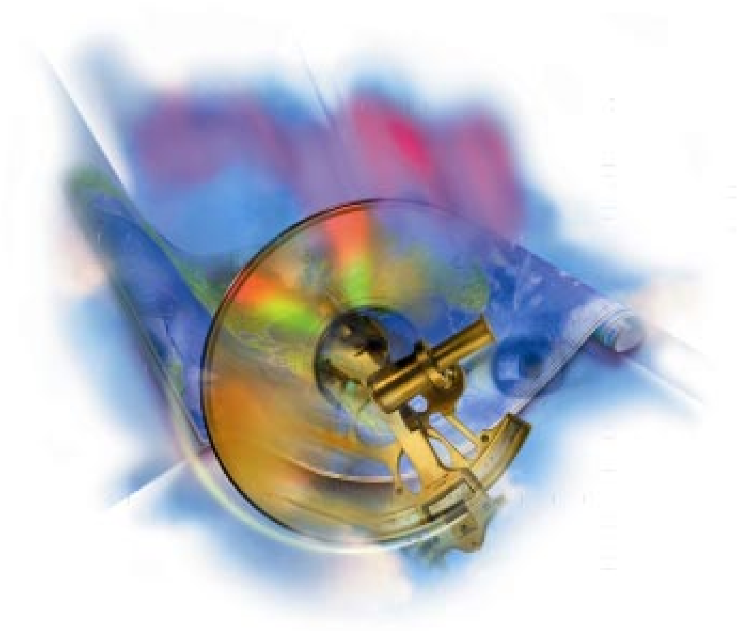
NOVELL PARTNER CONSULTING SERVICE OFFERINGS

NOVELL PARTNERNET CONFIDENTIAL

NDS Design

CONSULTANT GUIDE



Novell®

Table of Contents

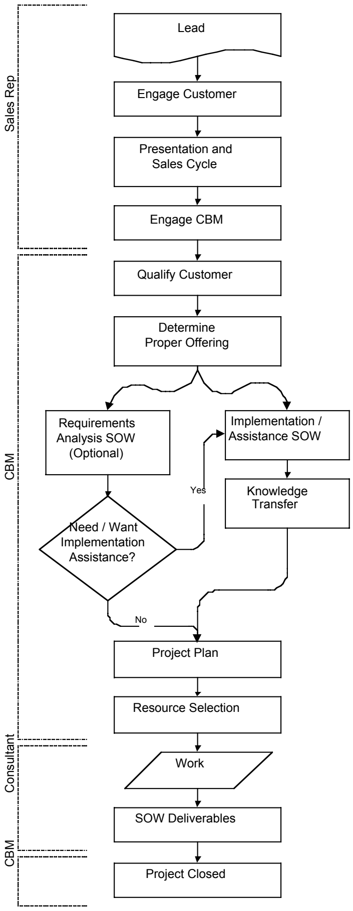
Overview of Engagement Methodology for NDS Design ... 4
Introduction ... 4
Purpose ... 5
Assumptions ... 5
Preflight Checklist ... 5
NDS Design Training Curriculum ... 5
Required Skills for NDS Design ... 5
Novell Courses or Equivalent Project Experience ... 5
Novell CNE NetWare 5 ... 5
Additional Novell Courses (Optional) ... 7
Non-Novell Skills/Courses ... 7
Resources to Be Developed ... 7
Reference Material ... 7
NDS Design Training Content ... 8
Recommended Skills ... 8
Novell Courses or Equivalent Project Experience ... 8
Reference Material ... 9
AppNotes ... 9
Preparing for the Initial Engagement Meeting ... 10
Pre-engagement Discussion with Client ... 10
Start of Engagement ... 10
Task 1—Conduct Initial Engagement Meeting ... 10
Items to Cover ... 11
Task 2—Prepare Preliminary Report ... 11
Task 3—Deliver Preliminary Report to Customer ... 11
Process 3—Develop Solution Design ... 12
Task 1—Design Top Level of NDS Tree ... 12
Task 2—Design Bottom Level of NDS Tree ... 14
NDS eDirectory Design Guidelines ... 16
NDS eDirectory Considerations ... 18
Task 3—Establish Naming Standards ... 20
Task 4—Design and Discuss NDS Security ... 25
NDS Security Overview ... 25
NDS Administration ... 33
Task 5—Develop Partition Design ... 36
Task 6—Develop Partition Replication Design ... 40
Task 7—Develop Network Time Management Design (Time Synchronization) ... 43
Task 8—Test and Verify ... 53
Task 9—Develop and Deliver NDS Design Report ... 54
Sample Project Plan ... 55
Closing the Engagement ... 56
Task 1—Closing Tasks ... 56
Task 2—Prepare Final Report ... 56
Task 3—Deliver Final Report to Customer ... 56
Sample Project Deliverable ... 57
Executive Summary ... 62
Introduction ... 62
Background ... 62
Assessment ... 62
Recommendations ... 62
Value ... 63
Overview ... 64
Who Should Read This Report ... 64
Acknowledgements ... 64
Follow-Up ... 64
What You Need to Know ... 64
How to Use the Information in This Report ... 64
Introduction ... 65
Statement of Work ... 65
Novell Directory Services Design ... 66
NDS Design Guidelines ... 66

The Four Principles of NDS Design ... 66
Understand the Use of NDS Objects ... 67
NDS Design Tasks ... 67
XYZ Corporation: Top of the Tree Design ... 68
XYZ Corporation: Bottom of the Tree Design ... 70
Apply Special Design Factors ... 70
Partition Design ... 71
Quick Design ... 71
Partition Diagram ... 72
Replica Placement ... 73
Partition and Replica Matrix ... 73
Network Time Management Design (Time Synchronization) ... 75
Types of Servers ... 75
Time Configuration ... 75
Time Communication ... 75
XYZ Corporation Time Synchronization Design ... 75
Naming Standards ... 78
Basic NDS Security Policy ... 82
Physical Security ... 82
Login Security ... 82
NDS Security ... 84
Summary ... 86
Transition Notes ... 87
Direction ... 87
Timeline ... 87
Appendix A: ... 88

Overview of Engagement Methodology for NDS Design

This overview of the engagement methodology provides information and guidance about how to conduct a consulting engagement. This overview is an organized collection of technical best practices (TBP) combined with sound consulting business practices that together ensure a successful engagement, increase customer satisfaction, minimize risk, and promote consistency in the designs and recommendations from Novell.

The figure below illustrates the process flow for the NDS Design engagement. Please note, a "CBM" refers to a defined Consulting Business Manager and a "CPL" refers to a defined Consulting Project Lead, if applicable.


Sales Rep
CBM
Consultant
CBM
Lead
Engage Customer
Presentation and Sales Cycle
Engage CBM
Qualify Customer
Determine Proper Offering
Requirements Analysis SOW (Optional)
Implementation / Assistance SOW
Knowledge Transfer
Need / Want Implementation Assistance?
Yes
No
Project Plan
Resource Selection
Work
SOW Deliverables
Project Closed

The process is subdivided into subprocesses. Each subprocess is divided into tasks, which are in turn divided into activities and further divided into steps.

For each consulting engagement, all elements of the process are identified and completed. Depending upon the practice and engagement type, a specific subprocess or its associated tasks may not be required. In such a case, these sections will not be included in the engagement documentation.

Introduction

Purpose

Using the information and the steps outlined in this document will help the Consultant in the performance of the following tasks:

- Gather the appropriate preflight information prior to starting the design project.

  Note: This methodology is not designed to "do all," "train all," or "teach all," nor does it replace any Novell product documentation. References may be made to other documents to help understand certain concepts or to help implement certain steps. This methodology is a living document that will be refined as new knowledge and experience is obtained and as underlying technology changes.

- Write NDS design status reports to tell the customer of the project's progress and status.

Assumptions

This document assumes that the customer's system consists solely of non-NDS components. Therefore, an NDS design is necessary.

Preflight Checklist

This document assumes that you have (or will have) the customer's completed preflight checklist (PFC) and that any deficiencies will be updated prior to the engagement.

NDS Design Training Curriculum

Required Skills for NDS Design

Consultant must have a thorough understanding of NetWare 4 and NetWare 5.

Upon successful completion of prerequisites and NDS Design training, the consultant can perform engagements that include the following:

- NDS Design and Implementation
- NDS Design Review

Novell Courses or Equivalent Project Experience

The following Novell Education courses will provide the fundamental knowledge of [NDS] required for the [NDS Design] Methodology. For more details please visit -http://www.novell.com/education

Novell CNE NetWare 5

Novell Course 529: NetWare 4.11 to NetWare 5 Update (or courses 560 & 570)

- This course focuses on introducing, explaining, and comparing significant changes, updates, and new features found in NetWare 5. The course assumes the student has prior experience with NetWare 3, NetWare 4, or intraNetWare. Central goals to the course are literacy and the ability to anticipate, design, and use the new feature set of NetWare 5.

Novell Course 560: NetWare 5 Administration (or course 529)

- In this course you will learn how to accomplish fundamental network management tasks on a NetWare 5 network.

Novell Course 570: NetWare 5 Advanced Administration (or course 529)

- This course provides students with the knowledge and skills they need to design, configure, and administer a complex NetWare 5 network. Skills learned include upgrading from a NetWare 3 environment, migrating to NetWare Distributed Print Services, executing Java-based utilities, network backup and configuring NetWare 5 for remote access.

Novell Course 575: NetWare 5 Design and Implementation

- This course provides students with the knowledge and skills they need to design, configure and administer a complex NetWare 5 network, as well as manage an implementation engagement. Discussed are the project management lifecycle, the charts and diagrams used, and many other skills necessary to do an NDS rollout.

Additional Novell Courses (Optional)

Novell Course 991: Advanced NDS

- This course raises the level of NDS expertise among networking professionals so they can maintain and troubleshoot some of the most common NDS issues. Someone who takes this course should not need to call Novell Technical Support regarding an NDS issue except to report an NDS bug or to request help on issues requiring DSDUMP.

Non-Novell Skills/Courses

Organization and attention to detail, as well as a background course in project management will benefit.

Resources to Be Developed

Utilities CD with preflight checklist, utilities referenced, and spreadsheets to aid in the collection of data.

Reference Material

- Novell's publicly available support site: http://support.novell.com
- Novell's NDS Cool Solutions site: http://www.novell.com/coolsolutions/nds/

NDS Design Training Content

Recommended Skills

The customer and consultant should have a good understanding of the following:

- NetWare 4
- NetWare 5
- NDS (Schema, Synchronization, Time Synch, etc.)

Novell Courses or Equivalent Project Experience

The following Novell Education courses will provide the fundamental knowledge of [NDS] required for the [NDS Design] Methodology.

Novell Course 529: NetWare 4.11 to NetWare 5 Update (or courses 560 & 570)

- This course focuses on introducing, explaining, and comparing significant changes, updates, and new features found in NetWare 5. The course assumes the student has prior experience with NetWare 3, NetWare 4, or intraNetWare. Central goals to the course are literacy and the ability to anticipate, design, and use the new feature set of NetWare 5.

Novell Course 560: NetWare 5 Administration (or course 529)

- In this course you will learn how to accomplish fundamental network management tasks on a NetWare 5 network.
- Course information can be found at this url: http://novell.netpub.com/cgi-bin/edcatalog/ilt_one_sresult?m=142

Novell Course 570: NetWare 5 Advanced Administration (Or Course 529)

- This course provides students with the knowledge and skills they need to design, configure, and administer a complex NetWare 5 network. Skills learned include upgrading from a NetWare 3 environment, migrating to NetWare Distributed Print Services, executing Java-based utilities; network backup and configuring NetWare 5 for remote access.
- Course information can be found at this url: http://novell.netpub.com/cgi-bin/edcatalog/ilt_one_sresult?m=143

Novell Course 575: NetWare 5 Design and Implementation

- This course provides students with the knowledge and skills they need to design, configure and administer a complex NetWare 5 network, as well as manage an implementation engagement. Discussed are the project management lifecycle, the charts and diagrams used, and many other skills necessary to do an NDS rollout.
- Course information can be found at this url: http://novell.netpub.com/cgi-bin/edcatalog/ilt_one_sresult?m=144
- Additional Novell courses (optional)

Novell Course 991: Advanced NDS

- This course raises the level of NDS expertise among networking professionals so they can maintain and troubleshoot some of the most common NDS issues. Someone who takes this course should not need to call Novell Technical Support regarding an NDS issue except to report an NDS bug or to request help on issues requiring DSDUMP.
- Course information can be found at this url: http://education.novell.com/general/coursedescription.html

Reference Material

- Novell's NDS Cool Solutions site: http://www.novell.com/coolsolutions/nds/
- Novell's Support site: http://support.novell.com

AppNotes

- http://developer.novell.com/research/appnotes/1993/april/a2frame.htm
- http://developer.novell.com/research/appnotes/1993/april/a4frame.htm
- http://developer.novell.com/research/appnotes/1993/november/a2frame.htm
- http://developer.novell.com/research/devnotes/1998/april/a3frame.htm
- http://developer.novell.com/research/devnotes/1998/october/a6frame.htm
- http://developer.novell.com/research/devnotes/1999/march/a1frame.htm
- http://developer.novell.com/research/appnotes/1997/february/a2frame.htm
- http://developer.novell.com/research/appnotes/1999/january/a2frame.htm
- http://developer.novell.com/research/appnotes/1998/october/a1frame.htm
- http://developer.novell.com/research/devnotes/1998/septembe/a1frame.htm

Preparing for the Initial Engagement Meeting

Before the initial engagement meeting, you should:

- Be familiar with the NDS Design consultant guide. Have a copy of this consultant guide with you during the entire project.
- Be familiar with the NDS Design consultant guide CD, which contains tools, white papers, and similar NDS aides. Have a copy of this CD with you during the entire project.
- Define the lab requirements you will need the customer to have in their lab (see the sample in Appendix A). Bring the completed lab requirements document to the initial engagement meeting.
- Be prepared to "chalk-talk" or provide a slide show presentation on the products and/or solutions from the Work Order Agreement (WOA).
- Be aware that an initial meeting might include high-level corporate or IS management personnel. Dress appropriately.

Pre-engagement Discussion with Client

This discussion is usually conducted via telephone and email. During this discussion:

- Schedule the initial engagement meeting(s).
- Try to schedule at least a four-hour block of time in which to meet with the customer's appropriate personnel (for example, their project manager, their NDS technical person, LAN/WAN person, and so forth). You want to ensure that all customer personnel who will have a part in this engagement are present at this meeting.
- If high-level management will be participating be prepared to provide a management-level overview of the project.
- Ensure that the following information will be available at the initial engagement meeting:

  * LAN/WAN diagrams including routing and switching infrastructure and link speeds.

  * TCP/IP infrastructure (DNS, DHCP)

  * NDS design documents
- Determine if system access requirements (e.g., badges) will be necessary for Your Consultant to gain access to the lab or any other meeting or work area. Arrange for access in advance.
- Discuss required levels of access for Consultants to the production and lab NDS trees and arrange for that access for Consultants to be provided in advance of the engagement.
- Discuss required levels of access to Internet and arrange for special requirements in advance. At a minimum, this should include access to proxy servers, if necessary. Make sure an async modem line is also available.

Start of Engagement

All tasks below should be completed before moving on to the rest of the engagement.

Task 1—Conduct Initial Engagement Meeting

This is your first on-site meeting with the customer. However, this meeting may consist of several meetings with different levels of company personnel. The goal for you is to cover all items below (in however many meetings are necessary) before moving on. The following information should be covered and documented during the meeting, as it will become the customer's preliminary report:

Items to Cover

- Introduce all your Consultant team members and their roles in this engagement.
- Determine all of the customer's team members and their roles in this engagement.
- Determine what the customer expects of Your Consultant. Essentially, you are just confirming that what was scoped in the WOA is consistent with what the customer wants. If there are great inconsistencies with the WOA and the customer's expectations, discuss with the CBM after the meeting.
- Collect the following documents from the customer (the ones you requested be on-hand for this meeting):

  The completed PFC, if the customer was handling this task. If you will be handling this task, determine when you can have access to the appropriate resources to complete the PFC.

  LAN/WAN diagrams including routing and switching infrastructure and link speeds. If this information is not available, determine when you can get it.

  TCP/IP infrastructure (DNS, DHCP). If this information is not available, determine when you can get it.

  These milestones should lay out the schedule for the rest of the project.

Task 2—Prepare Preliminary Report

The preliminary report is based upon the findings in the initial engagement meeting.

Task 3—Deliver Preliminary Report to Customer

Option: Have the CBM or CPL review the report first.

Process 3—Develop Solution Design

In this process, you create a design report for the customer documenting the overall process (approach) that Your Consultant recommends for their NDS design.

The following activities need to be completed in this recommended order.

Task 1—Design Top Level of NDS Tree

NDS tree design is logically split into a top-level design and a bottom-level design. The overall tree design takes the shape of an inverted tree with the [Root] object on top. Overall tree design should represent the shape of a pyramid, smaller at the top and wider at the bottom.

The top level refers to the layers of the tree that should represent your WAN infrastructure and typically includes the organization (O=) object and the first or second levels of organizational unit (OU=) objects. The Admin user object is usually created just below the organization layer (this is automatic with NetWare 4.x). Only a few users and network resources should be placed at the top levels in the tree. The top level of the tree is the most important functionally because it serves as the foundation for the rest of the tree. Changes to the top level of the tree impact objects in the lower levels of the tree, so you want to avoid adjusting this level too often to accommodate changes or growth.

Note: These design guidelines do not account for additional technology implementations (i.e., PeopleSoft, LDAP, ZEN, Pure IP, etc.). For detailed NDS design information specific to such implementations, please refer to the appropriate methodologies for each product.

Do these steps to review the top level design:

1. Determine the name of the NDS tree. (Please refer to the standards portion of this document)

   Define the top level of the NDS tree.

   Determine whether or not a Country object should be used in this tree. (Generally, it is recommended that the Country object not be used. However, this decision may be impacted if this tree will be participating in an X.500 public data network.)

2. Determine if the network is LAN only.

   If the network is a LAN, continue with step 3; otherwise go to step 4.

3. Design the top level of the NDS tree (LAN system).

   For a LAN-only system, design the top level of the NDS tree based on agreed functional areas with O=Organization at the top.

   Note: At this point it is necessary to address the issue of future growth. Remember, no company goes into business with the intent of going out of business. The goal of business is to grow. Even if they do not think they will encounter future growth that includes opening additional locations, it is wise to plan for growth up front instead of reconfigure later. This type of planning could involve placing location containers at the top of the tree. (Even if there is only one location now.)

   Consider the customer's future expansions, divestitures, and spin-offs when creating the top-level design. Your Consultant recommends that you design the NDS tree based on the corporate WAN and organization charts (organization charts take into consideration subsidiary company holdings; i.e., a second Organization container).

   The following are factors that ensure a good NDS design:

   - A tree designed around the network infrastructure
   - A properly partitioned and replicated NDS database
   - Good NDS naming standards
   - Effective time synchronization configuration

   A good NDS tree design meets a company's business needs, reduces the cost of managing the network, and easily accommodates increased growth and other corporate changes.

   For a LAN-only system, this completes the design of the top level of the NDS tree. Go to "Design Bottom Level of the NDS Tree."

4. Review WAN diagrams.

5. Determine the locations of all servers and the connectivity types on the network.

   Note: Pay close attention to bandwidth availability on the WAN. Be certain to design the upper layers to accommodate tree walking.

6. Identify the servers that will host the replicas. Or, identify locations where servers will need to be installed to hold replicas. Then update the server information table in the preflight checklist. (This is not replica placement yet; this is just knowing where the servers are and which ones will be used.)

7. Design the top level of the tree based on locations with servers (WAN links).

8. Determine the number of organizational units at the top level.

   Are there more than ten organizational units at the top level of the tree? If "yes," continue with step 9; if "no," go to "Design Bottom Level of the NDS Tree."

9. Add a regional "placeholder" container right below the O=Organization level.

   For example: If you had 12 OUs, they could be divided into 3 regional "placeholder" OUs for proper tree design.

Task 2—Design Bottom Level of NDS Tree

The bottom level refers to all layers of the tree below the representation of the WAN layers (top level) and typically represents workgroups, departments, or some other grouping of users and resources in a company. Changes to the bottom level of the tree do not impact as many objects as changes to the top level do. Users, resources, or complete departments (OUs) can be moved with little impact to the tree.

Note: These design guidelines do not address configurations for specific product implementations. Such product implementations are DA/Scope placement for SLP, DHCP, ZENworks, etc. (For specific NDS design guidelines, as applicable, please refer to the appropriate solution methodologies.)

Follow these steps to design the bottom level of the NDS tree.

1. Define the bottom level of the NDS tree. This is defined as the distinction between the top and bottom layers of the tree.

2. Review the LAN diagrams.

3. Determine the locations and quantities of servers at each location.

4. Determine resource allocation by server (identify applications and services on each server).

5. Determine resource utilization according to user and group (identify who uses the applications and services).

6. Using the information from steps 3, 4, and 5, update the server information table in the preflight checklist.

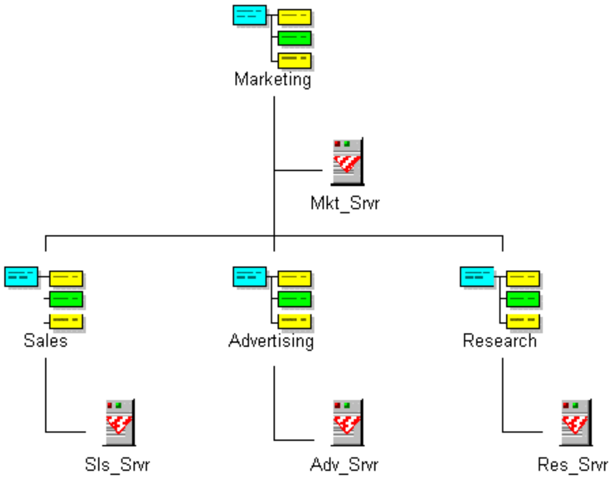
7. Identify whether the preferred network administration scheme is centralized or decentralized. (This will help guide your replica placement decisions.)

8. Design the bottom level of the NDS tree according to the agreed-upon standards.

9. Design the bottom level of the NDS tree in a manner that keeps users close to the resources they use.

10. Place resources where they are closest to the largest population of users that use the resource.

Example: The Mkt_Srvr holds common data/resources for the entire Marketing department. where the Sls_Srvr, Adv_Srvr, and Res_Srvr host information specific to each branch of the Marketing Department.



Placement of resources in this manner facilitates less complex rights assignments.

11. At this stage of the design it is extremely important to pay close attention not only to organizational structure (departments, organizations, etc.), but to how people in the organization work together (functional workgroups, etc.).

12. Avoid creating containers specifically for the purpose of holding a specific type of resource (i.e. a server container, a printer container, etc.).

13. It is important to remember to minimize the use of groups. Overuse of groups can significantly degrade performance (even with NDS ver. 8).

14. If directory master servers/replica farm servers are being used, identify a location *near* the top of the tree to hold these servers.

NDS eDirectory Design Guidelines

These guidelines are based on the total number of objects in the tree. Each column assumes that all objects will be stored on each server in the tree and is therefore based on number of objects on a single server. ***Note – NDS eDirectory was previously known as NDS 8.***

	10,000 Objects	100,000 Objects	1 Million Objects	10 Million Objects	10+ Million Objects
Data Base Size	150 MB	1.5 GB	15 GB	150 GB	150+ GB
Bandwidth for remote sites	Min 256kb Optimal T1	Min 512 KB Optimal T2	Min T1 Optimal ATM	Optimal ATM	Optimal ATM
Server RAM	Min 128 MB Opt 512 MB	Min 256 MB Opt 1 GB	Min 512 MB Opt 2 GB	Min 512 MB Opt 2 GB	Min 512 MB Opt 4 GB
NDS Cache Size	_ of Server RAM	_ of Server RAM	_ of Server RAM	_ of Server RAM	_ of Server RAM
Server Processor	Min 400 MHz	Min 400 MHz	Min 400 MHz	Min 400 MHz	Min 400 MHz
# of Processors	1	2	4	4	4
NIC Card	100 MB	100 MB	100 MB	100 MB	100 MB
# of Local Servers for Load Balancing	2	2	3	5	5
# of GEOs	50	40	15-20	10	10
Total Replicas per partition	100	80	60	50	50

Note: Performance test scripts and intstructions will be provided to enable users to perform their own benchmarks. These are PERL scripts that are being used at KeyLabs and will require UNIX clients to generate the appropriate load on the servers.

Note: These same guidelines apply to a WAN NDS design's lower layers as well.

Quick Design*

	NetWare 4.x ** (or mixed)	NetWare 5**
Partition size	Should not exceed 1000-1500 objects	Should not exceed 5000 objects
The number of child partitions per parent	Should not exceed 10-15 partitions	Should not exceed 30 partitions
Number of replicas per partition	Should not exceed 2-5 (typically 3) replicas	Should not exceed 10 replicas
Number of replicas per server	Should not exceed 7-10 replicas	Should not exceed 20 replicas
Number of replicas per dedicated "Replica Server"	Should not exceed 30 replicas	Should not exceed 60 replicas
Recommended hardware requirements	100 MHz, 64MB RAM & 6GB SYS:	300 MHz and 128MB RAM & 13GB SYS:

* It is assumed that the maximum figures in all cases will not be used at the same time. If you max out one row, you will probably compensate by going light on another.

****Caution:** These numbers assume a correct tree design with minimal group usage.

In some extreme cases, and only where the server hardware, available bandwidth and customer business needs dictate, it may be necessary to modify the above design. The above figures can be expanded up to the limits set in the Advance Design, but should never be in more than one row.

Advanced Design*

	NetWare 4.x** (or mixed)	NetWare 5**
Partition size	Up to 3500 objects	Up to 10,000 objects
The number of child partitions per parent	Should not exceed 35 – 40 partitions	Should not exceed 75 partitions
Number of replicas per partition	Should not exceed 10 replicas	Should not exceed 20 replicas
Number of replicas per server	Should not exceed 20 replicas	Should not exceed 40 replicas
Recommended hardware requirements	200 MHz Pentium Pro and 128MB RAM, & 10GB SYS:	400 MHz, 256MB RAM & 15GB SYS:

* Never use *all* of these figures at maximum. At most, start with Quick Design, and exceed by one row from the Advanced Design Table. Balanced application is important.

****Caution:** These numbers assume a correct tree design with minimal group usage.

NDS eDirectory Considerations

NDS eDirectory Design Guidelines

NDS eDirectory is a much more scalable directory than that of its predecessors. The design guidelines outlined in this document are based on the following assumptions:

- The directory is centralized rather than the fully distributed design that is recommended for earlier versions of NDS. Customers are building larger, dedicated directory servers and distributing them to key geographic locations. For instance, a company that has 100,000 users spread across 6 geographic sites (or GEOs) would typically distribute only the local information to each site. With NDS eDirectory, this same company would build one server with all 100,000 users and replicate it to all 6 sites.
- The directory servers are dedicated directory servers. Separate servers will be deployed to support other services, such as file and print.
- Users will access the directory via LDAP and SSL.

  Once the directory grows to one million objects, access can only be via LDAP. NDAP will probably not be available. Keep in mind, the largest company is probably around 150,000 users. The companies that are talking about 1 million and larger directories are focused on Internet type business. Internet access will be strictly through LDAP. SSL is included in this assumption because it is considered an important piece of doing business on the Internet. All of the performance testing is being done through LDAP and SSL.
- The resultant directory will support 300 randomized LDAP searches per second.
- Each object in the tree is, on average, 15kb with 20 attributes.
- NDS eDirectory is platform independent. NDS eDirectory will be available on NetWare 5, NT , Solaris and Linux shortly. The majority of the guidelines stated in this document will apply cross platform. We need to work out the server processor for each of the platforms. The guidelines for NetWare 4.x and 5 are NetWare only.

For a customer wishing to implement NDS eDirectory in the old distributed model, the guidelines stated for NetWare 4.x and NetWare 5 can be followed for NDS eDirectory.

NDS Cache

- By default, NDS eDirectory uses 8 KB of RAM for cache. This setting allows NDS eDirectory to run on servers without requiring more RAM. If you have sufficient RAM to increase the NDS cache size, you can increase NDS performance considerably for large databases by allocating more RAM to the NDS cache.
- Performance of BULKLOAD is affected considerably by cache size (more is faster).
- Cache size is set using the following command at the server console:

  SET DSTRACE = !m[hexadecimal KB] or **SET DSTRACE = !mb[bytes]**

  For example, the command SET DSTRACE = !m4F00 allocates approximately 20 MB of RAM to NDS cache. Once you have set the cache size, that setting is persistent; you won't need to place a command in the AUTOEXEC.NCF file to set the cache size every time the server reboots.

  The smallest tested cache size is 0 and the largest is 2 GB. NDS runs with either amount. Determining the proper cache size depends on the memory needs of other processes running on the same server, and on the amount of disk cache required. You should test a variety of cache sizes to find a good balance. If NDS is essentially the only application, give it as much cache as possible.

  All allocated cache will eventually be used. NDS performance on highly volatile data is improved with more cache. Very low cache-to-file size ratios noticeably degrade NDS performance.

  Note: Setting the cache too high results in insufficient memory for the server to handle several large-group queries sequentially.

ConsoleOne Instead of NWADMIN

For large containers (in excess of 5,000 objects), ConsoleOne will be required to read information. NWAdmin will not be able to read containers of this size.

New Features in ConsoleOne

ConsoleOne has the following new features:

- Browse huge NDS containers. You can browse NDS containers containing millions of objects. ConsoleOne retrieves and displays the contents one page at a time.
- Search or customize views. You can search or filter the contents of the right pane based on object name and type. If the right pane contains NDS objects, you can also search based on specific property values. You can set any container at the top of the left pane.
- Configure LDAP Services. You can configure LDAP v3 services on individual NetWare servers and control how LDAP-based access to NDS works for different groups of users.
- Manage All NDS Objects. You can create, move, rename, delete, and modify any type of NDS object defined in the schema of your NDS tree. Custom property pages are available on most object types, and a generic “Other” page lists any remaining properties. You can modify multiple objects of the same type simultaneously.

Workstation Requirements for ConsoleOne

The following hardware and software are required to run this release of ConsoleOne:

- Windows 95, 98, or NT
- 64 MB RAM with an equal amount of virtual memory (swapper space).
More RAM will improve performance
- 200 MHz or faster processor
- Java 1.1.7 (included with ConsoleOne)
- NetWare 5 client software
- New versions of a new NetWare client .DLL files (included with ConsoleOne)

PKI and LDAP Support

NDS eDirectory has MP enabled SSL and LDAP support. If there is a heavy SSL requirement, then add processors to server.

Task 3—Establish Naming Standards

To develop the naming standards, there are two basic assumptions to keep in mind:

- New tree implementation (not redesign)
- May have existing NetWare 3 or 4 implementations

The result of this portion of NDS Design is the creation of an NDS naming standards document, which should be incorporated into a corporate standards document. A standards document outline is provided, and development of a complete standards methodology is in progress.

Objects and their names are the foundation of NDS. A consistent naming standard is important for design of an NDS database that is flexible, easy to use, and meets the customers' business needs.

While a comprehensive review of network standards is beyond the scope of the NDS design engagement, it is important to determine any existing standards and policies that pertain to the network. Items for review include the following:

NetWare Administrative Policies

- Centralized or decentralized
- Roles and responsibilities
- Server installation
- User ID management

Corporate Network Security Standards

- User ID requirement
- Password requirement

Naming Standards

- User ID
- Printers and print queues
- Servers
- Server volumes

A complete NDS naming standard specifies name, syntax, standard properties and value formats (telephone numbers, addresses, etc.), and examples for the objects. These fields within the tree can be useful as a "global directory," and as a single administration mechanism for all applications and platforms.

Follow these steps to review the naming standards:

1. Determine if naming standards exist.
   - If naming standards do not exist, continue with step 2.
   - If naming standards do exist, go to step 3.
2. Define naming conventions for key container and leaf objects, including users, printers, servers, volumes, print queues, and organizational units. Follow the five main guidelines in the table below.

   Update the naming standards table in the preflight checklist (PFC).
3. Review and discuss customer's current naming standards.
4. Analyze the network for naming conflicts.
5. Perform naming maintenance by resolving any conflicts.
6. Document the newly established naming standards.
7. Update the naming standards table in the preflight checklist.

Five main guidelines for creating an NDS naming standards document:

Guideline	Objective
Simplify browsing and navigation of the NDS tree	Name the objects with purpose and consistency to provide a solid foundation for NDS browsing, navigation, and resource access.
Ease of maintenance of the NDS tree	Consistent naming provides a framework for administration, monitoring, and optimization of the tree/network, including the following activities: installing file servers, creating users and printers, modifying existing objects, and moving objects.
Ease of merging separate NDS trees	A shared naming standard between the two trees will help in promoting a seamless merge.
Unique NDS object names	Identify NDS objects which require naming exclusivity, such as services which advertise via Service Advertising Protocol (SAP). Create unique user names to avoid conflict when moving or creating users.
Avoid special characters (NDS has reserved some characters for its own operations.)	Avoid using the following special characters: • Period (.) • Plus (+) • Equal (=) • Backslash (\)

NDS naming and property standards should be created for each object class, however the main focus is on the following container and leaf objects:

- [Root] tree name
- Organization
- Organizational units
- Groups
- Organizational roles
- Printers and print queues
- Servers
- Volumes
- Users

The following table is an example of an NDS object naming standard:

NDS Object	Standard and Syntax	Example(s)
Tree Name	Represents entire corporation; 64 character maximum and can contain underscores and dashes. Company name or abbreviation. XXXX_Tree.	ACME_Tree
Organization	Company or division name or abbreviation. XXXX	ACME
Organizational Unit	Location, division, or department name or abbreviation, depending upon tree layer. XXXX	PRV (geographic location) SVCS (services division) ACCT (accounting department)

File and Print Servers	Unique server name.
	LLLDDDDT##, where:
	LLL = Location
	DDDD = Department
	T = Server type (examples):
	A = application server
	C = communications server
	D = database/SQL server
	E = e-mail server
	F = file server
	M = ManageWise server
	P = print server
	R = RADIUS dial in/out server
	S = SAA server
	T = test server
	X = fax server
	## = Sequential number
		PRVACCTF01

Volumes	Create additional volumes to separate application or data from NetWare operating system SYS volume. FileServerName_VolumeName	PRVACCTF01_SYS PRVACCTF01_VOL1 PRVACCTF01_APPS
Print Objects	Names should reflect functionality, not location. Department and location information are derived from NDS context. XXXXP## XXXXQ##, where: XXXX = Printer type & model P = Printer Q = Print Queue ## = Sequential number	HP4SIP01 HP4SIQ01 HP2100P33 HP2100Q33

NDS Object	Standard and Syntax	Example(s)

Queue Server	Unique name required to broadcast using SAP.
	LLLDDDDQS##, where:
	LLL = Location
	DDDD = Department
	QS = Queue Server
	## = Sequential number
		PRVISQS19
		CHIACCTQS23

User	First character of first name, plus entire last name. In the case of similar names, a two-digit tiebreaker will be used. **Note:** You might use first init., middle init. Last name instead. It could make it a little more difficult for a hacker to guess. FLLLLLLLLLLLLLL[##], where F = First character of first name LLLLLLLLLLLLL = Last name ## = sequential number, if needed	DSMITH03 DSMITH04 CKACHADURIAN
Groups	Function, application, or specific rights assignments common to a group of users in the same physical location. XXXXXXXX	PAYROLL
Organizational Role	Administrative function being performed. XXXXXXXX	ADMINS BACKUP PASSWD

An NDS object property standard should be developed for each object defined in the NDS object naming standard document. The property standard document will promote consistency in the creation of objects in the NDS tree.

For purposes of this document, only the properties that are optional for object creation but required for this standards definition are listed. A thorough property standard would identify each property, and whether the property is required (either by NetWare or as a defined standard), optional, or system (generated upon creation of the object). The following table is an example of an NDS object property standard:

NDS Object	Property	Standard
Organization	Description	Description of the company, especially if an abbreviation is used for the organization name
Organizational Unit	Description	Description of the location, department, or functional workgroup represented by the organizational unit
Servers	Description	Description of the server, including applications or special purposes that the server is performing
Groups	Description	Description of the group, including its function (rights assignments, drive mapping via login script, etc.)
	Rights to files and directories (if applicable)	Assign S, R, W, C, E, M, F, A rights to specific volumes, directories, or files
Users	Given name	Common name for user or nickname Example: Cindi

	Last name	Users last name; first character capitalized
	Full name	Users full name; first character capitalized Example: Cynthia
	Middle initial (if applicable)	Middle initial, capitalized
	Title	Full title. Example: Vice President of Marketing
	Description	Full-time, part-time, or temporary employee
	Location	Geographic – campus or building Example: Detroit office
	Department	User's primary department or functional workgroup
	Telephone	(801) 555-1212
	Fax	(801) 555-1213
Organizational Role	Description	Description for the function the role is performing Example: Password administrators for IS container
	Occupants	Users who will occupy the role
Printer	Description	Description to include location information (floor, corner, etc.)

Task 4—Design and Discuss NDS Security

This portion of NDS Design is the creation of a basic NDS security document for a new NDS implementation, and is not intended for re-design (although the same concepts may apply). Advanced security features such as Public Key Infrastructure Services (PKIS), Novell International Cryptographic Infrastructure (NICI), and Secure Authentication Services (SAS) can be found in Chapter 13 of *Novell's Guide to NetWare 5 Networks*, by Jeffery F. Hughes and Blair W. Thomas.

The consultant should possess skills for determining NDS object and property rights, file system rights, and inheritance issues.

NDS Security Overview

Securing the network encompasses many areas of security including physical access, login, NDS, and file system restrictions.

One of the first steps toward implementing network security is the creation of a corporate network security policy. Security definitions, roles, responsibilities, and procedures must be clearly stated and communicated to anyone who will use the resources of the network. It is important to review any existing security policy that the customer has in effect for the network. Creating a network security policy is not the intended result of this methodology, however, the information contained in this document should be considered for policy.

This document focuses on managing NetWare security, divided into the following three categories:

- Physical Security
- Login Security
- NDS Security

Physical Security

The following steps for controlling physical access to servers and workstations server are recommended:

1. Protect the servers.

   Keeping the server in a safe place is critical to preventing unauthorized access.

   - Place the server in a restricted access area, such as a data center.
   - Personnel authorized to access the servers should be clearly identified. Vendor or contract employees should be accompanied by company personnel.

2. Secure the server console.

   - Use the SECURE CONSOLE utility to prevent unauthorized users from loading NLMs outside of the SYS:SYSTEM directory, and from changing the date and time on the server.
   - Prevent any unauthorized keyboard entry at the console using the console-locking feature in SCRSAVER.NLM. In order to gain access to the console prompt, the user must authenticate to NDS.
   - Encrypt Remote Console (RCONSOLE) passwords to prevent them from being read from an NCF file.
   - RCONAG6.NLM and RCONSOLEJ can be used to gain remote access to a server's console through an IP connection on a NetWare 5 server.
   - Use REMOTE.NLM and RSPX.NLM to gain remote access to a server's console through an SPX connection (NetWare 4 and NetWare 5).
   - The encrypted password command file (LDRCONAG6.NCF or LDREMOTE.NCF) can be renamed and placed into a different directory other than SYS:SYSTEM for added security.
   - See the NetWare 5 documentation—utilities reference.

3. Protect the workstations.

   The security policy should include the following information for securing workstations:

   - Users must log out of the network before leaving their work location for the day (or, at the end of a shift).
   - Users, especially those with Supervisor rights to the NDS tree, containers, or objects must not leave their workstations unattended while logged in. If a workstation must be left unattended, password-protected screen savers or workstation lock features of the desktop operating system must be used.

4. Protect the data.

   - Install an integrated, network-wide virus protection system.
   - Install auditing tools such as AUDITCON (version 4.3.5 or higher) to track events on highly sensitive servers.
   - Implement an SMS-compliant backup system for all servers.
   - Periodically restore the data to verify the integrity of the backups and restore procedure.

Login Security

Once physical security has been established, the next step in preventing unauthorized access to network resources is login security. Login security consists of two phases: login and authentication. Additional login security measures, including global and personal login restrictions, complete the login security model.

Login/Password Authentication

The login phase, also referred to as the identification phase, occurs when a user establishes his or her identity with their name (login name) and password. The authentication phase uses encryption to verify that any requests the server receives are from legitimate clients.

Recommendations

- Create a unique login name for each user; do not use Guest or other generic login names.
- Always require a password (for more information see the section: “Login Restrictions”).

Login Restrictions

The following login restrictions, also referred to as user account restrictions, are optional login security features. Novell recommends implementing these features as requirements for each user login account.

Restriction	Recommendations
Account Expiration	• Specify an expiration date for a user account if the user is a temporary or limited contract employee. • Any attempt to log in after the account expires disables the account.
Password Restrictions	• Require a password. • Require unique passwords (for a password to be unique, it must be different from the previous eight passwords used by the account). • Allow user to change password • Minimum password length (5 to 8 characters) • Force periodic password changes (every 90 days) • Establish a limit of three grace logins
Network Address Restrictions	• Restrict the network locations (workstations) from which users can log in. • Implement in high security scenarios such as banking industry, brokerage firms, military installations, etc.
Time Restrictions	• Restrict login times according to user need. • Enable this for standard weekday working hours for general users. • Broaden the time period for network administrators or for other exceptions.
Connection Restrictions (Concurrent Login Sessions)	• Limit the number of workstations (connections) from which a user can be logged in at any one time to 2.
Intruder Detection/Lockout	• Restrict the number of incorrect login attempts in a predefined time before the account is locked. • Set three (3) incorrect attempts in a 30 minute period. Remain locked for 15 minutes.

NDS Security

NDS security is composed of object security and file system security. Both file system security and object security use similar systems of trustees, rights, inheritance, IRFs, and effective rights.

Definition of Terms

- **Trustee assignment:** A direct, explicit assignment of rights granted to an object for a specific file, directory, object, or propterty.
- **Inheritance:** The method by which rights to objects and files flow down to subordinate levels of the tree.

- **Inherited rights filter (IRF):** A filter used to block inherited rights
- **Effective rights:** Actions that an object can actually perform after all security factors are calculated against the object

File System Security

File system security regulates access to the files and directories in volumes on the network, and controls how users access that information. File system security consists of assigning trustee rights, and file and directory attributes.

Trustee Rights Assignments. Default rights assignments for system-created users and groups are explained below. The network administrator can change the rights as necessary for any network user or group.

A user home directory can be created during user object creation in NDS. A user object created with NetWare Administrator or NETADMIN is granted [RWCEMFA] to the user's home directory.

The following objects receive Supervisor rights to the file system. (NDS objects and their rights are discussed in the following section.)

- User who created server object
- Any object given NDS Supervisor object rights to the server object

A user in the same container as volume SYS receives Read and File Scan rights to SYS:PUBLIC by default. All other users must be granted these rights manually for them to log in.

Rights Required for Specific Tasks

Task	Rights Required
Open and read a file	**R**ead
See a filename	**F**ile Scan
Search a directory for files	**F**ile Scan
Open and write to an existing file	**W**rite, **C**reate, **E**rase, **M**odify*
Execute an EXE file	**R**ead, **F**ile Scan
Create and write to a file	**C**reate
Copy files from a directory	**R**ead, **F**ile Scan
Copy files to a directory	**W**rite, **C**reate, **F**ile Scan
Make a new directory	**C**reate
Delete a file	**E**rase
Salvage deleted files	**R**ead and **F**ile Scan on file and **C**reate at directory
Change directory or file attributes	**M**odify
Rename a file or directory	**M**odify
Change the Inherited Rights Filter	**A**ccess Control
Change trustee assignments	**A**ccess Control
Modify a directory's disk space assignment between users	**A**ccess Control

Recommendations

- Avoid individual trustee rights assignments

  File system security is easier to implement and manage when you grant rights to objects, such as container objects, that pass their rights to multiple users. If not everyone in the container should receive the same rights, then create a group within the container, and assign rights to the group.

- Specify a standard file system structure to ease file system administration across the network

  Consider the number of volumes on each server

  Will volumes be dedicated to a specific function, such as applications, data storage, etc.?

  What are the users' data storage needs?

  What network drive letters will be standard for applications, email, user directories, etc.?

  Which directories need to be represented by aliases or directory map objects?

- Plan file system rights

  Design the overall directory structure top-down, moving from lesser to greater access.

  Avoid granting excessive rights near the top of a file system structure.

  Use inheritance and the IRF to assign rights.

  Supervisor rights in the file system cannot be blocked.

- Make trustee assignments in the following order:

  1. [Public]
  2. Containers (including [Root])
  3. Groups and Organizational Roles
  4. Users

Explicitly assigning security equivalence is not recommended. Since trustee assignments and security equivalence flow down independently, rights granted through security equivalence can remain in effect unless blocked by an IRF. This complicates the calculation of effective rights.

File and Directory Attributes. Attribute security is a subsystem of file system security. Directory and file attributes assign properties to individual directories or files, which control actions that can or cannot be taken on a file or directory. Some attributes apply at the file level only, while others apply to both the directory and the file levels.

Recommendations

- Use with caution—attribute security can override rights granted with trustee assignments, and applies to all users. This will prevent users from completing tasks.
- See the section “Traditional File Services” in the NetWare 5 online documentation for the table listing of attributes, their description, and their application to file, directory, or both.

Objects and Properties

The core of NDS security is the Access Control List (ACL)—a property of every NDS object.

There are two types of ACL rights:

- Object rights
- Property rights

Object Rights

Object rights define who can access the object (trustee) and what the trustee can do with the object (rights). These rights include Browse, Create, Delete, Rename, Supervisor, and Inheritable.

Property Rights

Property rights limit access to only specific properties of an object. These rights include Compare, Read, Add Self, Write, Supervisor, and Inheritable.

Acquisition of object and property rights can occur in three ways:

Method of Acquisition	Description	Recommendations
Trustee Assignments	Explicit access is granted to an object for any other object or its properties.	Use container, Organizational Roles for trustee assignments. Avoid individual (user) trustee assignments.
Inheritance	If the Inheritable right is assigned at the container level, object and property rights flow down and are inherited by all container and leaf objects below, unless blocked by an Inherited Rights Filter (IRF). See additional information in the Default NDS Rights section.	Use caution with the Inheritable Right Feature, especially at higher level containers such as [Root].
Security Equivalence	Objects absorb rights by association with another object.	Do not use Security Equivalence by explicitily associating an object. See additional information in Default NDS Rights – Container Creation.

Default NDS Rights

In most cases, default NDS security is adequate for object and property rights. Only those users who regularly manage NDS objects need additional rights to manage objects. Most users do not need to create and delete objects or modify property values.

NDS provides the following default rights:

- User Admin has all rights in the NDS tree and in the NetWare file system.
- The [Public] trustee has the Browse right to the root of the tree.

  This enables all objects, by security equivalence to [Public], to browse the tree.
- User objects created in a container have the following file system rights on the Sys volumes in the container:

  Read and File Scan to the Login and Public folders

  Create to the Mail folder

  Users also have these rights on the Sys volumes in all parent containers, but not on the Sys volumes in subordinate containers.
- If a home directory is automatically created during User object creation, the user has all file system rights to the home directory, no matter where it is in the tree.

Use the following guideline to determine the need for additional rights assignments:

Guidelines	Explanations
Start with the default assignments.	Defaults are in place to give users access to the resources they need without giving them access to resources or information they do not need. Make additional assignments to network or container administrators.
Avoid assigning rights through the All Properties option.	This protects private information about users and other resources on the network. Although assigning property rights through the All Properties option may seem easier, this option grants many property rights that users, and sometimes even container administrators, do not need. The main reason for not granting additional rights with the All Properties option is that rights are then granted to the Object Trustees (ACL) property. Access to the Object Trustees (ACL) property is very important for security. It is the one property that controls the granting of additional rights to an object.
Use Selected Properties to assign Property rights.	This allows you to assign more specific rights and helps you avoid security problems. The best way to set up property rights is to use the Selected Properties option.
Use caution when assigning the Write Property right to the Object Trustees (ACL) property of any object.	This lets the trustee grant anyone, including himself or herself, all rights, including the Supervisor right. This is another reason to use extreme care when making rights assignments with All Properties. Access to the Object Trustees (ACL) property, especially with the Write property right, can create a breach in NDS security. Any user with the Write property right can make anyone a supervisor of that object.
Use caution when granting the Supervisor object right to a server object.	This gives Supervisor file system rights to all volumes linked to that server. This should only be done after careful consideration because this right gives the object Supervisor file system rights to all volumes linked to that server. One way to avoid assigning the Supervisor object right is by assigning all object rights except for Supervisor and not assigning the Write property right to the Object Trustees (ACL) property. Granting the Write property right to the Object Trustees (ACL) Property of the server object will also give Supervisor file system rights to all volumes linked to that particular server. Granting the Supervisor right to a server object is the one instance in which NDS rights are inherited in the file system.
Granting the Supervisor object right implies granting the Supervisor right to all properties.	For some container administrators, you might want to grant all object rights except the Supervisor right, and then grant property rights through the Selected Properties option.

Guidelines	Explanations
Use caution when filtering Supervisor rights with an IRF.	For example, a container administrator uses an IRF to filter the network administrator's rights to a particular branch of the NDS tree. If the network administrator (who has the Supervisor right to the container administrator's user object) deletes the user object of the container administrator, that branch of the NDS tree can no longer be managed.

Security Enhancements in NetWare 5

NetWare 5 includes security enhancements that allow control of which NDS object and property rights are inherited.

In NetWare 4, subordinate objects automatically inherit the object rights and All Properties Rights that are granted to parent containers. Selected properties rights, on the other hand, are not inherited in NetWare 4.

In NetWare 5, which rights should be inherited by subordinate objects can be defined:

- Define whether object rights granted at the container level can be inherited. As a result, inheritance can be blocked without creating an Inherited Rights Filter for each object that resides in a particular container object.
- Allow specific properties to be inherited. As a result, you can grant certain users the rights to manage attributes of objects such as passwords, addresses, and telephone numbers.

To specify which rights are inherited, use the new Inheritable right, which applies only to container objects. The Inheritable right can be set for object rights, all properties rights, or selected properties rights.

If the Inheritable right is selected, the trustee assignment you make for a container object flows down to all of the objects below it. If the Inheritable right is not selected, the trustee assignment applies only to the container object. Any subordinate objects do not inherit the rights you have specified.

The Inheritable right is enabled by default for object rights and all properties rights. The Inheritable right is disabled by default for selected properties. These default settings provide compatibility with NetWare 4.

The Password Management property allows the ability for a password administrator to be established. Refer to the "Administrative Responsibilities and Roles" section, below.

NDS Administration

Methods of Administration

NDS administration can be accomplished in two ways:

Method of Administration	Description	Recommendations

Centralized Administration	One person or group of people with Supervisor rights to the entire tree.	Implement Centralized Administration for small companies or large organizations with a centralized IS department. Use Organizational Roles, not Groups or Security Equivalence, to define the administrative access.
Distributed Administration	One person or group of people with designated Supervisor or special rights to manage distributed branches (containers) of the NDS tree.	Implement Distributed Administration for large companies which do not have a central IS department. Use Organizational Roles, not Groups or Security Equivalence, to define the administrative access.

Specify Container Admin Roles

In the table below, specify which containers will have container admins, what type of admin will be used, the rights they will have to NDS objects and the file system, and who will occupy the role.

Container	Admin Type	Object Rights	File System Rights	Occupants

Administrative responsibilities can be divided into the following roles and characteristics:

Role	Characteristics
Enterprise-Wide Admin	• Object and file system rights: All rights starting at [Root] • Controlled by organizational role object in a hidden NDS tree security area
Backup Admin	Object rights: • No object rights to anything else in the container • No ability to change users of, add users to, or remove users from this role • Ability to install servers, but no rights to perform partition operations File system rights: • All file system rights to all volumes and servers within the container • Controlled by organizational role objects in containers throughout the tree
Server Admin	Object rights: • All rights within the container except Create and Rename (can modify existing objects: passwords, group memberships, and login scripts) • No ability to partition or install servers File system rights: • All rights to the following directories or volumes: PUBLIC, APPS, USERS • Controlled by organizational role objects in containers throughout the tree

Identify precautions related to specific security practices. For example, you could warn network administrators to avoid granting the Supervisor NDS right to server objects, because this right is inherited by the file system.

Create a standard for the directory structure and drive mappings. Each server's directory structure would be the same for these applications. This eases administration and helps mobile users access resources.

Role	Characteristics
Password Admin	Object rights: • Limited property rights for user objects, passwords, groups, login scripts, and so forth. • No rights to create or rename objects • No rights to partition or install servers File system rights: • None • Controlled by organizational role object in container where such management is required
Special Use Admin The Special Use Admin is a special role only for the servers not controlled by IS, such as those in a software engineering department	Object rights: • Minimal rights to NDS objects • Ability to assign group membership rights, and to change passwords and login scripts • No ability to create objects, add users to or remove users from this role, or partition and install servers File system rights: • All rights to server file systems • Controlled by organizational role objects in containers not controlled by IS

Task 5—Develop Partition Design

Partitions are logical boundaries in the NDS database. Based on Novell's current NDS specifications, partitioning works best if it is localized and does not have leaf objects on both sides of a WAN link. This is called "spanning the WAN" and it degrades performance.

You must distinguish between the following two types of containers:

- Structural
- Functional

Structural Containers. These containers are used to create the triangular design necessary for proper partitioning. These containers should be small, containing only subordinate containers. Partition boundaries are set using these structural containers, in order to divide the tree by region and to assist in following the size limits outlined later in this task.

Functional Containers. These containers are used to house the actual users and resources of the tree. These containers should be placed locally, at the site level, and will become the roots of the individual site partitions. Functional containers should follow the following rules of partitioning quite closely.

- Base partitions on the WAN infrastructure. Create functional containers to support partitioning on a site level.
- Do not create a partition that contains objects on both sides of a WAN link. Partition around the local servers in each geographic area.

Note: Refer to the previous tasks concerning top & bottom layer tree design for more information on structural and functional containers.

Spanning WAN links with a partition is a concern, not due to the NDS synchronization traffic, but rather that all the replica servers in a partition must communicate with each other. If a WAN link is slow or undependable, NDS will not synchronize until the link is back up. It is for this reason that we recommend that NDS partitions do not span WAN links.

Note: NDS requires SAP 0278 to communicate properly and authenticate over NDS. If you are using IPX, make sure this SAP type is not filtered on the routers.

The [Root] partition should remain small and typically includes the [Root] object and the O=OrganizationName container only. The partition structure below this point depends on the physical layout of the organization. If the organization has a Wide Area Network (WAN), the design of the upper partitions should reflect its physical topology. If there is no WAN, the design becomes more functional in nature directly from the [Root] partition, through to the bottom layers of the tree.

Mixed Tree—NDS eDirectory and Pre-NDS 8 Trees

- Size of partition is dependent on lowest common denominator in replica ring. If there is a server that is non-SKADS in replica ring, then the characteristics of that partition is dependent on the version of NDS on the non-SKADS server.
- Non NDS eDirectory servers need to be at a minimum of NetWare 4.11 with latest version of DS.

Local Area Network Only

Without a WAN, the LAN only network is designed functionally, with the upper partitions based directly upon resource use. Departments, divisions and workgroups become the defining factors in a single-site network. Essentially, a LAN is designed in the same fashion as the lower layers of a WAN tree. Use the following quick design guidelines.

Note: These same guidelines apply to a WAN NDS Design's lower layers as well.

Quick Design*

	NetWare 4.x ** (or mixed)	NetWare 5**	NDS eDirectory**
Partition size	Should not exceed 1000 – 1500 objects	Should not exceed 5000 objects	Should not exceed 10,000 objects
The number of child partitions per parent	Should not exceed 10 – 15 partitions	Should not exceed 30 partitions	Should not exceed 30 partitions
Number of replicas per partition	Should not exceed 2 – 5 (typically 3) replicas	Should not exceed 10 replicas	Should not exceed 10 replicas
Number of replicas per server	Should not exceed 7 – 10 replicas	Should not exceed 20 replicas	Should not exceed 40 replicas
Number of replicas per dedicated "Replica Server"	Should not exceed 30 replicas	Should not exceed 60 replicas	Should not exceed 100 replicas
Recommended hardware requirements	100 MHz, 64MB RAM & 6GB SYS:	300 MHz and 128MB RAM & 13GB SYS:	400 MHz, 256MB RAM & 28 GB SYS:

* It is assumed that the maximum figures in all cases will not be used at the same time. If you max out one row, you will probably compensate by going light on another.

****Caution:** These numbers assume a correct tree design with minimal group usage.

In some extreme cases, and only where the server hardware, available bandwidth and customer business needs dictate, it may be necessary to modify the above design. The above figures can be expanded up to the limits set in the Advanced Design, but should never be in more than one row.

Advanced Design*

	NetWare 4.x** (or mixed)	NetWare 5**	NDS eDirectory**

Partition size	Up to 3500 objects	Up to 10,000 objects	Up to 100,000 objects
The number of child partitions per parent	Should not exceed 35 – 40 partitions	Should not 75 partitions	Should not exceed 35 – 40 partitions
Number of replicas per partition	Should not exceed 10 replicas	Should not exceed 20 replicas	Should not exceed 10 replicas
Number of replicas per server	Should not exceed 20 replicas	Should not exceed 40 replicas	Should not exceed 20 replicas
Recommended hardware requirements	200 MHz Pentium Pro and 128MB RAM, & 10GB SYS:	400 MHz, 256MB RAM & 15GB SYS:	450 MHz, 512MB RAM & 55GB SYS:

* Never use *all* of these figures at maximum. At most, start with Quick Design, and exceed by one row from the Advanced Design table. Balanced application is important.

****Caution:** These numbers assume a correct tree design with minimal group usage.

Wide Area Networks

With a WAN, the LAN only network is extended to encompass more than one site, each with its own LAN, while each LAN is still designed functionally, with each site's partitions still based upon resource use. Structural partitions are added to the upper layers to reflect physical topology. Use the following guidelines to partition an NDS tree for a wide area network:

- Base partitions on the WAN infrastructure. Create functional containers to support partitioning on a site level.
- Do not create a partition that contains leaf objects on both sides of a WAN link. This is called "spanning the WAN" and it degrades performance.
- Partition around the local servers in each geographic area.

Keep the partition size small (from the Quick Design table above).

Partition the rest of the tree based on each geographic location in an organization. Split the NDS databases into partitions that contain only the information needed by a central set of users. Since tree partitions are typically based on the physical layout of the WAN, Novell recommends making each separate site location its own partition.

The quick design guidelines outlined above are still recommended in all but extreme cases.

Note: Novell recommends dividing NDS into partitions for scalability.

NDS WAN Traffic

Novell recommends carefully monitoring the number of objects in partitions which are replicated over WAN links. This is especially critical for links with low available bandwidth. These recommendations are based on the following assumptions:

- Users perform one or two logins and logouts per day
- NDS traffic should not occupy more than 5% of total available bandwidth
- The partitions are replicated to three servers (default)

	Optimum/maximum number of objects replicated across WAN links by bandwidth													
Speed	32k		64k		128k		256k		512k		T1		T3	
Objects	100	300	500	1000	800	2000	1500	3500	3000	5000	3000	5000	3000	5000

Design the Partition Structure

Follow these steps to design the partitions:

1. Design the structure of the upper layers based upon the guidelines above.

2. Partition off the [Root] of the NDS tree.

3. Create partitions based on the WAN locations identified in the top-level design.

   Caution: Do not span the WAN.

   If LAN, only go to step 4.

4. Design the structure of the lower layers based on the Quick Design tables above. Use one of these options to determine the potential number of objects per container:

   Option 1—If there are fewer objects per container than the maximum (from the table above) leave the container in the parent partition.

   Option 2—If there are more objects per container than mentioned above, create a new partition in the container.

   Note: If this does occur, you might want to revisit your bottom-layer design.

5. Update the partition table in the PFC.

Repeat these steps for each container.

Task 6—Develop Partition Replication Design

While partitions are logical boundaries in an NDS database, replicas are physical copies of partitions that you place on NetWare servers. Replicas provide:

- Fault tolerance for the NDS database
- Faster access to network resources

Use the following guidelines for replica placement:

- Always have 3 replicas for fault tolerance.

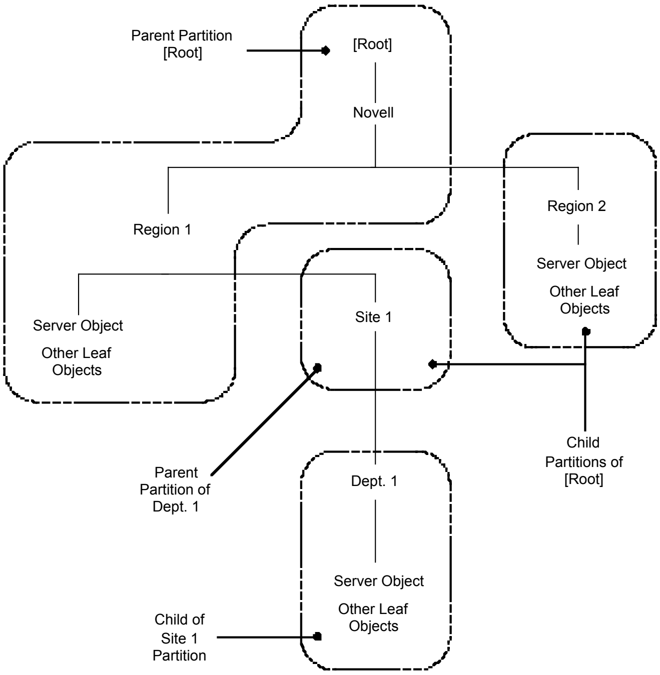
  Exception: For a location that has only one server, place the master replica for that partition locally, and store a read/write replica at the next nearest WAN location. (This is the one hop rule for NDS replication.) This assumes that the administration is distributed by site. In most cases, try to store the master replica where it will be accessed most.
- Minimize the number of replicas per partition. More replicas may mean more management if a partition needs to be repaired. All replicas (and subordinate references) in a replica set need to be contacted to perform synchronization and repair operations. If any are down or unreachable, the action will be put on hold until the missing replicas become available. Do not exceed the recommended number of replicas per partition (from the Quick Design tables).
- Replicate locally unless a location only has one server.
- Do not place more replicas than the Quick Design tables suggest.
- On a replica server (a server containing only NDS replicas) do not place more than the suggested number from the Quick Design tables, including subordinate references.
- Good replica placement reduces, but will not necessarily eliminate, subordinate references. It may be necessary to introduce additional layers of partitions in order to control subordinate reference placement. These layers are typically referred to as “placeholder” layers.

  Subordinate references exist to facilitate discovery of data within the NDS tree. They allow the client to “walk the tree” in order to find resources. Their size is substantial and they must be treated as a full replica for purposes of determining replica counts per server. They cannot be used to authenticate users. Finally, they must be available (on-line and reachable) in order to perform partition boundary operations. If a subordinate reference is not available, the operation will stall indefinitely until such time as the subordinate reference becomes available. This can cause a substantial backup in NDS synchronization and should be avoided if possible.

  Subordinate references are placed automatically by NDS according to the following rule. Any server that contains a replica of a parent partition (but does not contain a child of that parent) will be given a subordinate reference to that child. In simple terms, it is a placeholder or pointer to where the information can be found on another server in the replica set.

As shown in the following figure, any server that held a replica in the [Root] replica ring, but did not have a replica of the Region 2 replica ring, would be told where that information can be found by being given a subordinate reference to the information (A pointer to where the replica is stored).

Proper replica placement also provides bindery service access when necessary, and improves name resolution.



Example of Parent-Child Relationships

Note: Novell recommends against the use of read-only replicas because users cannot use them to authenticate without access to a read/write replica. Read-only replicas do, however, participate in replica synchronization, which can cause unnecessary NDS traffic. Read-only replicas are available in NDS because they are part of the X.500 specification.

Mixed-Tree Environments

During the migration of NetWare 4.x to 5, a mixed-tree environment is created. While this is a normal condition, it requires special handling and attention. There are issues surrounding the placement of replicas that need to be monitored. It is important to impress clients with the need to monitor this situation as the recommendations will change as new patches and DS versions are released, and technical best practices are refined.

Current best practices dictate the following:

- It is not currently recommended to house a master replica of a mixed (NetWare 4 & 5) replica set on a NetWare 4.x server.

  Note: A master replica can be successfully placed on a NetWare 4.11 server only if the NetWare 4.11 is running DS 6.06 or greater and if there are no NetWare 5 servers running Pure/IP.

  The first issue is addressed by updating the DS, while the second can be circumvented with a properly placed Migration Agent. Please see the Pure/IP section of the NetWare 5 methodology for details on placing MAs.
- Under most circumstances, house the master replica of any partition with replicas on both NetWare 4.11 and NetWare 5 servers in it, on a NetWare 5 server with IPX enabled.
- When inserting a NetWare 5 server into a replica ring, the master replica must be on a NetWare 5 server.
- Upgrade the schema of the DS tree by upgrading a server holding a replica of [Root] before inserting any other NetWare 5 servers into the tree.

  Note: When upgrading the schema using the upgrade wizard, the schema is only upgraded from the root of the partition containing the server, downward in the tree. Therefore, if you upgrade a non-[Root] server, the schema will be extended only from that partition downward. Parts of your tree will be using different versions of the schema. This can cause problems with partition operations later.
- Currently, Move Sub-Tree Operations in a mixed-tree environment require special handling. When moving partitions within the tree, you must first place the master replica of the partition being moved on a server that is outside of that partition. You may move it back once all moves are completed and synchronized. This will be addressed in a later revision of DS.
- These recommendations may change. You and your client must be diligent in keeping abreast of current situations concerning this topic.

Replica Placement

Follow these steps for creating and placing replicas:

1. Review the top-level NDS tree design.

2. Review the bottom-level NDS tree design.

3. Review the server information table. (In the PFC)

4. Determine and verify server location by partition.

   Note: Replicas do not have to be placed on servers within the partition.

5. Upgrade the server information table.

   Append the location of each server to the server information table in the PFC.

6. Review customer system and needs.

   The following questions need to be answered before replicas can be created and placed:
   - Is there more than one server available locally to hold a partition?
   - Is the customer system a WAN or LAN-only system?
   - Does the customer want off-site disaster recovery?
   - What protocols are in use (IP/IPX, Pure/IP, Pure/IPX) per server?

7. Create and place replicas.

   Create and place replicas according to the system environmental conditions described in the following table:

System Environment	Replica Placement
One (only) server available locally	Place a R/W replica on the local server and place the master on a secure server at a regional/corporate site no more than one WAN hop away. (Other methodologies may require local master storage.)
Multiple servers in partitions	Place all replicas locally if possible. If off site storage is deemed necessary, place no more than one WAN hop away.
LAN-only	Place master and 2 R/W replicas at the minimum for fault tolerance. Ideally, these servers should not be used for other services.
WAN	Place replicas on local servers if possible Place read/write replicas no more than one WAN hop away from the master replica.
Mixed-Protocol	
All IPX replica servers	Place master on either NetWare 4.11 or NetWare 5 server.
Mixed IPX & Pure/IP replica servers	Place master on NetWare 5 server with IPX and IP running (or use a Migration Agent).
Pure/IP replica servers with NetWare 4.11 (no replica)	Place master on NetWare 5 server with IPX and IP running. (or use a Migration Agent) There is currently a problem with the processing of backlinks and external references if the master is on a NetWare 4 server.
Disaster	
Off-site disaster recovery needed	As outlined above, place replicas locally unless you have a business need to place them remotely. Off-site disaster recovery should be examined closely to see if its benefits outweigh the additional traffic, and inconvenience of possible failed WAN links. In any case, place the off-site replica on a reliable server in a secure, reliable facility.

8. Complete the replica matrix in the PFC.

Task 7—Develop Network Time Management Design (Time Synchronization)

To develop a network time management (time synchronization) design, following these steps:

1. Assess extent of the network system.
   If the customer's network system is or includes a WAN, continue with step 2.
   If the customer's network system is a LAN, go to step 11.

2. Review the completed NetWare Server Information table in the preflight checklist.
   Obtain time zone, Daylight Savings time zone observance, and offset.

3. Assess the quantity of servers.
   If there are more than 30 servers in the network, continue with step 4.
   If there are 30 or less servers in the network, go to step 11.

4. Plan the Custom Time Provider Group.

   Determine which servers will be voting members of the time provider group.

   Adherence to the WAN infrastructure is critical, as these servers must be able to contact each other for polling and voting.

5. Create a Time Provider Group matrix.

   Identify Reference, Primary, and Secondary time servers.

6. Update the NetWare Server Information table in the preflight checklist.

   Append the Time Provider Group matrix to the NetWare Server Information table in the preflight checklist.

7. Determine if SAP is an issue.

   If SAP is an issue for the customer, continue with step 8; otherwise, go to step 10.

8. Create configured lists for each time server with SAP=OFF.

   Load MONITOR.NLM - Server Parameters - Time

   TIMESYNC Configured Sources = ON

   TIMESYNC Service Advertising = OFF

   TIMESYNC Time Sources = list from Time Provider Group matrix

   TIMESYNC Type = Reference, Primary, or Secondary

9. Print the TIMESYNC.CFG files from each time server and go to step 12.

10. Create the time provider group with SAP = ON.

    Load MONITOR.NLM - Server Parameters - Time

    TIMESYNC Configured Sources = OFF

    TIMESYNC Service Advertising = ON

    TIMESYNC Type = Reference, Primary, or Secondary

    Go to Step 12.

11. Use the Default Time Configuration method.

    Create one Single Reference timeserver; all other servers are econdary time servers.

12. Document the time synchronization design.

    After reviewing the information in the following section, document the time synchronization design and incorporate it into the final NDS design.

Determine Network Time Synchronization Configuration

The last step in NDS design NDS is to determine the time synchronization configuration. Time synchronization is the ability of NetWare servers to coordinate and maintain consistent time among all servers in the NDS tree. Time synchronization is necessary to ensure that each NDS event receives an accurate time stamp. Without an accurate time stamp, objects created or changed on one server may not be able to replicate to another file server.

While NDS does not require the correct time, it does require that all servers agree on the same time. Time syncing will be the very first thing checked before partitioning or merging operations occur, and each of these operations will report an error if time is not synchronized.

The TIMESYNC.NLM coordinates time stamps between all servers, and maintains each server’s Universal Time Coordinated (UTC), also known as Greenwich Mean Time (GMT).

Note: Some software applications may require the correct time, therefore setting the correct time on your file servers is recommended.

Design Basics

The objective in planning the time synchronization strategy is to determine an efficient time synchronization method to use, and then identify the best way to set up and manage that method across the network.

Definition of Terms

- Service Advertising Protocol (SAP): A Novell protocol used by servers to advertise their services to the network.
- TIMESYNC NLM: A Novell proprietary time synchronization service available on NetWare. TIMESYNC.NLM is a protocol-independent time synchronization management tool. See comparisons between NetWare 4.x and NetWare 5, below.
- Network Time Protocol (NTP): An Internet protocol specification (RFC 1305). NTP is a way to share time among different operating systems and platforms, such as Windows NT, Macintosh, UNIX, and NetWare.

Time synchronization design requires consideration of the network environment:

- NetWare 4.x: TIMESYNC.NLM uses IPX as its communication protocol, relying on SAP 026b (timesync), SAP 0004 (file server).
- NetWare 5: TIMESYNC.NLM uses TCP/IP as its communication protocol, while retaining it's ability to work over IPX. Time can flow from IPX to IP and vice-versa, as long as there is at least one server that has both IP and IPX to bridge the two sides. The Migration Gateway solution is not needed for this purpose.
- Mixed operating systems (NetWare, Windows NT, Unix, Macintosh): TIMESYNC.NLM is enhanced to include NTP functions for use on NetWare 5.

  This makes it possible for NetWare networks to synchronize time with NTP networks, NTP networks to synchronize time with NetWare networks, and NetWare networks to obtain time from reference time sources on the Internet.

For more information, see the section titled "NTP and TIMESYNC Features and Setup" later in this document.

TIMESYNC.NLM

The latest version of TIMESYNC.NLM, v5.12 and higher, uses the hardware clock to check time instead of the software clock established by the NOS. The unreliability of the software clock for checking time (timer interrupts being lost), prompted the change to the hardware clock.

In all types of time servers, including Primaries and Secondaries who adjust their clocks, both the hardware and software clock will be updated once the time is checked with the hardware clock.

Types of Servers

Every NetWare server in an NDS tree must participate in the time synchronization process, regardless of whether it holds an NDS replica or not. There are four time server types:

- Single Reference—time provider
- Reference—time provider
- Primary—time provider
- Secondary—time consumer

The time server type is dependent upon the Time Configuration method chosen, and is set at the server console by typing SET TIMESYNC TYPE = [*time server type*] or using the MONITOR.NLM and choosing Server Parameters, Time, and selecting Timesync Type.

Time Configuration

Time Configuration outlines a strategy for time server definitions and placement, for which there are two options:

- Default—Single Reference Time Server

  Pros: Simple, requires no advanced planning or configuration files, thus reducing the possibility of time synchronization errors.

  Cons: Single point of failure if the Single Reference time server fails. Every other server on the network must contact this Single Reference Server.

- Custom—Time Provider Group

  Pros: Greater fault tolerance and accessibility by distributing the time servers to multiple locations.

  Cons: Requires careful planning. Configuration files on each server must be maintained if configured time sources will be used.

Time Communication

Time Communication outlines a strategy which identifies how the servers will communicate with each other. Three options exist:

- Default—Service Advertising Protocol (SAP) Method

  Pros: Requires no intervention, as this is the default communication method.

  Cons: Since SAP is self-configuring, there is no protection against misconfigured timeservers. Also causes a small increase in network traffic.

- Custom—Configured Lists

  Pros: Added flexibility and control of time synchronization communications.

  Cons: If SAP is set to OFF or if a server is removed, the configured list on each server must be configured or updated. When installing a new server into the tree, the Timesync.cfg file must be updated on the server in order for Directory Services to be installed.

- Combination—Configured lists and SAP

  Pros: Added fault tolerance if a time provider is not available in a server's list, then SAP can be used.

  Cons: Added network traffic.

The following information is required, independent of the Time Configuration and Time Communication components:

- The time zone in which the server is installed
- The observance of daylight savings time
- Daylight savings time offset (if applicable)

Time synchronization design and implementation is relatively easy and quick for any size NetWare network. Once implemented, very little additional activity is required to maintain time synchronization functions.

Design Specifics

Time Configuration

The physical location of the file servers, with respect to WAN/LAN infrastructure and the network connectivity between them, must be considered for the Time Configuration method to be used. For purposes of this methodology, the Default (Single Reference Time Server) configuration is defined for a LAN-only network, and the Custom (Time Provider Group) configuration is defined for a WAN environment.

- **LAN-only Network**

  The default—single reference time server method is for small networks that have fewer than 30 file servers and are on a LAN network only—no WAN links exist.

  With this method, one file server is designated as the single reference time server and is the sole time provider in the network, and all remaining servers are designated as secondary time servers. Do not use reference or primary servers with this configuration. Doing so will generate an error message at the file server console stating that a single reference time server cannot exist with another time provider (such as a reference or a primary).

  This method is very simple to administer because it requires no custom configuration files. Rather, secondary servers ask for time from the single reference server using SAP.

- **WAN Environment**

  The custom—time provider group method provides greater fault tolerance in a WAN environment by distributing the time providers throughout the geographical locations in the network. Servers in a time provider group poll each other to vote on the correct time.

  With this method, one reference time server and two to seven primary time servers are used in a time provider group. The time provider group in turn provides time to all other servers, which are secondary time servers. Each of the primary time servers should be placed close to the secondary time servers which will receive time from them, and the Primary time server should have a reliable network link to the Reference time server.

  With extremely large networks (i.e., hundreds of servers across the globe), companies can have more than one time provider group. Each reference server must synchronize with the exact same external time source.

  Recommendations

  Do not exceed five time providers in a time provider group.

  The vast majority of the network should be Secondary time servers. Place primary/single/reference time servers at key locations.

Time Communication

Once the time configuration method is chosen (default or custom), there are three options for establishing time synchronization communication:

- Service advertising protocol (SAP)
- Configured lists communication
- Combination of both options

Service Advertising Protocol (SAP). The SAP communication method is the default, requires no manual configuration, and is generally used with the default time synchronization configuration. SAP does not require custom configuration changes to the time servers as new NetWare servers are added to the network.

By default, time providers such as reference, primary, or single reference servers advertise their presence on the network using SAP 0x026B. The SAP from the time servers can cause a small amount of traffic on your network. Therefore, do not use this method for communicating if the network requires a reduction in SAP traffic. If SAP is used for time synchronization communication, then any routers that connect your NetWare servers cannot filter SAP 0x026B.

Configured Lists Communication. This method requires system administrators to provide a special configuration file (SYS:\SYSTEM\TIMESYNC.CFG) for every server. TIMESYNC.CFG specifies exactly which servers should be contacted for providing and receiving time.

If SAP is not being used, every server in the NDS tree must have a configured list to participate in network time. Configured lists reduce the SAP traffic for SAP 0x026B on the network because they specify the time providers by name or IP address in NetWare 5. Configured lists give the system administrator complete control of the time synchronization hierarchy. If you use this option, do not filter SAP 0x0004 (file server) on the network because time providers use it to locate one another.

Note: This option has both pros and cons. On the one hand, no one can insert a server into the tree without an appropriately configured TIMESYNC.CFG file since time must synchronize before NDS can be installed or a replica placed on that server. However, if SAP is not turned off and the TIMESYNC.CFG is not configured, the server cannot be added into the tree.

Combination of Both Options. A configured list can be used in conjunction with SAP. In this case, the server gets time from the servers in its configured list as long as at least one of them is available. If none are available, the server uses SAP. This adds a little more SAP traffic, but the combination provides increased fault tolerance.

When any server initiates contact with other servers during its polling cycle, it first reads from its configured list (SYS:\SYSTEM\TIMESYNC.CFG), then writes the information into a table. If other servers are using SAP and this server is responding to SAP broadcasts, the server then adds servers that are using SAP to the bottom of the table.

Primary and Reference servers contact everything in their configured lists and SAP lists to resolve their votes. On the other hand, if a Secondary server can resolve its synchronization efforts from the first server in its configured list or the SAP list, that is as far as it will look. It stops there and will not proceed down the table.

With this combination method, do not filter SAP 0x0004 (file server) or SAP 0x026B (time synchronization) on the network.

Recommendations

Determine the customer's issues with overall network traffic and any issues related to SAP usage.

If a reduction in network traffic is needed, create configured lists with SAP = Off. (See the sample time synchronization design towards the end of this document, which incorporates the use of NTP time sources in NetWare 5.)

Time Synchronization Traffic

Time synchronization traffic is not a frequent process. Once the time synchronization system stabilizes, time synchronization occurs by default every ten minutes and is controlled by the SET command:

> SET TIMESYNC polling interval = ***n***
>
> *where* default ***n*** is 600 seconds (10 minutes) in a range of 10-2,678,400 seconds

When time is not synchronized, polling occurs every 10 seconds (the minimum) until synchronization is reestablished. Increasing the TIMESYNC polling interval parameter as soon as time is stabilized on the network can reduce time synchronization traffic.

Actual traffic load is determined by how many time exchanges (that is, the polling count parameter) configured for each polling interval. For voting servers in the time provider group, default traffic is represented as:

- N(N-1) * (polling count) * 332
- *where* N = the number of servers in the time provider group
- *where* default polling count = 3 in a range of 1-1,000 (set TIMESYNC polling count = *x*)
- *where* Each timesync NCP packet is 166 bytes, multiplied by two for a send/receive pair = 332

Recommendations

Keep the Polling Interval setting at the default of 600 seconds, with the number of time providers is under 10.

Do not set the Polling Count below the default value of 3, especially if time synchronization is operating across a WAN.

As the number of servers in the time provider group increases, so does the amount of traffic per default 10 minutes. The general rule is to have 4-5 servers in the time provider group. This is a guideline, not a "fail" number. In very large global networks, create multiple time provider groups on the network.

A secondary server can serve as a time source for other secondary servers (reference, primary and single time source servers cannot point to a secondary). However, problems in the time structure may result as the number of levels removed from a "real" time provider increases. Secondary time servers as time providers to other secondary servers is not a recommended method of distributing time.

NTP and TIMESYNC Features and Setup

Since the initial release of NetWare 5, NTP functions have been incorporated into TIMESYNC.NLM. Both NetWare and NTP time services are supported, allowing the server to act as both an NTP server and an NTP client.

TIMESYNC NLM is actually an adaptation of NTP, and uses the same algorithms as NTP to account for network delay when obtaining time from a time source. For simplicity some features of NTP have been not been included in TIMESYNC NLM.

TIMESYNC.NLM can accept time providers in the following formats:

- SAP name
- Internal network number
- IP address
- DNS names (FQDN)
- NDS name (FDN)
- IP-ADDRESS:123 (this is the only form that uses the NTP protocol)

Configuring an NTP Time Source

To configure TIMESYNC to use the NTP protocol, add the NTP time source to the server's configured list. The format is IP-ADDRESS:123, which tells the TIMESYNC.NLM to use the NTP protocol on port 123 instead of the NetWare time services protocol.

- Identify the NetWare Single or Reference time server
- Verify that TIMESYNC.NLM on the Single or Reference time server is version 5.12 or higher.
- Identify the primary NTP time sources on the NTP network. See http://www.connectotel.com/netware
- Update the configuration of the Single or Reference servers to obtain time from NTP servers. This is achieved either by modifying the set parameters from the console prompt, or from MONITOR.NLM:
- Set TIMESYNC Time Sources = 1.2.3.4:123;5.6.7.8:123

To ensure fault tolerance, configure multiple NTP time sources in the list.

Caution: Do not apply any atomic clock or other external time sources to any time servers when using NTP. Doing so may cause time synchronization corruption.

When TIMESYNC.NLM is configured to obtain time from NTP time sources, the local hardware clock of the Single or Reference is inconsequential.

If TIMESYNC NLM has to communicate with an NTP source across the firewall, incoming UDP (User Datagram Protocol) traffic for UDP port 123 must be permitted. Since port 123 is the well known port for NTP, this should not be a security issue.

Sample Time Synchronization Design

Time Configuration = Custom - Time Provider Group

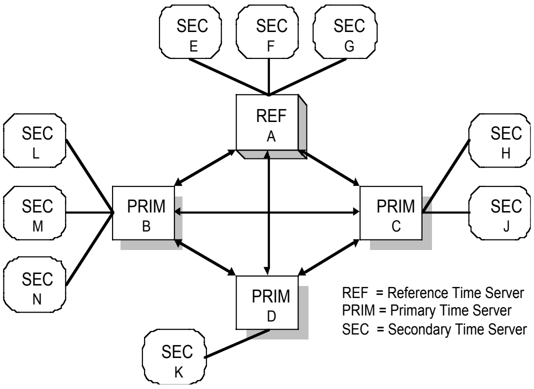
Time Communication = Custom - Configured List (no SAP)

Create one time provider group with four time providers (one Reference server and three primaries). The time providers will be in location #1 (one Reference and one Primary), location #2 (one Primary), and location #3 (one Primary). The Reference server will get its time from an NTP time source Examples of this configuration are shown in the Time Provider Group drawing and matrix, below.

If TIMESYNC.CFG lists the time providers in order according to proximity, all remaining file servers will be Secondary servers and will get their time from the physically closest time provider, either the Reference or one of the three primaries.

These time providers vote to determine the appropriate network time with respect to all the different time zones in the network. The Reference server has a weight factor of 16 and the primaries have a weight factor of 1.

This allows better WAN link utilization and decreases the chance of a server being inserted into the corporate production tree by mistake—the new server requires time synchronization (default uses SAP 026B) to install NDS properly and be placed into a container.


SEC E
SEC F
SEC G
REF A
SEC L
SEC H
SEC M
PRIM B
PRIM C
SEC J
SEC N
PRIM D
SEC K
REF = Reference Time Server
PRIM = Primary Time Server
SEC = Secondary Time Server

Time Provider Group Drawing

Time Provider Group Matrix

Time Server Type	Location	Server Name	IP Address	Configured List
Reference	1	RefA	172.31.21.59	18.72.0.3:123;128.115.14.97:123
Secondary	1	SecE	172.31.21.61	172.31.21.59;172.31.21.76
Secondary	1	SecF	172.31.21.63	172.31.21.59;172.31.21.76
Secondary	1	SecG	172.31.21.65	172.31.21.59;172.31.21.76
Primary	1	PriB	172.31.21.76	172.31.21.59;172.27.21.35
Secondary	1	SecL	172.31.21.77	172.31.21.76;172.31.21.59
Secondary	1	SecM	172.31.21.79	172.31.21.76;172.31.21.59
Secondary	1	SecN	172.31.21.81	172.31.21.76;172.31.21.59
Primary	2	PriC	172.27.21.35	172.31.21.59;172.31.21.76
Secondary	2	SecH	172.27.21.37	172.27.21.35;172.31.21.59
Secondary	2	SecJ	172.27.21.39	172.27.21.35;172.31.21.59
Primary	3	PriD	172.26.21.19	172.31.21.59;172.31.21.76

Secondary	3	SecK	172.26.21.20	172.26.21.19;172.31.21.59

Troubleshooting

DS Error -659

DS Error -659 is a time synchronization error.

Check time synchronization through DSREPAIR.NLM. After loading DSREPAIR at the server console, select Time Synchronization. This will provide an immediate view of how time is operating on the network by displaying every server, DS Version, Replica Depth, Time Type, and whether the server is In Sync (yes or no). Additionally, the list shows how far off (in seconds) a server is from being completely synchronized.

NDS allows a default +/-2 second differential for a server to still be considered fully synchronized.

There are some exceptional conditions that may cause the servers to fall out of time synchronization. Some of the conditions can be:

- A clogged network
- A faulty router
- An NLM that hogs CPU cycles and prevents the software clock from being updated
- An NLM that sets off clock interrupts so that the software clock does not get updated

If the network uses SAP to establish time synchronization, verify that SAP 26B is being received at the server:

- Load IPXCON at the server console, and select Services.
- View the list of services. SAP 26B should appear in the right column.

If it does not, there may be a problem with the router filtering out SAP 26B.

TIMESYNC.NLM Debug Switches

To view the Timesync Debug screen , Set TIMESYNC DEBUG = 7 at the server console.

The Timesync Debug screen provides valuable information such as:

- Time Server Type of the server
- Which server was contacted for time and its time server type
- At what time polling took place
- What was the time offset discovered
- If time is synchronized or not

This information is displayed at each polling interval.

Task 8—Test and Verify

Note: Consultants should obtain their own copy of the Logic Source for NDS CD from their practice manager or visit http://www.support.novell.com/logicsource/

Logic Source for NDS is the most comprehensive technical support resource ever written for NDS. It represents the entire logic flow of NDS and provides an in-depth understanding of the concepts, processes, and operations. This CD is an excellent resource for resolving NDS problems.

Verify Partition Status in NDSMGR

Using NDSMGR, identify any partition problems.

If there are partition problems, then complete the following steps:

1. Use the Logic Source CD to determine the cause of the problems.
2. Perform the resolution tasks recommended by the Logic Source CD.

Verify Replica Synchronization Status

Using DSREPAIR, identify any replica synchronization problems.

If there are replica synchronization problems, then complete the following steps:

1. Use the Logic Source CD to determine the cause of the problems.
2. Perform the resolution tasks recommended by the Logic Source CD.

Verify Timesync Status

Using DSREPAIR, identify any time synchronization problems.

If there are time synchronization problems, then complete the following steps:

1. Use the Logic Source CD to determine the cause of the problems.
2. Perform the resolution tasks recommended by the Logic Source CD.

Verify NDS Tree Stability

Verify that the NDS tree is stable and complete.

Prepare System Design Report

The information in this report will be set up and tested in the lab.

Task 9—Develop and Deliver NDS Design Report

Follow these steps to review and deliver the NDS design report:

1. Schedule a project manager review.
2. Deliver the system design report to the customer.

Sample Project Plan

Done by project manager

Task List
Obtain Lead
• Generate proposal and statement of agreement
• Tentatively schedule engagement and resources
• Obtained signed statement of agreement
• Obtain signed purchase order
• Send preflight checklist to customer (optional if customer will complete)
• Commit scheduled engagement and resources
Develop solution design
Design top level of NDS tree
Design bottom level of NDS tree
Review NDS design guidelines
Review NDS eDirectory considerations
Establish naming standards
Design and discuss NDS security
Discuss NDS administration
Develop partition design
Develop partition replication design
Develop network time management design (time synchronization)
Test and verify NDS design
Develop and deliver NDS design report

Closing the Engagement

Task 1—Closing Tasks

Task 2—Prepare Final Report

The final report will detail:

(1) What's been done (emphasizing all WOA objectives have been met)

(2) What remains to be done by the customer; optionally, mention a new WOA could be created to finish the implementation

Task 3—Deliver Final Report to Customer

Option: Have the CBM or CPL review the report first.

Sample Project Deliverable

The following section is a template for a report that would be delivered to a client following your consultant engagement.

This report is intended to be printed on both sides of the paper—therefore, there are elements that seem odd when viewed in order, but are correct when printed as intended. For example, the copyright and trademark statements on the second page should be printed on the back of the cover page.

NDS Design Report

Project Title Goes Here

Prepared for:

Customer Company Name Goes Here

If draft, note revision number here—If not a draft, delete text

Report Date:	Date goes here
Prepared By:	Consultant name goes here
WOA Number:	Work order agreement number goes here
Filename:	Name of file goes here

Copyright

Trademarks

Table of Contents

Executive Summary ... 61
Introduction ... 61
Background ... 61
Assessment ... 61
Recommendations ... 62
Value ... 62

Overview ... 63
Who Should Read This Report ... 63
Acknowledgements ... 63
Follow-up ... 63
What You Need to Know ... 63
How to Use the Information in This Report ... 63

Introduction ... 64
Statement of Work ... 64

Novell Directory Services Design ... 65
NDS Design Guidelines ... 65
The Four Principles of NDS Design ... 65
Understand the use of NDS objects ... 66
NDS Design Tasks ... 66
XYZ Corporation: Top of the tree design ... 67
Organizational unit locations ... 67
Using regional OUs ... 68
XYZ Corporation: Bottom of the tree design ... 69
Apply special design factors ... 69
Partition Design ... 70
Quick Design ... 70
Partition Diagram ... 71
Replica Placement ... 72
Partition and Replica Matrix ... 73
Network Time Management Design (Time Synchronization) ... 74
Types of Servers ... 74
Time Configuration ... 74
Time Communication ... 74
XYZ Corporation Time Synchronization Design ... 75
Time Provider Group Drawing ... 75
Time Provider Group Matrix ... 76
Naming Standards ... 77
Basic NDS Security policy ... 81
Physical Security ... 81
Servers ... 81
Workstations ... 82
Protecting the Data ... 82
Login Security ... 82
Login/Password Authentication ... 82
Login Restrictions ... 83

NDS Security ... 84
File System Security ... 84
Objects and properties ... 85
NDS Administration ... 85

Summary ... 86

Transition Notes ... 86
Direction ... 86
Timeline ... 86

Appendix A: 87

Executive Summary

Introduction

XYZ Corporation relies upon its computer network for daily business operations. Novell Directory Services (NDS) helps companies to reach higher levels of productivity and efficiency by making the network easier to access and manage. This ease of use and administration significantly lowers the total cost of ownership (TCO) of a network. Leveraging NDS as the global directory provides benefits such as application accessibility and desktop management. A consultant was asked to assist XYZ Corporation with their NDS tree design, and make recommendations for implementation.

Background

Provide information about the company and its current technologies, and how the technologies enable them to operate in their industry.

The technologies in place enable XYZ Corporation to provide comprehensive administrative support to a system of independent businesses which deliver safe, reliable transportation services. These services are provided throughout the United States, and portions of Canada and Mexico.

XYZ Corporation is a large and growing organization with over 1,000 desktop computers and several servers. The current IntraNetware (NDS) environment consists of one production tree. Each Carrier Group administers their branch of the tree, independently of the other Carrier Groups. A decentralized approach to administration is feasible in such a geographically diverse organization like XYZ Corporation. However, in order to protect the overall system reliability and manage the network efficiently, XYZ Corporation should implement standards consistently throughout the tree, and several key processes should be handled centrally. These processes include NDS partitioning, schema management, and patch management. Management and security of network resources at the Carrier Group and department levels can still be maintained. The efficiencies achieved from a coordinated, centralized, and distributed management model for the NDS tree will reduce the total cost of ownership of the network.

Assessment

Summarize the key points from the Technical Assessment/Impact Study Report.

XYZ Corporation has built a very powerful system on Novell' s enterprise network operating system. Leveraging NDS is a key component in reducing the cost of ownership of the XYZ Corporation network. We observed a number of factors escalating the cost of network management. These include:

- Inconsistent and/or outdated software revision levels on the NDS servers
- Lack of consistent standards throughout the NDS network
- Periodic server outages caused by NDS synchronization issues

A complete NDS design and our recommendations for efficiently operating the NDS tree at XYZ Corporation was conducted. The details of this report focus on the long term strategy of NDS for XYZ Corporation, as a single point of administration for the network.

Recommendations

While there is no absolute method to design an NDS tree, there are four principles derived from Novell's experiences which should be applied toward achieving an efficient design. Efficiency is achieved when the tree is stable and the design provides for the least amount of NDS synchronization traffic. These principles apply regardless of the size of the company.

The primary design goals for the XYZ Corporation NDS tree are to organize and represent the network resources, to design a flexible tree where changes are easily made, and to represent the entire organization in a single tree.

Following are the key recommendations for the XYZ Corporation NDS tree, which are presented and substantiated in this document.

- Review and understand NDS Design Guidelines
- Design the NDS tree
- Divide NDS into partitions and replicas to provide scalability and fault tolerance
- Configure an efficient time synchronization strategy for NDS operations
- Create and implement standards for consistency and ease of use
- Implement security measures to protect network resources

Value

The following benefits are derived from a well-planned NDS design:

- Organizes the network resources (such as printers and servers) for ease of access, manageability, and lower cost
- Provides a consistent plan for the rollout of NetWare, including naming standards and migration strategies that can be used at all sites during implementation
- Provides flexibility so that as the corporation changes both organizationally and physically, the tree can accommodate those changes without major modification

Overview

This report is divided into three sections:

- Introduction
- Detailed NDS design solution
- Appendices

Who Should Read This Report

Determine who, within the customer's organization, should read this document. The document may be intended for a variety of readers—some may only read a subset of the document. Others may read the entire document. Whoever the readers are, list them here by position or title, not by personal name.

Acknowledgements

We would like to thank XYZ Corporation for the opportunity to assist you in the design of the XYZ Corporation NDS tree.

Follow-Up

We are committed to ensuring that XYZ Corporation receives maximum benefit from this report. Please feel free to contact <Consulting Branch Manager> with any questions you may have. We will also follow up with you after you have had time to review this report to ensure it meets your needs.

What You Need to Know

Before your customers can understand the information and implement the recommendations in your document, they must have certain skills and knowledge. List here the skills and knowledge that anyone using the products in this project must have. If there are additional things that only this customer needs to know, add them here.

How to Use the Information in This Report

Provide content maps, guidelines, directions, or instructions on how the information is organized in this report.

Introduction

We conducted a <Consulting Engagement> for XYZ Corporation from <dates of visit>, 2000 for Novell Directory Services design. This report details the design solution and recommendations for the XYZ Corporation NDS tree. References may be made to information contained in the *Technical Assessment/Impact Study Report*.

While on-site, we analyzed your <specialties> environments in an effort to determine your specific needs. Based on that analysis, this report provides some recommended technical solutions for implementation. These solutions have been created exclusively for XYZ Corporation and they are intended to help you improve your network manageability, leading to its increased performance.

Statement of Work

The project scope from the work order between Novell and XYZ Corporation is shown below. This the final deliverable within this scope.

Insert the NDS Design Statement of Work here. The report detail follows these items. Example:

Develop NDS Design

- Review NDS Design Guidelines
- Design Top Level of NDS Tree
- Design Bottom Level of NDS Tree
- Design Partitions
- Create and Place Replicas
- Create Network Time Management Design (Time Synchronization) Strategy
- Review Existing Naming Standards & Develop
- Develop Basic NDS Security policy
- NDS eDirectory Considerations
- NDS eDirectory Design Guidelines
- Test and Verify
- Report

Novell Directory Services Design

NDS Design Guidelines

Novell Directory Services (NDS) is an information name service in NetWare that organizes network resources such as users, groups, printers, servers, volumes, and other physical network devices into a hierarchical tree structure.

The Four Principles of NDS Design

Understanding and applying the four principles of NDS design will enable XYZ Corporation to construct an NDS tree that provides network efficiency and information accessibility for the entire organization. These four principles apply regardless of the type or size of the network. We have reviewed these principles with XYZ Corporation, and has provided detailed recommendations for implementation of the XYZ Corporation tree:

Principle 1: The NDS tree should represent the network infrastructure.

- The NDS tree should be designed and optimized to reflect the location and placement of the network resources.
- NDS design occurs in two phases:
  - The design of the top layer of the tree: The top layer of the tree must take into account the network infrastructure and any wide-area links based on geographic locations.
  - The design of the bottom layer. The bottom layer of the tree is designed around local-area network infrastructure, reflecting the departments and workgroups. Company organization charts and similar documents are used as a guideline.

Principle 2: Divide NDS into partitions and replicas to provide scalability and fault tolerance.

- Partitioning is the method by which NDS is logically segmented for greater efficiency across multiple NetWare servers.
- Replication is the physical placement of NDS partitions on various servers, which provides both fault tolerance and immediate information access to the users.

Principle 3: Use NDS objects to establish the organization, network administration, and user access.

- Create and implement standards for consistency and ease of use
- Implement security measures to protect network resources

Principle 4: Configure an efficient time synchronization strategy for NDS operations.

- Time synchronization is necessary for the proper functioning of NDS

Understand the Use of NDS Objects

A basic prerequisite for designing an NDS tree is to understand the use and placement of the NDS objects, which will represent the XYZ Corporation resources in the tree. A review of the most common NDS objects was conducted.

NDS Design Tasks

Completion of the following tasks will lead to a successful design and implementation of NDS at XYZ Corporation.   We have gathered some of the information required to complete these tasks in the Technical Assessment/Impact Study Report:

- Gather corporate documents
    - The wide area network (WAN) diagrams
    - A list of the major locations or campuses
    - A list of departments, divisions, and workgroups
    - A list of current and planned servers, printers and other resources
- Design the top level of the tree
- Design the bottom level of the tree
- Review and modify the tree if necessary
- Design the NDS partitions and replica placement
- Create a time synchronization strategy
- Review and develop naming standards
- Develop basic NDS security policy

XYZ Corporation: Top of the Tree Design

NDS tree design is logically split into two phases: the top-level design and the bottom-level design. The overall tree design takes the shape of an inverted tree with the [Root] object on top. Overall tree design should represent the shape of a pyramid, smaller at the top and wider at the bottom.

The top level refers to the first layers of the tree that represents XYZ Corporation's WAN infrastructure and includes the organization (O=) object and the first or second levels of organizational unit (OU=) objects. The Admin user object will be created just below the organization layer; only a few users and network resources should be placed at the top levels in the tree.

The top level of the tree is the most important functionally because it serves as the foundation for the rest of the tree. Changes to the top level of the tree impact objects in the lower levels of the tree, therefore adjusting this level to accommodate changes or growth should be avoided as much as possible.

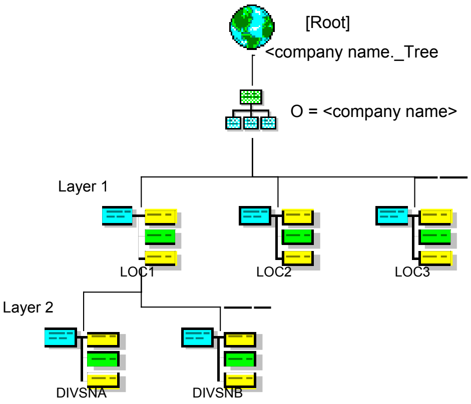
The top level contains [ROOT] XYZ Corporation_Tree, the Organization object XYZ Corporation, a location (first) layer (based on site), and a function or division (second) layer (based on services provided within the site.)

Standard guidelines for top of tree design have been followed, and this design is very scalable. There are a few areas which may need special attention, and they are discussed within the NDS tree description below.

Organizational Unit Locations

Each XYZ Corporation location should be represented as an Organizational Unit (OU) container in the tree. These location OUs are typically geographical sites within the company and represent the network infrastructure. A T1 link exists between each of the three location OUs. Under each location OU can exist one or more function/division OUs. Below each function/division OU are the department OUs, which will be represented later in the tree.

The topmost layers of the XYZ Corporation tree are shown in the diagram below. The OU names used in the diagram are those which were stated during our on-site visit, and may not be the actual names used in final production.



Using Regional OUs

Because XYZ Corporation has services worldwide, we discussed the future use of regional locations, which could be placed at the first level (just below O=XYZ Corporation). These regional OUs could be represented by country name (US, Canada, Mexico). This placeholder level is important to the design of the tree, mainly because it provides for the locations in the tree to match the major segments of the WAN infrastructure. Transcontinental links are functionally the top of the WAN infrastructure. Additionally, should network resources be implemented within the other regional OUs, namely Canada and Mexico. Then this structure will keep the pyramid-shape and access methods to those resources can be implemented consistently and efficiently.

XYZ Corporation: Bottom of the Tree Design

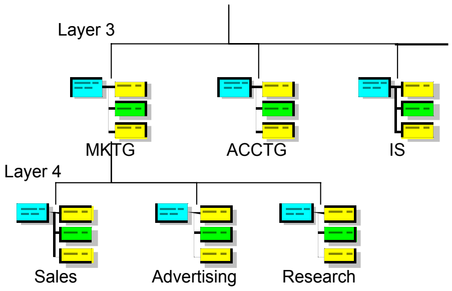
The bottom level refers to all layers below the representation of the WAN layers.

The bottom level includes the remaining hierarchy of OU and leaf objects for the XYZ Corporation organization. These lower OU objects are the departments and workgroups that contain the objects for users, servers, printers, queues, and other network resources.

Organization charts were used to assist in the design of the bottom level of the XYZ Corporation tree. Within each function/division at layer 2, OUs can be created to represent the departments, workgroups, and teams at the various locations of the company.

A tree designed with these organizational units at the bottom level, rather than at the top, is the most flexible and easiest for users and system administrators to use.

By using organization charts to determine the initial design of the bottom level, users will have some familiarity with the tree layout. As shown in the following diagram, the bottom level of the NDS tree is designed in a manner that keeps users close to the resources they use:



Apply Special Design Factors

Certain factors may need to be considered in the design of the bottom level of the tree. These factors impact only the users and network resources that are in the bottom-level container objects and do not alter the top-level tree design:

- Centralized versus decentralized administration
- Network infrastructure and partitions
- Location of physical devices
- Login scripts
- Bindery Services: Proper replica placement provides bindery service access when necessary, and improves name resolution. See the Partition and Replica section.

Partition Design

The [Root] partition should remain small and typically includes the [Root] object and the O= OrganizationName container only. The partition structure below this point depends on the physical layout of the organization. Since XYZ Corporation has a Wide Area Network (WAN), the design of the upper partitions should reflect its physical topology.

Use the following guidelines to partition the NDS tree for XYZ Corporation's wide area network:

- Base partitions on the WAN infrastructure. Create functional containers to support partitioning on a site level.
- Do not create a partition that contains leaf objects on both sides of a WAN link. This is called, "spanning the WAN" and it degrades performance.
- Partition around the local servers in each geographic area.
- Keep the partition size small.
- Limit the number of subordinate partitions

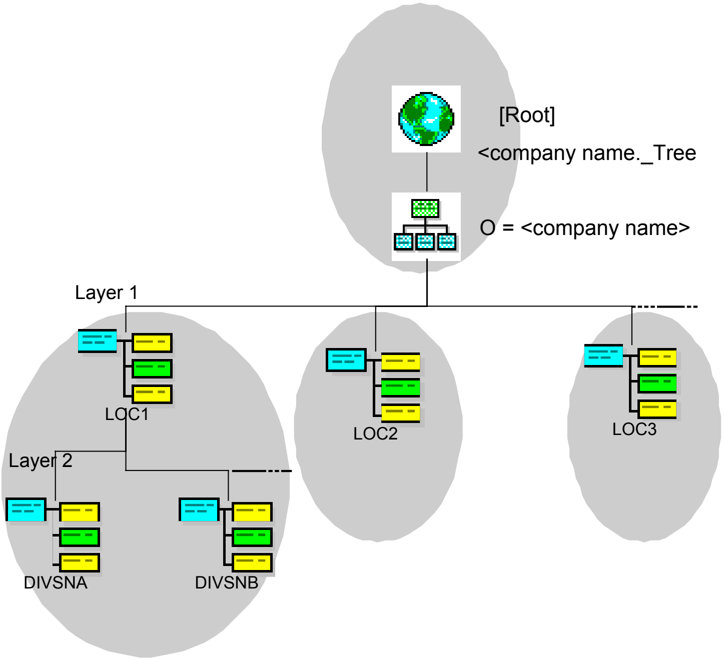
Partition the rest of the tree based on each geographic location in an organization. Split the NDS databases into partitions that contain only the information needed by a central set of users. Since tree partitions are typically based on the physical layout of the WAN, we recommend making each separate site location its own partition.

The quick design guidelines outlined below are recommended for partition design and replica placement at XYZ Corporation:

Quick Design

	NetWare 4.x ** (or mixed)	NetWare 5**
Partition size	Should not exceed 1000 – 1500 objects	Should not exceed 5000 objects
The number of child partitions per parent	Should not exceed 10 – 15 partitions	Should not exceed 30 partitions
Number of replicas per partition	Should not exceed 2 – 5 replicas, typically 3	Should not exceed 10 replicas
Number of replicas per server	Should not exceed 7 – 10 replicas	Should not exceed 20 replicas
Number of replicas per dedicated "Replica Server"	Should not exceed 30 replicas	Should not exceed 60 replicas
Recommended hardware requirements	100 MHz, 64MB RAM & 6GB SYS:	300 MHz and 128MB RAM & 13GB SYS:

Partition Diagram



Replica Placement

The primary goal of replication is to eliminate a single point of failure for an NDS partition. The two main objectives of replica design are to provide fault tolerance and reduce synchronization traffic. The following general guidelines are recommended for replica placement:

- Always have three replicas for fault tolerance
- Replicate locally
- Maximum Number of seven to ten Replicas per Partition
- Maximum Number of 15 Replicas per Server
- Replicate to Reduce Subordinate References
- Replicate to provide bindery service access
- Replicate to improve name resolution

We have reviewed the following information as it pertains to XYZ Corporation:

System Environment	Replica Placement
One (only) server available locally	Place a R/W replica on the local server and place the master on a secure server at a regional/corporate site no more than one WAN hop away. (Other methodologies may require local master storage.)
Multiple servers in partitions	Place all replicas locally if possible. If off site storage is deemed necessary, place no more than one WAN hop away.
LAN-only	Place master and 2 R/W replicas at the minimum for fault tolerance. Ideally, these servers should not be used for other services.
WAN	Place replicas on local servers if possible Place read/write replicas no more than one WAN hop away from the master replica.
Mixed-Protocol	
All IPX replica servers	Place master on either NetWare 4.11 or NetWare 5 server.
Mixed IPX & Pure/IP replica servers	Place master on NetWare 5 server with IPX and IP running. (or use a Migration Agent)
Pure/IP replica servers with NetWare 4.11 (no replica)	Place master on NetWare 5 server with IPX and IP running. (or use a Migration Agent) There is currently a problem with the processing of backlinks and external references if the master is on a NetWare 4 server.
Variable	
Off-site disaster recovery needed	As outlined above, place replicas locally unless you have a business need to place them remotely. Off-site disaster recovery should be examined closely to see if its benefits outweigh the additional traffic, and inconvenience of possible failed WAN links. In any case, place the off-site replica on a reliable server in a secure, reliable facility.

Partition and Replica Matrix

The following matrix outlines the partitions and replica placement for XYZ Corporation. Include a partition and replica matrix here.

The best method for tracking the storage of partitions and replicas in NDS is the use of a partition and replica matrix. The matrix will also aid in performing NDS health check and redesign operations.

The partition and replica matrix prepared for XYZ Corporation is shown below.

Partition Names	**Server01** (name) ____________	**Server02** (name) ____________	**Server03** (name) ____________	**Server04** (name) ____________
[Root]	M	R/W	R/W	. . .
LOC1	M	R/W	R/W	
LOC2	R/W	M	R/W	
LOC3	R/W	R/W	M	
. . .				

Network Time Management Design (Time Synchronization)

The last step in NDS design NDS is to determine the time synchronization configuration. Time synchronization is the ability of NetWare servers to coordinate and maintain consistent time among all servers in the NDS tree. Time synchronization is necessary to ensure that each NDS event receives an accurate time stamp. Without an accurate time stamp, objects created or changed on one server may not be able to replicate to another file server.

The objective in planning the time synchronization strategy is to determine an efficient time synchronization method (configuration) to use, and then identify the best way to set up and manage that method across the network (communication).

The TIMESYNC.NLM coordinates time stamps between all servers, and maintains each server's Universal Time Coordinated (UTC), also known as Greenwich Mean Time (GMT).

The Network Time Protocol (NTP) is an Internet protocol specification (RFC 1305) that allows different operating systems and platforms, such as Windows NT, Macintosh, UNIX, and NetWare to share time. TIMESYNC.NLM is enhanced to include NTP functions for use on NetWare 5. We have designed the time synchronization strategy for XYZ Corporation using an NTP time source.

Types of Servers

Every NetWare server in an NDS tree must participate in the time synchronization process, regardless of whether it holds an NDS replica or not. There are four time server types:

- Single Reference—time provider
- Reference—time provider
- Primary—time provider
- Secondary—time consumer

Time Configuration

Time Configuration outlines a strategy for time server definitions and placement.

A custom **Time Provider Group** will be used for the XYZ Corporation NDS tree. The custom Time Provider Group will provide XYZ Corporation with greater fault tolerance and accessibility by distributing the time servers to multiple locations.

Time Communication

Time Communication outlines a strategy which identifies how the servers will communicate with each other.

A custom **Configured List** communication strategy will be used for the XYZ Corporation NDS tree. The custom Configured List provides added flexibility and control of time synchronization communications.

XYZ Corporation Time Synchronization Design

Time Configuration = Custom - Time Provider Group

Time Communication = Custom - Configured List (no SAP)

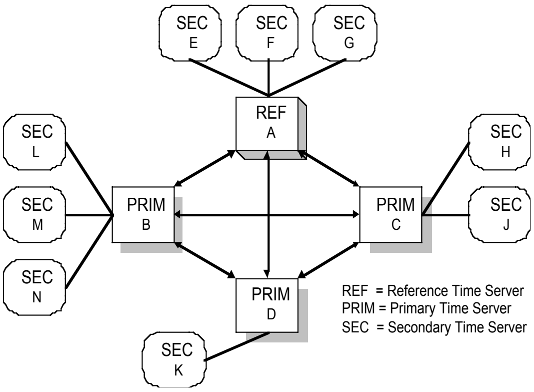
Create one time provider group with four time providers (one Reference server and three primaries). The time providers will be in LOC1 (one Reference and one Primary), LOC2 (one Primary), and LOC3 (one Primary). The Reference server will get its time from an NTP time source.

The time synchronization strategy for XYZ Corporation is shown in the Time Provider Group drawing and matrix below.

If TIMESYNC.CFG lists the time providers in order according to proximity, all remaining file servers will be Secondary servers and will get their time from the physically closest time provider (either the Reference or one of the three primaries).

These time providers vote to determine the appropriate network time with respect to all the different time zones in the network. The Reference server has a weight factor of 16 and the primaries have a weight factor of 1.

This allows better WAN link utilization and decreases the chance of a server being inserted into the corporate production tree by mistake—the new server requires time synchronization (default uses SAP 026B) to install NDS properly and be placed into a container.


SEC E
SEC F
SEC G
REF A
SEC L
SEC H
SEC M
PRIM B
PRIM C
SEC J
SEC N
PRIM D
SEC K
REF = Reference Time Server
PRIM = Primary Time Server
SEC = Secondary Time Server

Time Provider Group Drawing

Time Provider Group Matrix

Time Server Type	Location	Server Name	IP Address	Configured List
Reference	1	RefA	172.31.21.59	18.72.0.3:123;128.115.14.97:123
Secondary	1	SecE	172.31.21.61	172.31.21.59;172.31.21.76
Secondary	1	SecF	172.31.21.63	172.31.21.59;172.31.21.76
Secondary	1	SecG	172.31.21.65	172.31.21.59;172.31.21.76
Primary	1	PriB	172.31.21.76	172.31.21.59;172.27.21.35
Secondary	1	SecL	172.31.21.77	172.31.21.76;172.31.21.59
Secondary	1	SecM	172.31.21.79	172.31.21.76;172.31.21.59
Secondary	1	SecN	172.31.21.81	172.31.21.76;172.31.21.59
Primary	2	PriC	172.27.21.35	172.31.21.59;172.31.21.76
Secondary	2	SecH	172.27.21.37	172.27.21.35;172.31.21.59
Secondary	2	SecJ	172.27.21.39	172.27.21.35;172.31.21.59
Primary	3	PriD	172.26.21.19	172.31.21.59;172.31.21.76
Secondary	3	SecK	172.26.21.20	172.26.21.19;172.31.21.59

Naming Standards

Objects and their names are the foundation of NDS. A consistent naming standard is important for design of an NDS database that is flexible, easy to use, and meets the customers' business needs.

The following existing standards and policies that pertain to the network at XYZ Corporation were reviewed:

NetWare Administrative Policies

- Centralized or decentralized
- Roles and responsibilities
- Server installation
- User ID management

Corporate Network Security Standards

- User ID requirement
- Password requirement

Naming Standards

- User ID
- Printers and Print Queues
- Servers
- Server volumes

A complete NDS Naming Standard specifies name, syntax, standard properties, value formats (telephone numbers, addresses, etc.), and examples for the objects. These fields within the tree can be useful as a, "global directory", and as a single administration mechanism for all applications and platforms.

The following table is an example of an NDS Object Naming Standard

NDS Object	Standard and Syntax	Example(s)
Tree Name	Represents entire corporation; 64 character maximum and can contain underscores and dashes. Company name or abbreviation. XXXX_Tree.	ACME_Tree
Organization	Company or division name or abbreviation. XXXX	ACME
Organizational Unit	Location, division, or department name or abbreviation, depending upon tree layer. XXXX	PRV (geographic location) SVCS (services division) ACCT (accounting department)

NDS Object	Standard and Syntax	Example(s)

File and Print Servers	Unique server name.
	LLLDDDDT##, where:
	LLL = Location
	DDDD = Department
	T = Server type (examples):
	A = application server
	C = communications server
	D = database/SQL server
	E = e-mail server
	F = file server
	M = ManageWise server
	P = print server
	R = RADIUS dial in/out server
	S = SAA server
	T = test server
	X = fax server
	## = Sequential number
		PRVACCTF01

Volumes	Create additional volumes to separate application or data from NetWare Operating System SYS volume. FileServerName_VolumeName	PRVACCTF01_SYS PRVACCTF01_VOL1 PRVACCTF01_APPS
Print Objects	Names should reflect functionality, not location. Department and location information are derived from NDS context. XXXXP## XXXXQ##, where: XXXX = Printer type & model P = Printer Q = Print Queue ## = Sequential number	HP4SIP01 HP4SIQ01 HP2100P33 HP2100Q33

Queue Server	Unique name required to broadcast using SAP.
	LLLDDDDQS##, where:
	LLL = Location
	DDDD = Department
	QS = Queue Server
	## = Sequential number
		PRVISQS19
		CHIACCTQS23

User	First character of first name, plus entire last name. In the case of similar names, a two-digit tiebreaker will be used. **Note:** You might use First init., Middle init. Last name instead. It could make it a little more difficult for a hacker to guess. FLLLLLLLLLLLLLL[##], where F = First character of first name LLLLLLLLLLLLLL = Last name ## = sequential number, if needed	DSMITH03 DSMITH04 CKACHADURIAN

NDS Object	Standard and Syntax	Example(s)
Groups	Function, application, or specific rights assignments common to a group of users in the same physical location. XXXXXXXX	PAYROLL
Organizational Role	Administrative function being performed. XXXXXXXX	ADMINS BACKUP PASSWD

An NDS object property standard should be developed for each object defined in the NDS object naming standard document. The property standard document will promote consistency in the creation of objects in the NDS tree.

For purposes of this document, only the properties which are optional for object creation but required for this standards definition are listed. A thorough property standard would identify each property, and whether the property is required (either by NetWare or as a defined standard), optional, or system (generated upon creation of the object).

The following table is an example of an NDS object property standard for XYZ Corporation:

NDS Object	Property	Standard
Organizational Unit	Description	Provide a description of the location, department, or functional workgroup which is represented by the Organizational Unit.
Servers	Description	Provide a description of the server, including applications or special purposes that the server is performing.
Groups	Description	Provide a description of the group, including its function (rights assignments, drive mapping via login script, etc.)
	Rights to Files and Directories (if applicable)	Assign S, R, W, C, E, M, F, A rights to specific volumes, directories, or files.
Users	Given Name	Common name for user or nickname. Example: Cindi
	Last Name	User’s last name, first character capitalized.
	Full Name	User’s full name, first character capitalized. Example: Cynthia
	Middle Initial (if applicable)	Middle Initial, capitalized.
	Title	Full Title. Example: Vice President of Marketing
	Description	Full Time, Part Time, or Temporary Employee.
	Location	Geographic—Campus or Building. Example: Detroit Office.
	Department	Department or functional workgroup in which the user primarily works.
	Telephone	(801) 555-1212
	Fax	(801) 555-1213

Basic NDS Security Policy

Securing the network encompasses many areas of security including physical access, login, NDS, and file system restrictions.

The following three categories of NetWare security have been reviewed for the NDS tree design at XYZ Corporation:

- Physical Security
- Login Security
- NDS Security

Physical Security

Servers

Keeping the server in a safe place is critical to preventing unauthorized access.

The following steps for controlling physical access to servers and workstations server are recommended for XYZ Corporation:

- Place the server in a restricted access area, such as a data center.
- Personnel authorized to access the servers should be clearly identified. Vendor or contract employees should be accompanied by company personnel.

Secure the server console

- Use the SECURE CONSOLE utility to prevent unauthorized users from loading NLMs outside of the SYS:SYSTEM directory, and from changing the date and time on the server.
- Prevent any unauthorized keyboard entry at the console using the console-locking feature in SCRSAVER.NLM. In order to gain access to the console prompt, the user must authenticate to NDS.
- Encrypt Remote Console (RCONSOLE) passwords to prevent them from being read from an NCF file.

Workstations

This section addresses access to workstations while they are connected to the network. Physically securing stationary workstations to the desktop or worksurface is a good idea, however this practice is usually seen in a lab or training room.

The Security Policy for XYZ Corporation should include the following information for securing workstations:

- Users must log out of the network before leaving their work location for the day, or at the end of a shift.
- Users, especially those with Supervisor rights to the NDS tree, containers, or objects must not leave their workstations unattended while logged in. If a workstation must be left unattended, password-protected screen savers or workstation lock features of the desktop operating system must be used.

Protecting the Data

- Install an integrated, network-wide virus protection system.
- Install auditing tools such as AUDITCON (version 4.3.5 or higher) to track events on highly sensitive servers.
- Implement an SMS-compliant backup system for all servers.
- Periodically restore the data to verify the integrity of the backups and restore procedure.

Login Security

Once physical security has been established, the next step in preventing unauthorized access to network resources is login security. Login security consists of two phases: login and authentication. Additional login security measures, including global and personal login restrictions, complete the login security model.

The following recommendations have been made for XYZ Corporation:

Login/Password Authentication

The login phase, also referred to as the identification phase, occurs when a user establishes their identity with their name (Login Name) and password.

The authentication phase uses encryption to verify that any requests the server receives are from legitimate clients.

- Create a unique Login Name for each user. Do not use Guest or other generic Login Names.
- Always require a password (see additional information in Login Restrictions)

Login Restrictions

The following login restrictions, also referred to as user account restrictions, are optional login security features. We recommend implementing these features as requirements for each user login account at XYZ Corporation:

Restriction	Recommendations
Account Expiration	Specify an expiration date for a user account if the user is a temporary or limited contract employee. Any attempt to log in after the account expires disables the account.
Password restrictions	Require a password. Require unique passwords (for a password to be unique, it must be different from the previous eight passwords used by the account). Allow user to change password Minimum password length (5–8 characters) Force periodic password changes (every 90 days) Establish a limit of 3 grace logins
Network Address Restrictions	Restrict the network locations (workstations) from which users can log in. Implement in high security scenarios such as banking industry, brokerage firms, military installations, etc.
Time Restrictions	Restrict login times according to user need. Enable this for standard weekday working hours for general users. Broaden the time period for network administrators or for other exceptions.
Connection Restrictions (Concurrent Login Sessions)	Limit the number of workstations (connections) from which a user can be logged in at any given time to two
Intruder Detection/Lockout	Restrict the number of incorrect login attempts in a predefined time before the account is locked. Set a limit of three incorrect attempts in a 30 minute period. Remain locked for 15 minutes.

NDS Security

NDS security is composed of object security and file system security. Both file system security and object security use similar systems of trustees, rights, inheritance, IRFs, and effective rights.

File System Security

File system security regulates access to the files and directories in volumes on the network, and controls how users access that information. File system security consists of assigning trustee rights, and file and directory attributes. The following recommendations have been made for XYZ Corporation:

- Avoid individual trustee rights assignments
- File system security is easier to implement and manage when you grant rights to objects, such as container objects, that pass their rights to multiple users. If not everyone in the container should receive the same rights, then create a group within the container, and assign rights to the group.

- Specify a standard file system structure to ease file system administration across the network:

  Consider the number of volumes on each server

  Will volumes be dedicated to a specific function, such as applications, data storage, and so forth?

  What are the users' data storage needs?

  What network drive letters will be standard for applications, email, user directories, and so forth?

  Which directories need to be represented by aliases or directory map objects?

- Plan File System Rights

  Design the overall directory structure top-down, moving from lesser to greater access.

  Avoid granting excessive rights near the top of a file system structure.

  Use inheritance and the IRF to assign rights.

  Supervisor rights in the file system cannot be blocked.

- Make trustee assignments in the following order:

  1. [Public]
  2. Containers (including [Root])
  3. Groups and Organizational Roles
  4. Users

Explicitly assigning security equivalence is not recommended. Since trustee assignments and security equivalence flow down independently, rights granted through security equivalence can remain in effect unless blocked by an IRF. This complicates the calculation of effective rights.

File and Directory Attributes

Attribute security is a subsystem of file system security. Directory and file attributes assign properties to individual directories or files, which control actions that can or cannot be taken on a file or directory. Some attributes apply at the file level only, while others apply to both the directory and the file levels.

- Use with caution—attribute security can override rights granted with trustee assignments, and applies to all users. This will prevent users from completing tasks.
- See the section "Traditional File Services" in the NetWare 5 online documentation for the table listing of attributes, their description, and their application to file, directory, or both.
-

Objects and Properties

Add recommendations from Basic NDS Security document.

NDS Administration

Centralized

Distributed

Summary

Provide a concluding summary of the material covered in this report.

In this consulting engagement, Consultants have explained and conducted the following steps with XYZ Corporation in relation to NDS tree design:

- Gathered and reviewed XYZ Corporation's corporate documents
- Designed the top level of the XYZ Corporation tree
- Designed the bottom level of the Landstar tree
- Considered extenuating factors and adjusted the tree design as necessary

Transition Notes

You have reached this point because the project is moving forward. The customer needs to know what to expect next. Give an idea of what will happen, or need to happen here. Details are provided in the next two subsections.

Direction

Give the customer answers to the questions, “Where do we go next?” or, “What do we do next?”

Timeline

Give the customer a sequence of events, or sequence of steps to follow next. Specific dates should be worked out with the customer and presented here.

Appendix A:

Present supplemental material here. Use as many appendices as needed, separating the information into logical groupings. Each appendix should be separated by a page break.

This section includes Novell technical information documents (TIDs), Novell AppNotes, Novell web site documentation, etc. More information on TIDS is located at -

http://developer.novell.com/support/