

- ♦ Browse object right
- ♦ Compare and Read right to the CA Public Key property. (To view rights to other properties, select the property from the Selected Properties list.)

Security Equivalence

Security equivalence means having the same trustee assignments as another object. When you make one object security equivalent to another object, the rights of the second object are added to the rights of the first object.

For instance, suppose you make User object Joe security equivalent to the Admin object. After you create the security equivalence, Joe has the same rights to the NDS tree as Admin.

NOTE: Security equivalence is only effective for one step. For instance, if you make a third user security equivalent to Joe in the example above, that user will not receive Admin rights.

Security equivalence is recorded in NDS as values in the User object's Security Equal To property.

When you add a User object as an occupant to an Organizational Role object, that User automatically becomes security equivalent to the Organizational Role object. The same is true when a User becomes a member of a Group object.

Access Control List (ACL)

The Access Control List (ACL) is also called the Object Trustees property. Whenever you make a trustee assignment, the trustee is added as a value to the Object Trustees (ACL) property of the target.

This property has strong implications for network security for the following reasons:

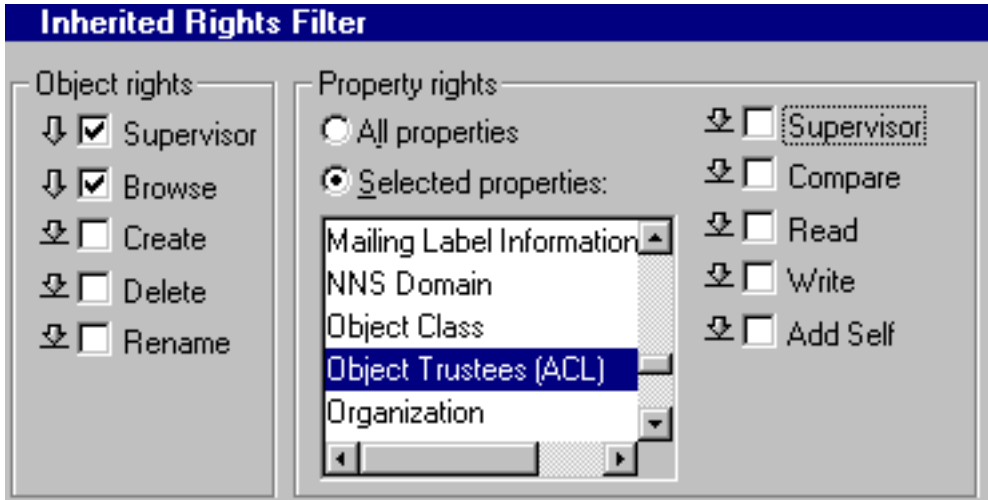
- ♦ Anyone who has the Supervisor or Write right to the Object Trustees (ACL) property of an object can determine who is a trustee of that object.
- ♦ Any users with the Add Self right to the Object Trustees (ACL) property of an object can change their own rights to that object. For example, they can grant themselves the Supervisor right.

For these reasons, you should be careful giving Add Self rights to all properties of a container object. That assignment makes it possible for the trustee to become Supervisor of that container, all objects in it, and all objects in containers beneath it.

Inherited Rights Filter (IRF)

An Inherited Rights Filter (IRF) limits the inheritance of rights. When you create an IRF, you specify the rights which can be inherited from the parent object.

The NWAdmin screen you use to create an IRF is shown below.



Notice the check marks under Object rights next to Supervisor and Browse. These indicate that objects inherit the Supervisor and Browse rights assigned to container targets higher in the tree (but no other rights).

Notice also that under Property rights, no rights are selected to the Object Trustees (ACL) property. This indicates that no assignments to that property will be inherited from containers higher in the tree.

NWAdmin will not allow you to filter the Supervisor object right without granting that right explicitly. Such an IRF would cut off all management of the target object and all objects lower in the tree.

Default Rights for a New NetWare Server

When you install a new NetWare Server object into an NDS tree, the following NDS trustee assignments are made:

<i>Default Trustees</i>	<i>Default Rights</i>
Admin (first NDS server in the tree)	Supervisor object right to [Root]
[Public] (first NDS server in the tree)	Browse object right to [Root]
NetWare Server	Admin has the Supervisor object right to the NetWare Server object, which means that Admin also has the Supervisor right to the root directory of the file system of any NetWare volumes on the server.
Volumes (if created)	[Root] has the Read property right to the Host Server Name and Host Resource properties on all Volume objects. This gives all objects access to the physical volume name and physical server name. Admin has the Supervisor right to the root directory of the file systems on the volume. For volume SYS, the container object has Read and File Scan rights to the volume's \PUBLIC directory. This allows User objects under the container to access NetWare utilities in \PUBLIC.
User	If home directories are automatically created for users, they have the Supervisor right to those directories.

Delegated Administration

NDS allows you to delegate administration of a branch of the NDS tree, revoking your own management rights to that branch. One reason for this approach might be that special security requirements require a different administrator with complete control over that branch.

Delegated administration is accomplished by

1. Granting the Supervisor object right to a container.
2. Creating an IRF at that container which filters the Supervisor and any other rights you want blocked.

WARNING: If you delegate administration to a User object and that object is subsequently deleted, there will be no objects with NDS rights to manage that branch.

4

Terms

This section contains a list of terms you will find helpful when using NDS.

NDS Server

A server with NDS installed. NDS servers can hold replicas of the NDS database and synchronize those replicas with other NDS servers. NDS servers are represented in the NDS tree by NetWare Server objects.

Replica Synchronization

Replica synchronization ensures that changes to Directory objects are synchronized among all replicas of the partition.

This means that any server that holds a replica of a partition must communicate with the other servers to synchronize a change.

Two types of replica synchronization can occur:

- ♦ Immediate sync occurs after any change to a Directory object, or any addition or deletion of an object in the NDS tree. By default, the immediate sync process runs ten seconds after any change is saved. Immediate sync also applies to changes in Network Address and Revision attributes to the User object.
- ♦ Slow sync occurs for specific changes to a Directory object that are repetitive and common to multiple objects such as changes to login properties. An example of this would be a password change or an update to Login Time and Last Login Time attributes when a user logs in or out.

The slow sync process runs only in the absence of an immediate sync process, by default 30 minutes after particular changes are made.

Schema Synchronization

Schema synchronization ensures that the schema is consistent across the partitions in the NDS tree and that all schema changes are updated across the network.

This process runs once every four hours by default.

Limber

Limber ensures that the replica pointer table is updated when a server name or address is changed. Such changes occur when

- ♦ The server is rebooted with a new server name or IPX™ internal address.
- ♦ An address is added for an additional protocol.
- ♦ Any time the database is opened, such as after running DSREPAIR or unloading and loading NDS.
- ♦ When communication is established with an additional server in the tree.

When a server is booted, the limber process compares the server's name and IPX address with those stored in the replica pointer table. If either are different, NDS™ automatically updates all replica pointer tables that contain a listing of that server.

The limber process also checks that the tree name is correct for each server in a replica ring.

Limber runs by default five minutes after the server boots up and then every three hours.

Backlink

Backlink verifies external references, which are pointers to Directory objects that are not stored in the replicas on a server.

The backlink process runs two hours after the local database is opened and then every thirteen hours.

Connection Management

Servers in a replica ring require a highly secure connection for transferring NetWare[®] Core Protocol[™] (NCP[™]) packets. These secure connections, called virtual client connections, are established by the connection management process.

If a server-to-server connection is lost, the connection management process establishes the connection again when needed.

The connection management process may also need to establish a virtual client connection for schema synchronization or backlink processes. Time synchronization might also require such a connection, depending on the configuration of time services.



Novell Trademarks

Access Manager is a registered trademark of Novell, Inc. in the United States and other countries.

Advanced NetWare is a trademark of Novell, Inc.

AlarmPro is a registered trademark of Novell, Inc. in the United States and other countries.

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppTester is a registered service mark of Novell, Inc. in the United States and other countries.

BrainShare is a registered service mark of Novell, Inc. in the United States and other countries.

C-Worthy is a trademark of Novell, Inc.

C3PO is a trademark of Novell, Inc.

CBASIC is a registered trademark of Novell, Inc. in the United States and other countries.

Certified NetWare Administrator in Japanese and CNA-J are service marks of Novell, Inc.

Certified NetWare Engineer in Japanese and CNE-J are service marks of Novell, Inc.

Certified NetWare Instructor in Japanese and CNI-J are service marks of Novell, Inc.

Certified Novell Administrator and CNA are service marks of Novell, Inc.

Certified Novell Engineer is a trademark and CNE is a registered service mark of Novell, Inc. in the United States and other countries.

Certified Novell Salesperson is a trademark of Novell, Inc.

Client 32 is a trademark of Novell, Inc.

ConnectView is a registered trademark of Novell, Inc. in the United States and other countries.

Connectware is a registered trademark of Novell, Inc. in the United States and other countries.

Corsair is a registered trademark of Novell, Inc. in the United States and other countries.

CP/Net is a registered trademark of Novell, Inc. in the United States and other countries.

Custom 3rd-Party Object and C3PO are trademarks of Novell, Inc.

DeveloperNet is a registered trademark of Novell, Inc. in the United States and other countries.

Documenter's Workbench is a registered trademark of Novell, Inc. in the United States and other countries.

ElectroText is a trademark of Novell, Inc.

Enterprise Certified Novell Engineer and ECNE are service marks of Novell, Inc.

Envoy is a registered trademark of Novell, Inc. in the United States and other countries.

EtherPort is a registered trademark of Novell, Inc. in the United States and other countries.

EXOS is a trademark of Novell, Inc.

Global MHS is a trademark of Novell, Inc.

Global Network Operations Center and GNOC are service marks of Novell, Inc.

Graphics Environment Manager and GEM are registered trademarks of Novell, Inc. in the United States and other countries.

GroupWise is a registered trademark of Novell, Inc. in the United States and other countries.

GroupWise XTD is a trademark of Novell, Inc.

Hardware Specific Module is a trademark of Novell, Inc.

Hot Fix is a trademark of Novell, Inc.

InForms is a trademark of Novell, Inc.

Instructional Workbench is a registered trademark of Novell, Inc. in the United States and other countries.

Internetwork Packet Exchange and IPX are trademarks of Novell, Inc.

IPX/SPX is a trademark of Novell, Inc.

IPXODI is a trademark of Novell, Inc.

IPXWAN is a trademark of Novell, Inc.

LAN WorkGroup is a trademark of Novell, Inc.

LAN WorkPlace is a registered trademark of Novell, Inc. in the United States and other countries.

LAN WorkShop is a trademark of Novell, Inc.

LANalyzer is a registered trademark of Novell, Inc. in the United States and other countries.

LANalyzer Agent is a trademark of Novell, Inc.

Link Support Layer and LSL are trademarks of Novell, Inc.

MacIPX is a registered trademark of Novell, Inc. in the United States and other countries.

ManageWise is a registered trademark of Novell, Inc. in the United States and other countries.

Media Support Module and MSM are trademarks of Novell, Inc.

Mirrored Server Link and MSL are trademarks of Novell, Inc.

Mobile IPX is a trademark of Novell, Inc.

Multiple Link Interface and MLI are trademarks of Novell, Inc.

Multiple Link Interface Driver and MLID are trademarks of Novell, Inc.

My World is a registered trademark of Novell, Inc. in the United States and other countries.

N-Design is a registered trademark of Novell, Inc. in the United States and other countries.

Natural Language Interface for Help is a trademark of Novell, Inc.

NDS Manager is a trademark of Novell, Inc.

NE/2 is a trademark of Novell, Inc.

NE/2-32 is a trademark of Novell, Inc.

NE/2T is a trademark of Novell, Inc.

NE1000 is a trademark of Novell, Inc.

NE1500T is a trademark of Novell, Inc.

NE2000 is a trademark of Novell, Inc.

NE2000T is a trademark of Novell, Inc.

NE2100 is a trademark of Novell, Inc.

NE3200 is a trademark of Novell, Inc.

NE32HUB is a trademark of Novell, Inc.

NEST Autoroute is a trademark of Novell, Inc.

NetExplorer is a trademark of Novell, Inc.

NetNotes is a registered trademark of Novell, Inc. in the United States and other countries.

NetSync is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare 3270 CUT Workstation is a trademark of Novell, Inc.

NetWare 3270 LAN Workstation is a trademark of Novell, Inc.

NetWare 386 is a trademark of Novell, Inc.

NetWare Access Server is a trademark of Novell, Inc.

NetWare Access Services is a trademark of Novell, Inc.

NetWare Application Manager is a trademark of Novell, Inc.

NetWare Application Notes is a trademark of Novell, Inc.

NetWare Asynchronous Communication Services and NACS are trademarks of Novell, Inc.

NetWare Asynchronous Services Interface and NASI are trademarks of Novell, Inc.

NetWare Aware is a trademark of Novell, Inc.

NetWare Basic MHS is a trademark of Novell, Inc.

NetWare BranchLink Router is a trademark of Novell, Inc.

NetWare Care is a trademark of Novell, Inc.

NetWare Communication Services Manager is a trademark of Novell, Inc.

NetWare Connect is a registered trademark of Novell, Inc. in the United States.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare Distributed Management Services is a trademark of Novell, Inc.

NetWare Document Management Services is a trademark of Novell, Inc.

NetWare DOS Requester and NDR are trademarks of Novell, Inc.

NetWare Enterprise Router is a trademark of Novell, Inc.

NetWare Express is a registered service mark of Novell, Inc. in the United States and other countries.

NetWare Global Messaging and NGM are trademarks of Novell, Inc.

NetWare Global MHS is a trademark of Novell, Inc.

NetWare HostPrint is a registered trademark of Novell, Inc. in the United States.

NetWare IPX Router is a trademark of Novell, Inc.

NetWare LANalyzer Agent is a trademark of Novell, Inc.

NetWare Link Services Protocol and NLSP are trademarks of Novell, Inc.

NetWare Link/ATM is a trademark of Novell, Inc.

NetWare Link/Frame Relay is a trademark of Novell, Inc.

NetWare Link/PPP is a trademark of Novell, Inc.
NetWare Link/X.25 is a trademark of Novell, Inc.
NetWare Loadable Module and NLM are trademarks of Novell, Inc.
NetWare LU6.2 is trademark of Novell, Inc.
NetWare Management Agent is a trademark of Novell, Inc.
NetWare Management System and NMS are trademarks of Novell, Inc.
NetWare Message Handling Service and NetWare MHS are trademarks of Novell, Inc.
NetWare MHS Mailslots is a registered trademark of Novell, Inc. in the United States and other countries.
NetWare Mirrored Server Link and NMSL are trademarks of Novell, Inc.
NetWare Mobile is a trademark of Novell, Inc.
NetWare Mobile IPX is a trademark of Novell, Inc.
NetWare MultiProtocol Router and NetWare MPR are trademarks of Novell, Inc.
NetWare MultiProtocol Router Plus is a trademark of Novell, Inc.
NetWare Name Service is trademark of Novell, Inc.
NetWare Navigator is a trademark of Novell, Inc.
NetWare Peripheral Architecture is a trademark of Novell, Inc.
NetWare Print Server is a trademark of Novell, Inc.
NetWare Ready is a trademark of Novell, Inc.
NetWare Requester is a trademark of Novell, Inc.
NetWare Runtime is a trademark of Novell, Inc.
NetWare RX-Net is a trademark of Novell, Inc.
NetWare SFT is a trademark of Novell, Inc.
NetWare SFT III is a trademark of Novell, Inc.
NetWare SNA Gateway is a trademark of Novell, Inc.
NetWare SNA Links is a trademark of Novell, Inc.
NetWare SQL is a trademark of Novell, Inc.
NetWare Storage Management Services and NetWare SMS are trademarks of Novell, Inc.
NetWare Telephony Services is a trademark of Novell, Inc.
NetWare Tools is a trademark of Novell, Inc.
NetWare UAM is a trademark of Novell, Inc.
NetWare WAN Links is a trademark of Novell, Inc.
NetWare/IP is a trademark of Novell, Inc.

NetWire is a registered service mark of Novell, Inc. in the United States and other countries.

Network Navigator is a registered trademark of Novell, Inc. in the United States.

Network Navigator - AutoPilot is a registered trademark of Novell, Inc. in the United States and other countries.

Network Navigator - Dispatcher is a registered trademark of Novell, Inc. in the United States and other countries.

Network Support Encyclopedia and NSE are trademarks of Novell, Inc.

Network Support Encyclopedia Professional Volume and NSEPro are trademarks of Novell, Inc.

NetWorld is a registered service mark of Novell, Inc. in the United States and other countries.

Novell is a service mark and a registered trademark of Novell, Inc. in the United States and other countries.

Novell Alliance Partners Program is a collective mark of Novell, Inc.

Novell Application Launcher is a trademark of Novell, Inc.

Novell Authorized CNE is a trademark and service mark of Novell, Inc.

Novell Authorized Education Center and NAEC are service marks of Novell, Inc.

Novell Authorized Partner is a service mark of Novell, Inc.

Novell Authorized Reseller is a service mark of Novell, Inc.

Novell Authorized Service Center and NASC are service marks of Novell, Inc.

Novell BorderManager is a trademark of Novell, Inc.

Novell BorderManager FastCache is a trademark of Novell, Inc.

Novell Client is a trademark of Novell, Inc.

Novell Corporate Symbol is a trademark of Novell, Inc.

Novell Customer Connections is a registered trademark of Novell, Inc. in the United States.

Novell Directory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries.

Novell Distributed Print Services is a trademark and NDPS is a registered trademark of Novell, Inc. in the United States and other countries.

Novell ElectroText is a trademark of Novell, Inc.

Novell Embedded Systems Technology is a registered trademark and NEST is a trademark of Novell, Inc. in the United States and other countries.

Novell Gold Authorized Reseller is a service mark of Novell, Inc.

Novell Gold Partner is a service mark of Novell, Inc.

Novell Labs is a trademark of Novell, Inc.

Novell N-Design is a registered trademark of Novell, Inc. in the United States and other countries.

Novell NE/2 is a trademark of Novell, Inc.

Novell NE/2-32 is a trademark of Novell, Inc.

Novell NE3200 is a trademark of Novell, Inc.

Novell Network Registry is a service mark of Novell, Inc.

Novell Platinum Partner is a service mark of Novell, Inc.

Novell Press is a trademark of Novell, Inc.

Novell Press Logo (teeth logo) is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Replication Services is a trademark of Novell, Inc.

Novell Research Reports is a trademark of Novell, Inc.

Novell RX-Net/2 is a trademark of Novell, Inc.

Novell Service Partner is a trademark of Novell, Inc.

Novell Storage Services is a trademark of Novell, Inc.

Novell Support Connection is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Technical Services and NTS are service marks of Novell, Inc.

Novell Technology Institute and NTI are registered service marks of Novell, Inc. in the United States and other countries.

Novell Virtual Terminal and NVT are trademarks of Novell, Inc.

Novell Web Server is a trademark of Novell, Inc.

Novell World Wide is a trademark of Novell, Inc.

NSE Online is a service mark of Novell, Inc.

NTR2000 is a trademark of Novell, Inc.

Nutcracker is a registered trademark of Novell, Inc. in the United States and other countries.

OnLAN/LAP is a registered trademark of Novell, Inc. in the United States and other countries.

OnLAN/PC is a registered trademark of Novell, Inc. in the United States and other countries.

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

Open Look is a registered trademark of Novell, Inc. in the United States and other countries.

Open Networking Platform is a registered trademark of Novell, Inc. in the United States and other countries.

Open Socket is a registered trademark of Novell, Inc. in the United States.

Packet Burst is a trademark of Novell, Inc.

PartnerNet is a registered service mark of Novell, Inc. in the United States and other countries.

PC Navigator is a trademark of Novell, Inc.

PCOX is a registered trademark of Novell, Inc. in the United States and other countries.

Perform3 is a trademark of Novell, Inc.

Personal NetWare is a trademark of Novell, Inc.

Pervasive Computing from Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Portable NetWare is a trademark of Novell, Inc.

Presentation Master is a registered trademark of Novell, Inc. in the United States and other countries.

Print Managing Agent is a trademark of Novell, Inc.

Printer Agent is a trademark of Novell, Inc.

QuickFinder is a trademark of Novell, Inc.

Red Box is a trademark of Novell, Inc.

Reference Software is a registered trademark of Novell, Inc. in the United States and other countries.

Remote Console is a trademark of Novell, Inc.

Remote MHS is a trademark of Novell, Inc.

RX-Net is a trademark of Novell, Inc.

RX-Net/2 is a trademark of Novell, Inc.

ScanXpress is a registered trademark of Novell, Inc. in the United States and other countries.

Script Director is a registered trademark of Novell, Inc. in the United States and other countries.

Sequenced Packet Exchange and SPX are trademarks of Novell, Inc.

Service Response System is a trademark of Novell, Inc.

Serving FTP is a trademark of Novell, Inc.

SFT is a trademark of Novell, Inc.

SFT III is a trademark of Novell, Inc.

SoftSolutions is a registered trademark of SoftSolutions Technology Corporation, a wholly owned subsidiary of Novell, Inc.

Software Transformation, Inc. is a registered trademark of Software Transformation, Inc., a wholly owned subsidiary of Novell, Inc.

SPX/IPX is a trademark of Novell, Inc.

StarLink is a registered trademark of Novell, Inc. in the United States and other countries.

Storage Management Services and SMS are trademarks of Novell, Inc.

Technical Support Alliance and TSA are collective marks of Novell, Inc.

The Fastest Way to Find the Right Word is a registered trademark of Novell, Inc. in the United States and other countries.

The Novell Network Symbol is a trademark of Novell, Inc.

Topology Specific Module and TSM are trademarks of Novell, Inc.

Transaction Tracking System and TTS are trademarks of Novell, Inc.

Universal Component System is a registered trademark of Novell, Inc. in the United States and other countries.

Virtual Loadable Module and VLM are trademarks of Novell, Inc.

Writer's Workbench is a registered trademark of Novell, Inc. in the United States and other countries.

Yes, It Runs with NetWare (logo) is a trademark of Novell, Inc.

Yes, NetWare Tested and Approved (logo) is a trademark of Novell, Inc.

ZENworks is a trademark of Novell, Inc.

