C.N.A. 5 (50-639)

Network Definition

A group of computers that communicate and share resources.
Hardware that consists of servers, workstations, networks boards, communication media (i.e., cable) and peripheral devices (i.e., printers).

Minimum Hardware Requirements for Netware 5 server

Pentium processor
64MB RAM
35MB DOS partition
600MB SYS partition
VGA Video adapter and display
CD-Rom
Network Board

Network Resources and Network Services

A **resource** is something you use, such as a printer.

A **service** is the system or method of accessing the resource (how to get your job from your workstation to a network printer).

The services that are provided by NetWare are:

Novell Directory Services (NDS) This is the brain of the network. It is a database that contains all resources set up in the network (user accounts, printers, servers, etc.).

Security There are different levels of security that can be applied on the network. Login security; file system security; NDS security; physical security.

File System The file system can be implemented for data to be stored on a server instead of the local hard drive of a workstation.

Network Printing Printers can be attached to the network and shared to users who are connected to the network.

Application Access Applications can be installed on a server and shared out to user accounts or downloaded and installed on their workstations using Application Launcher.

ZenWorks Starter Pack. ZenWorks is a product that can be installed to import workstations in to the NDS and to manage and maintain network applications.

Storage Management Services (SMS) This is Novell's terminology for backup. Most installations will purchase third party software to backup and recover the file system and NDS.

Login

Gaining access to the network resources and services is done through the login process. It is mandatory and a security issue. A valid user account is required. A password is optional.

Once the Client software is installed on a workstation, the options to gain access to the login are:

The Novell Client login window, which appears after the workstation, boots up
Choose Start | Programs | Novell | NetWare Login
Right click the red 'N' in the system tray and select NetWare Login
Run C:\Novell\Client32\LoginW95.exe (95/98)
Run WINNT\System32\LoginWNT.exe (NT/2000)

Login Sequence:

Prompts/Validates Username --->Result: Denied or
Checks Account Restrictions --->Result: Denied or
Prompts for Password --->Result: Denied and Intruder Detection Notified (if enabled) or
Access granted.

Context

Context describes what part of the tree an object resides in.

Two types of context available: Current context
Name context

Context versus Current Context

Context is the container where the object has been created.
Current Context is the location where you are 'currently' sitting in the tree.
In a comparison to the file system, a file is created in a directory – which would be the file's context. You could be pointing to a directory somewhere else in the file system or right at the root of the volume – which would be the current context.
Name context - Defines where an object resides in the tree.

Naming Conventions

There are two naming conventions for NDS: Distinguished Name
Relative Distinguished Name

Distinguished Name

A Distinguished Name is the fully qualified name of an object in the NDS.
Put another way, it is the full path of where the object resides starting from the object and walking up the tree to (not including) [Root].

When sending this information to NDS, you identify that it is the full path by starting the name with a period.

Example: *.ADMIN.CORP.NYC.EMA. or*
.CN=ADMIN.OU=CORP.OU=NYC.O=EMA

NDS identifies the leading period and will not do any further name resolution.

Relative Distinguished Name

A Relative Distinguished Name is relative to where your current context is or where you are currently sitting in the tree.

The difference to NDS is that you do not start the relative name with a leading period. NDS takes the information provided and adds on the current context to build a distinguished name. NDS only uses distinguished names.

Example: If your current context is .CORP.NYC.EMA, you would use ADMIN. NDS identifies that there is no leading period, takes ADMIN + .CORP.NYC.EMA to build a distinguished name of .ADMIN.CORP.NYC.EMA

If your current context was higher, then you would provide more information to walk up to the current context.

Trailing periods can be used with Relative names. It works like the CD.. command in DOS. Each trailing period is the equivalent of moving up one level in the tree or removing an item from left side of the current context.

Example: *ADMIN or CN=ADMIN*

Typeful versus Typeless

The NDS design was based on the X500 International standard. With that come attributes that can be used to fully qualify the object type. Using the attribute is typeful, no attribute is typeless.

Attributes

C- Country container.
O- Organization container.
OU- Organizational unit container.
CN- Common Name of the leaf object.

These can be used with Distinguished or Relative Distinguished names.

Examples

Typefull distinguished name :	.CN=Admin.OU=Corp.OU=NYC.O=EMA
Typeless distinguished name:	.Admin.Corp.NYC.EMA

Novell Directory Services (NDS)

* The NDS is a hierarchical database. It resides on a server on the SYS volume. It contains objects that represent the resources that are on the network (users, printers, servers).

* All network requests go through the NDS.

* When you login to the network – you login once through a process called authentication. Once successfully logged in you have access to

any NDS resource or file system where you have been granted rights or privileges.

- The NDS is composed of 3 components: Objects; Properties; Values
- An object represents a resource (user, printer, server, group, etc.).
- Each object has properties. These are fields of information about the object.
- The entry to the property is called the value.
- An example is a user. A user is an object created in the NDS. A user object has properties such as title, first name, telephone number. The entry against that property, such as, Manager, Bob, 234-0987 are the values.
- The NDS is hierarchical, or a tree design. Think of the file system on your hard drive.
- C: is the top of the file system, also known at the root. Under the root of C: you can create directories, under those directories you can create sub-directories and decide where the individual files are placed.
- The NDS structure is similar.
- [ROOT]
- At the top of the tree is [ROOT], always referenced with the square brackets. You can have only one [Root] per tree. It is a placeholder and the only object that does not have properties or values.

NDS Container Objects

[ROOT]

At the top of the tree is [ROOT], always referenced with the square brackets. You can have only one [Root] per tree. It is a placeholder and the only object that does not have properties or values. The [ROOT] cannot be deleted or renamed. And only and alias that points to an organization can exist under the [ROOT].

Country container

A Country container can only exist directly below the [Root]. It must be a valid X500 country code. (UK for United Kingdom, US for United States). It is optional. It is also limiting in that it can only have an *Organization* container or *Alias leaf object* under it. You could not place user accounts, servers or any other leaf objects under a Country container. You can have multiple Country containers, but all must be under [Root].

Organization container

An Organization container is created under [Root] or if there is a Country container it would be created under it. An Organizational Unit container or any leaf object can be created under an Organization container. At least *one* Organization container is required. It is usually named after the Company.

Organizational Unit container

An Organizational Unit container can be created under an Organization or an Organizational Unit container. It can contain all leaf objects. It is an optional container.

Alias

Logical NDS pointer. Can only point to *a Country, Organization or Organization Unit object* when used as a Container object.

NDS Leaf Objects

A Leaf object represents a resource such as a user, printer, server, or group. It is the end-most object like a file in the file system. You cannot create a file under a file and you cannot create anything under a leaf. Leaf objects (other than an Alias) can be created under an Organization or Organizational Unit container. And you can have to leaf object with the same name , but they'll have to be under a different context. The following lists commonly used leaf objects :

User

Represents an individual who will access the network.

Alias

Logical NDS pointer. Used as a shortcut to point to a leaf object in another container.

Template

Template used to create users with predefined settings.

Organizational Role

Defines a position in organization. Used to assign privileges to individuals in a certain position.

Profile

Contains login script commands that can be applied to users.

Directory Map

Represents a logical pointer to a directory in the server file system. Used to centrally manage drive mappings.

Application

Provides ability to manage applications as NDS objects.

NDPS Printing

Novell Distributed Print Services manages printing in the Netware 5 environment. Downloads necessary drivers to the workstation. Supports TCP/IP.

Printer Agent:

A Printer Agent is created for each printer. A Printer Agent can be a software entity running on a server representing a local, remote, or network-attached printer, or a Printer Agent can be a software entity embedded within a network-attached printer.

NDPS Manager

An NDPS Manager is an object created in the NDS and can support unlimited number of printer agents. (A printer agent represents a printer.). Multiple NDPS Managers can be created in NDS, but only one NDPS Manager can be loaded and running on a server at a time. The NDPS Manager would support all printer agents assigned to it. If you have multiple servers, you can run multiple NDPS Managers, one per server.

NDPS Gateway:

- A gateway translates NDPS queries to printer specific language. Third-party gateways provide bi-directional feedback and control between the client and the physical printer.
- Sent jobs to printers that are not NDPS aware
- Sent jobs to printing systems that requier queues

NDPS Broker:

An NDPS Broker is an object created in the NDS when the NDPS product is installed on a server and when no other broker exists within three hops of another server. It will be created in the same container as the server and will reside on that server. It maintains three services:

<u>SRS</u> - Service Registry Services - registers information of Public Access Printers.
<u>ENS</u> -Event Notification Services - configurations for print job and printer notification. Notification can be configured for email, pop-up menus, and creation of log-files.
<u>RMS</u> - Resource Management Services – A database of printer drivers, banners, printer definitions and fonts.

Printer Types

<u>Public:</u>

The Public Access printer is created through the NDPS Manager. It does not have an object in the NDS; therefore little security can be place on it. It is available to everyone logged in to the network. The information configured for this printer is stored in the Service Registry Services of the NDPS Broker object.

<u>Controlled Access:</u>

A Controlled Access Printer gives you control of the printer. It is configured by creating an object in NDS. You can specify who can print to it, who has control of the jobs and who can configure access to print queues. When creating the NDPS Printer object you specify the NDPS Manager who supports it. You have tree levels of administring : User – Operator – Manager.

- It offers simple or automatic installation
- Reduces administration costs
- Reduces Networking problems
- Improves networking performance
- It offers a full range of event and status notification options

Novell PrintManager

SYS:Public\Win32\NWPMW32.exe

The Novell Printer Manager allows you to:

- Manually configure printers on a workstation
- Maintain and update the printer list
- View a list of all print jobs
- Receive information and event notification for jobs and printers
- Change job order

Managing the file system

Utilities

NetWare Administrator

- A GUI application used to manage the NDS and file system.
- Help is available by pressing F1 or by choosing the help menu option.
- You can create an object by :
  1. Using the toolbar
  2. Rightclicking on a container
  3. Using the object menu

FILER

A DOS-based utility used to manage files/directories, display volume information, salvage and purge files.

CONSOLE1

Java based management utility (requires Java Runtime Environment). Can be used to create User, Group, Organization, and Organizational Unit objects.

Commands

Path = servername_SYS:PUBLIC\MGMT\CONSOLE1.EXE

FLAG - Changes file/directory attributes.

NDIR - Used to view files, directories and volumes.

NDIR /S	-	See subdirectories
NDIR /L	-	See if longfiles are supported
NDIR /DO	-	Directories only
NDIR AC	-	Accessed
NDIR /FO	-	Files only
NDIR /MAC	-	See if macintosh machines are supported

NCOPY - Copies directory structure, and files (including Netware attributes).

RENDIR - Renames a directory.

UIMPORT - Used to import users from a database to NDS. (Delimited ASCII file) Sample syntax: UIMPORT LIST.CTL LIST.DAT

Salvaging Deleted Files

Files can be recovered through the Salvage utility in Filer, NetWare Administrator and Explorer. Files cannot be recovered when:

- disk space begins to run out. The oldest erased file will be written over first.
- a file is purged – with the purge attribute, it cannot be recovered.
- DELETED.SAV

* Is a system created directory to recover deleted files when its directory has been deleted.

Managing Volume Space Usage

There are two ways to restrict user accounts on how much data they can store on the network:

* by the total amount of data in a directory;
* by the total amount of data on an entire volume.

If you restrict the amount of data that can be placed in a directory –the limit is set at the directory and will include all data and sub-directories created within it, regardless of who places data in it.

If you restrict by volume, you are charging a user account by the amount of the size of each file that the user creates (the owner property), regardless of where that file is stored on the volume. This restriction is placed on the volume specifying the user account.

Compression

Netware compression is analogous to ZIP file compression. It is enabled on every volume by default and can save an average of 63% of disk space. Attributes to override compression settings are:

DC – Don't compress
IC – Immediate compress

Block Sub-allocation

Block Sub-allocation optimizes disk space by taking the last piece of the file that does not require a full block and writing it to an unused portion of another block.

Migration

Migration is where you can purchase a device known as a jukebox. This is a readable/writeable optical device that can be configured through Novell's High Capacity Storage System or through third party software that allows you 'migrate' data off a volume to this jukebox which is 'nearline' storage instead of 'offline' storage (back-up tape). It looks to the user like the data is still on the volume. The attribute to keep files from being migrated is DM – Don't Migrate.

MAP command options

MAP
Displays a list of current drive mappings.

MAP X:=SERVER1\SYS:
Maps the X drive to the SYS volume on SERVER1.

MAP N SERVER1\SYS:
Maps the next available drive to the SYS volume on SERVER1.

MAP DEL X:
Deletes the drive mapping to X:

MAP S2:=SYS:SYSTEM
Makes the SYS:SYSTEM directory the second search drive.

MAP C S2:
Changes S2: from a search drive to a network drive.

Netware 5 File System

The file system organizes internal disks into one or more volumes.
To rename a physical volume, change its name at the server with NWCONFIG.
To rename a logical volume in the NDS, use NetWare Administrator.
NetWare default directory structure:

SYS
Contains OS files, NLMs and NDS programs. Should be reserved for NetWare.

PUBLIC
Contains user utilities and commands.

NLS
Contains message and help files for multi-lingual support.

ETC
Sample files to configure TCP/IP.

DELETED.SAV
Contains recoverable files that have been deleted and the directory that they resided in was also deleted.

SYSTEM
Contains Netware operating system files.

MAIL
If the server was upgraded from a previous version, contains user login scripts and print job configuration files.

NDS and File System Rights

The following concepts apply to both NDS security and the file system security.

Trustees

A Trustee is used for assigning rights to a specific object, directory or file. The Trustee is the 'who' that is added to the Access Control List (ACL) of the object, directory or file and the 'what' are the rights assigned to the Trustee. The objects that can be used for assigning rights are Users, Groups, Organizational Roles, Containers, [Root] and [Public]. Accounts who belongs to any of these will receive the rights assigned at that level and carry them from that point down in either the file system or NDS. This is known as Inheritance.

Inheritance

When rights are granted to a directory in the file system or a container in the NDS the rights from that point will flow down to all files and sub-directories or all containers and leaf objects below. This is called Inheritance.

There are two ways to stop the flow of inheritance.

- Make a new assignment to the object that was granted the rights from above. This new assignment will over-write the old assignment. This can grant more or less rights. If you want the rights to be maintained from the assignment above, you must grant them those rights in the new assignment.
- The second way is to place an Inheritance Rights Filter (IRF). Think of the filter sitting on top of the object, directory or file – filtering out rights flowing in to it. This filter affects everyone who may have rights – it cannot be selective as to who you filter rights from.

An exception here is within the file system. If you grant the supervisor right in the file system, it cannot be taken away at a lower level with either a new assignment or a filter. This does not apply in the NDS.

Effective Rights

The rights can be coming from other objects that the user belongs to where additional rights have been assigned. An individual assignment will only overwrite a previous individual assignment. If this user belongs to groups, organizational roles, containers or has been granted security equivalence where any of these have been granted additional rights, they are additive.

This is called Effective Rights. Check the 'Effective Rights' to see the total sum of rights the user has and then check the user's 'Security Equal To' page as to where rights may come from.

Security Equivalence

- Users can also be made security equal to another user. They will obtain any additional rights that users may have. It should be used as a temporary assignment – if a user needs the rights on a permanent basis, make a trustee assignment. Security equivalence is set at the user object.

[ROOT] versus [PUBLIC]

*	[ROOT] is represented as an object at the top of the NDS tree. The [PUBLIC] trustee does not have an NDS object and is only available as a trustee assignment. [PUBLIC] has the same position in the tree as [ROOT]. Every object is a member of both [ROOT] and [PUBLIC]. The difference is that rights assigned to [ROOT] can be received once you are authenticated (logged in). [PUBLIC] means you are 'connected' to, but not logged in to the network.

NDS Security

NDS versus File Rights

*	Rights never flow from the file system into the NDS. Rights will flow from the NDS in to the file system when someone has the Supervisor object right to the Server object. They will have all file rights including Supervisor to all volumes that belong to that server. Also, if they obtain the Write property right to the Object Trustee (ACL) property of the server object, they will also receive all rights including supervisor to all volumes on that server. The Supervisor right in the NDS can be removed with an IRF (Inheritable Rights Filter) and can be removed at a lower level with a new trustee assignment.

Default NDS Rights

*	Users will receive the Browse object right to all objects in the Tree from the trustee assignment of [Public] to [Root]. Users also receive the Read Property right to All Properties of their user account. This means they can Read any setting made to any property of themselves. They also receive Selected Property assignments of Read and Write to the Login Script and Printer Configuration properties. [ROOT] is made a trustee of a user and granted Read to Group Membership and Network address selected properties. [Public] is made a trustee of a user and granted Read to the Default Server selected property.

*	NDS has two sets of rights. Rights against the object itself, and rights to what you can do the values of the properties that belong to that object.

OBJECT RIGHTS

Supervisor

The Supervisor object right implies all object rights. By granting the Supervisor Object right also implies granting the Supervisor right to All Properties.

Browse

Allows you to see objects in the NDS.

Create

Allows you to create an other object. You will only see Create on a container, not on a leaf object.

Delete
Allows you to delete an object.

Rename
Allows you to change the name of the object.

Inheritable
Allows you to decide whether the assignment will flow from the container down. You will not see the inheritable option on a leaf object.

PROPERTY RIGHTS

Supervisor - The Supervisor Property right implies all other property rights.

Compare - Compare allows a comparison to be run against the value and receive a True or False response. If you have the Read right, Compare is implied.

Read - Allows you to see the value**.**

Write - Allows changes to be made to the value. If you have the Write property right to the 'Object Trustees (ACL)' property of any object, this will allow you to make a trustee assignment to anyone and grant all rights including Supervisor.

Add/Remove Self - Allows you to add or remove yourself as a value of the property, but you cannot change any other value of the property. If you have the Write right, Add/Remove Self is implied.

Inheritable - Allows you to decide whether the assignment will flow from the container down. You will not see inheritable on a leaf object.

All Properties versus Selected Properties

* An assignment of rights to All Properties will grant those rights to every property of that object. An assignment to Selected Properties will grant rights only to the properties selected where more or less rights were granted. An assignment to a selected property will overwrite rights granted to All Properties for that particular property.

* In NetWare 5 at a container's Selected Properties – all properties of all objects, container and leaf, are available for selection. Therefore if an assignment is made to a selected property at a container that applies to a leaf or container object and the inheritable right is checked, that assignment will inherit to any object that has that property.

* Selected Properties overwrite All Properties - both can be inherited.

* To use a Directory Map object, a trustee assignment is required with a minimum of Read to the Path property.

* To use a Profile object, a trustee assignment is required with a minimum of Read to the Login Script property.

Managing File System Security

Directory & File Rights

Supervisor – Implies all rights.
Read – Read the contents of an existing file and launch executables.
Write – Grants rights to open and change contents of existing files.
Create – Create new files and directories.
Erase – Erase existing files and directories.
Modify – Set attributes and change the name of files and directories.
File Scan – See files and directories. but unable to open/copy.
Access Control - Set Inheritance Rights Filters and make trustee assignments
– granting all rights except Supervisor.

Default Rights

- When a user account and home directory are created at the same time, the user is made a trustee of the directory and granted all rights except Supervisor.
- The container where the SYS volume resides is made a trustee of the SYS:Public directory and granted Read and File Scan.

Attributes

Attributes can be described as another level of security for files and directories. They can potentially overwrite the ability to perform an action that the rights allow you to do without them. If you have applied a read-only attribute on a file, you cannot erase it even though you have the erase right. The Modify right allows you to change the attribute to a read-write and then you could erase it. Utilities to set attributes are:

NetWare Administrator; Filer; Flag

Other issues concerning security

- Rights from NDS do not transfer into the file-system, except for Supervisor rights to a server object.

- The creator is made an owner of a file or directory he or she creates. The container that contains the SYS volume is always given RF access to SYS:PUBLIC. All other containers must recieve rights through a trustee assignment.
- A user is granted RWCEMFA access to his or her home directory when the user account and home directory are created at the same time.
- In NetWare Administrator:
  The 'Rights to Files and Directories' page is used to assign rights from a user's aspect.
  The 'Trustees of this Directory' page is used to assign rights from a directory's aspect.

IRF (Inherited Rights Filter):
When the filter is applied, the rights that are not checked are the rights allowed to pass through.
If Joe has RF rights, and goes through an IRF with only F specified (not checked), Joe keeps only F rights.

Security equivalence:
Means that one object's access rights are specified to be equivalent of another object's access rights.

Ancestral Inheritance:
By default, any object is security equivalent to its parent container.

Server Security
Implement the following steps to ensure file server security:
1) Restrict physical access to the file server.
2) Lock the file server console using SCRSAVER.NLM.
3) Load SECURE CONSOLE to allow NLMs to only be loaded from the SYS:SYSTEM directory.

Login Scripts

There are four login scripts and they execute in the following order:
Container Login Script
Profile Login Script
User Login Script
Default Login Script

Container Login Script
The commands written in a container login script will execute for the users logging in that belong to that container.

Profile Login Script
A profile is an NDS object which contains login script commands written as values to the login script property. The profile must be assigned to the user (one profile per user) and the user must have rights to the profile.

User Login Script
A user login script can be written for an individual at the login script property of that user.

Default Login Script
The default login script will only run if there is no user login script. It has essential commands such as a mapping to the SYS:Public directory. It cannot be edited. It is hardcoded in the LOGIN.EXE that is found in SYS:Public and SYS:Login directories.

Commands and Identifiers

Login scripts have two components: commands and identifier variables.

Commands

MAP Creates drive letters to point to directories in the file system.

REM REMARK * ; Commenting out a line – the login script ignores anything after a remark.

Example : REM MAP F:=SYS:PUBLIC

NO_DEFAULT Turns off the execution of the Default login script.

or @ Runs an external command from the login script. # means go execute the command and stops. @ means go execute the command and the login script keeps processing.

Example : #CAPTURE P=HPLJColor5

FDISPLAY Displays the contents of a text file. 'F' is for filtering reveal codes from the word processor.

INCLUDE Calls in and executes additional login script commands in either a text file or another login script.

WRITE Writes the line to the screen. Double quotes encapsulate the line.

Identifier Variables

Identifier variables allow you to enter a variable (such as LAST_NAME) rather than a specific name (such as Jones) in a login script command. When the login script executes, it substitutes real values for the identifier variables. Variables must be typed in upper case (capitals). When using identifier variables with the WRITE statement or MAP commands they need to be preceded with a %.

Sample Syntax: WRITE "Good %GREETING_TIME,%LOGIN_NAME"

Zenworks

Design Guidelines

- Create groups in the same container as the associated application.
- Limit a group to 1,500 members.
- Never span group members in containers over WAN links.
- Keep groups and users in the same partition.
- Do not place users in more than 64 groups.

Installation of ZENworks Starter Pack

Requirements:

- Server: 175MB free disk space 7MB free of 128MB RAM (NetWare 5)

- Workstation: 5MB disk space Pentium with 16MB RAM
- Supervisor right to [Root]

Workstation Manager

The workstation manager component is installed on servers and workstations with the installation of ZENworks (server) and the Novell Client (workstation). This allows you to configure Microsoft policies through NetWare Administrator (NWAdmin32). It is made up of modules on the workstation and provides a NetWare Administrator snap-in.

Registering Workstations

A workstation must first be registered before it can be imported into the NDS. This is done through the workstation registration program.

There are three methods available for Workstation Registration:

- Application Launcher – ZenWorks automatically creates two application objects pointing to WSREG32.EXE and WSREG16.EXE.
- Scheduler – A Scheduler program is available from the Novell Client (WSREG32.EXE) and runs each time a user logs in. An icon is placed in the System Tray.
- Login Script – The WSREG32.EXE and WSREG16.EXE can be placed in a login script as commands to run at each login.

Log File

A registration log file is created on the workstation: C:\WSREG32.LOG

Importing Workstations

- Registered workstations have to imported into the NDS to become workstation objects.
- A User Policy Package is required where the Workstation Import Policy has been enabled and associated with a container.
- Workstations can be manually imported through Tools in NetWare Administrator

Policy Packages

There are three types of policy package objects that can be created:

- Container
- User
- Workstation

The User and Workstation packages are platform specific (they must match the operating system they will be used on – Windows 3.1, 95/98, NT/2000)

Container Package

- Can only be associated with a container.
- Contains a search policy to determine how far up the tree to search for policies. (Default is up to [Root])

User Policy Package

- A user policy allows you to define ‘rules’ against a user account regardless of which workstation they log in to.

Workstation Policy Package

- A workstation policy package is applied to a workstation object that has been imported into the NDS, regardless of who logs in at the workstation.

- Some policies, such as Remote Management, appear in both the workstation and user policies. These can be configured to be applied to either the workstation or the user.

- When a User authenticates to the network, the Workstation Manager checks for any policies assigned to the User and checks for policies assigned to any groups the user belongs to.

Associating Objects with Policy Packages

- An enabled policy in a policy package is not effective unless the policy package is associated with an object. You can associate policy packages with Users, Groups, Workstations, Workstation Groups, or containers, depending on the type of policy package.
- Just like assigning different rights for different users in NDS, you can set a general policy for most users, and a unique policy for a unique user. Unless otherwise specified in a Search policy, when the system starts searching for the associated policy packages for an object, it starts at the object and works its way up the tree. Any enabled policy in a policy package associated directly with an object (user or workstation) takes control, even if a contradicting policy in a policy package is higher in the tree (group or container).
- If the user has both workstation and user policy packages associated with it, the user policy packages apply first. Within the user policy packages, individual policies are applied based on the following criteria:

Search Order

Policies are applied in this default search order:

- User policy packages (Policy packages associated directly with the user)
- Group policy packages
- Container policy packages

Enabling a search policy and configuring that policy can change this search order.

Effective Policies

- Effective policies are the total sum of all enabled policies in all policy packages associated directly or indirectly to an object. Just as the effective rights in NDS flow down the tree, policy package associations flow down the tree, unless there is an explicit association for an object with a policy package.
- When the system calculates the effective policies for an object, it starts with all policy packages assigned to that object. It then looks up the tree (assuming that the search order starts at the leaf objects and goes up towards the root of the tree) for associations made to parent containers. The first enabled policy it finds is the one it uses, just as the system looks up the tree for effective rights.

Policy Associations and Inheritance

- You can associate policies to the object itself (User or Workstation), to the group the object is a member of (Group or Workstation Group), or to any container specified in the distinguished name of the object up to the root of the tree. A policy associated to an object takes precedence over a policy associated to a group, which takes precedence over a policy associated to a container. This is according to the default search policy.
- For example, suppose the Remote Management policy is not enabled in a User Policy Package associated with the User object. However, the Remote Management policy is enabled in the User Policy Package associated with the container where User objects reside. The result is that the enabled Remote Management policy is the effective policy for the user.
- ZENworks looks up the tree for effective policies (assuming that the search order starts at the leaf objects and goes up towards the root of the tree). The first enabled policy it finds wins.

Cumulative Policies

These policies allow multiple policy packages to be in effect from different associated policies. The cumulative policies include:

- Enabled User/Computer System Policies
- Enabled User/Computer Extensible Policies
- Scheduled Action Policies

Application Launcher

The Application Launcher component of ZENworks allows you to create objects to distribute applications.

Benefits

Single point of application administration

- Location Independent (your applications goes with you)
- Push and Pull software distribution to workstations
  Push = automatic install or forced run
  Pull = user initiated

- Application Fault Tolerance and Load Balancing – it can be configured such that users have access to applications on multiple servers in case one becomes unavailable
- File Rights Assignment through the Application object
- Roaming Profile support

Application Launcher Components

Administrator Components

- Application Launcher snap-in for NetWare Administrator
- SnAppShot

User Components

- Application Launcher window
- SYS:\PUBLIC\NAL.EXE
- Application Explorer
- SYS:\PUBLIC\NALEXPLD.EXE

Application Explorer can only be run on Windows 95/98, NT/2000.
The icons can be placed in the:

- Application Explorer Window
- Windows Explorer
- Start Menu
- System Tray
- Desktop

Shortcuts on the Desktop have a red arrow.

Simple versus Complex Applications

Simple

A simple application points to the executable and is run from the server. A simple application is created with an Application object in the NDS pointing to the executable and associating who can use it. There are additional configurations that can be applied that define how the object will be used.

Complex

A complex application contains the application itself plus configurations such as registry settings. This is done by creating an NDS object after using the snAppShot utility.

snAppShot Utility

An Application Object template (AOT) is created with a utility called snAppShot (Snapshot.exe). It takes a snapshot (the before picture) of the workstation operating system including registry settings. Once complete, it pauses so you can install the application. Once the installation is complete, you take the ‘after’ snapshot. Once complete, it takes the difference between the before and after picture and bundles the difference in the AOT. It also creates an AXT file – Application Object Text Template. The AOT is in binary format and cannot be edited. The AXT can be edited. This AOT can be configured in an Application object and rolled out to workstations where the application will be installed. It also has a verification process so that if a file associated with the application becomes deleted or corrupt it will re-install the AOT files.

Configuring Application Objects

Environment Page

Allows you to:

- Set the working directory
- Define how the application will be run (minimized, hidden, maximized)
- Provide 16-bit Windows-On-Windows support
- Clean up resources such as mapped drives or other connections
- Use a wrapper executable to launch the appropriate operating system file.

System Requirements

You can specify the requirements needed for the application to run or be installed such as:

- The specific version of the operating system (98, NT)
- Processor (486, Pentium II)
- The amount of RAM
- The amount of free disk space

Distribution Schedules and Availability

You can schedule when applications are delivered or available.

Load Balancing and Fault Tolerance

Load balancing allows you to have copies of the same application on multiple servers to balance access to the applications. Fault tolerance allows you to set up primary and alternate sources of application access in case of failure of the primary server.

Client 32

- Supports both TCP/IP (Required for Internet) and IPX (Required for older Novell Networks) Protocols.

- Requires ODI (Legacy Dos/Win 3.x), or NDIS (Win95, NT) capability.
- Benefits are :
  - Fewer Harware components
  - Multiple protocols on the same cable.
  - Flexible Configurations