OCTOBER 1993

NOVELL® RESEARCH

NetWare 3.12 Enhancements

Jennifer Heldenbrand
EPD Manager
Novell Education Department

Larry E. Morris
Senior Editor
Systems Research Department

As an update and enhancement release of NetWare 3.11, NetWare 3.12 includes the latest LAN drivers, disk drivers, and administrative utilities. It also includes a number of key enhancements, such as CD-ROM support, Packet Burst and LIP support, NCP Packet Signature, and the new VLM DOS client architecture. While NetWare 3.12 supports several new NLMs, it also supports all NLMs that use APIs published for NetWare 3.11. This AppNote discusses these enhancements and gives some implementation guidelines for NetWare 3.12.

Contents

Acknowledgements

Special thanks to Kelley Lindberg, Kirk Matheson, Gordon Smith, and Joe Smith for their help with this AppNote.

Much of this AppNote is taken from the NetWare 3.11 to 3.12 Update Seminar, the student manual for Novell Education Course 507. The half-day seminar covers all of the material in this AppNote as well as such topics as new console commands, utility changes, NetWare 3.12 server and client installation and upgrade, Novell ElectroText, and Storage Management Services. This seminar is offered at Novell Authorized Education Centers. Call 800-233-3382 for more information.

Introduction

NetWare 3.12 is an update release to the successful NetWare 3.1x line. It incorporates all fixes and

patches that have been distributed for 3.11 since its introduction. NetWare 3.12 also includes new features that improve performance, increase security, and add functionality.

Key enhancements to NetWare 3.12 include the following:

- A simplified install procedure and an improved menu system
- Bundling of 5-user NetWare for Macintosh, MHS basic services, and First Mail E-mail with the OS
- New VLM (Virtual Loadable Module) client architecture
- New client tools to better support MS-Windows
- Support for CD-ROM installation
- Support for CD-ROM read-only volumes
- Updated LAN drivers, disk drivers, and utilities
- Support for Packet Burst and Large Internet Packet Exchange
- Standard Ethernet 802.2 frame support
- File system, memory, and routing enhancements
- More efficient RIP and SAP code

NetWare 3.12 is compatible with NetWare 4.01 in that 4.01 provides bindery emulation, which allows most 3.x services to interoperate seamlessly. NetWare 3.x volumes can be defined and administered within the context of NetWare 4.01 Directory Services. In addition, NetWare 3.x users can submit jobs to print queues located on a NetWare 4.01 server.

Regardless of which NetWare operating system you currently have licensed, an upgrade path is available to take you to almost any user configuration of NetWare 3.12 or 4.01. In addition, customers can purchase NetWare 3.12 now and upgrade to 4.01 in the future.

In many respects, NetWare 3.11 and 3.12 represent similar environments. The learning curve is virtually flat for users who know NetWare 3.11.

NLMs that use Novell's CLIB interface to the operating system will run unmodified on NetWare 3.12. The only exception might be if the NLM is performing some specific version checking for NetWare 3.11. The NetWare 3.12 Sales Guide includes a list of NetWare 3.12-compatible NLMs.

NetWare 3.12 supports the following client types:

- DOS (MS-DOS, Novell DOS, and MS-Windows)
- OS/2 2.0 and 2.1
- Macintosh
- UNIX (optional)

Support is also planned for Microsoft Windows NT as a NetWare client.

NetWare 3.12 Requirements

Recommended product requirements are as follows:

- A PC (or PC compatible) machine with an 80386, 80486 (SX or DX), or Pentium processor

- A minimum of 6 MB of RAM
- A hard disk with sufficient storage for the size of a network. A minimum of 15 MB is required for NetWare's system related files.
- An additional 25 MB of disk space if you plan to install NetWare 3.12 electronic online documentation on the server.
- One network interface card. Additional cards may be required if you are installing the server as a router between networks or network segments.
- Network cabling (Ethernet, 10Base-T, Token-Ring, Arcnet, etc.)
- A compatible CD-ROM reader if you are installing from CD-ROM or if CD-ROM read-only volumes are to be attached to the server. Electronic text located on the CD-ROM is also accessible as a read-only volume.
- LAN and disk drivers for devices not supported by drivers included with NetWare 3.12. (The NetWare 3.12 Sales Guide lists device drivers included with NetWare 3.12.)

Summary of Update Features

As an updated release to NetWare 3.11, 3.12 provides the following features:

- Bundling of all patches and fixes created for NetWare 3.11. This means that resellers no longer have to download these various patches from NetWire and apply them during installation.
- Updated Novell and third-party LAN drivers and disk drivers. All LAN drivers and disk drivers previously provided in NetWare 3.11 or on NetWire have been updated to their most current version to simplify the installation process. NetWare 3.12 supports all LAN, disk, and back-up devices currently supported in NetWare 3.11 and 2.2, including the new Rev. E type LAN drivers.
- Updated print and management utilities. The latest versions of print and management utilities have been included with NetWare 3.12.
- Updated services such as TCP/IP, Btrieve, and NMA for NetView. A number of improvements have been made to these bundled services, and NetWare 3.12 constitutes a complete refresh of these services.
- Current NETX/ODI shell. In addition to the new VLM/ODI client architecture, NetWare 3.12 also includes the latest version of the NETX/ODI client shell. Provided for backward compatibility, NETX provides support for applications that may not have been tested for compatibility with the new VLM client architecture.
- Current OS/2 client requester for OS/2 2.1. IBM's recently released OS/2 2.1 is now fully supported as a client operating system in NetWare 3.12.

Summary of Enhancement Features

NetWare 3.12 includes the following enhancements, each of which is discussed in detail later in this AppNote:

- Packet Burst support. Using the Packet Burst sliding window architecture, NetWare servers and clients can send and receive multiple packets at one time, without acknowledging each packet individually.
- Large Internet Packet (LIP). When transmitting across multiple segment hops, NetWare 3.12 negotiates the largest size packet that can be accommodated by any router along the route.

- Support for standard 802.2 Ethernet frame types. NetWare 3.12 sets the default Ethernet frame type to 802.2 on both the client and the server.
- NCP packet signature. NCP packet signature provides the option for network administrators to further restrict trusted client sessions by signing each packet received and sent on the wire.
- Routing enhancements. NetWare 3.12 operating system code has been enhanced to provide improved handling of routing information.
- Memory pool enhancement. The default value and the range of values available for the Alloc Short Term Memory pool have been increased.
- File system enhancements. The file system in NetWare 3.12 has been enhanced by cache read ahead, enhanced extended attribute support for OS/2 2.1, and introduction of the CD-ROM loadable module.
- SET parameter changes. Modifications have been made to the default values of certain SET parameters. Generally, these changes provide more support for clients or enhance the server's capabilities.
- New VLM DOS client architecture. Novell's new VLM/ODI client architecture takes advantage of the networking features built into later versions of DOS. The VLM/ODI architecture modularizes and adds substantial power and flexibility over earlier versions of NetWare shells.
- New NLMs. NetWare 3.12 introduces new NLMs that help manage connections and increase capabilities for developers and future enhancements.

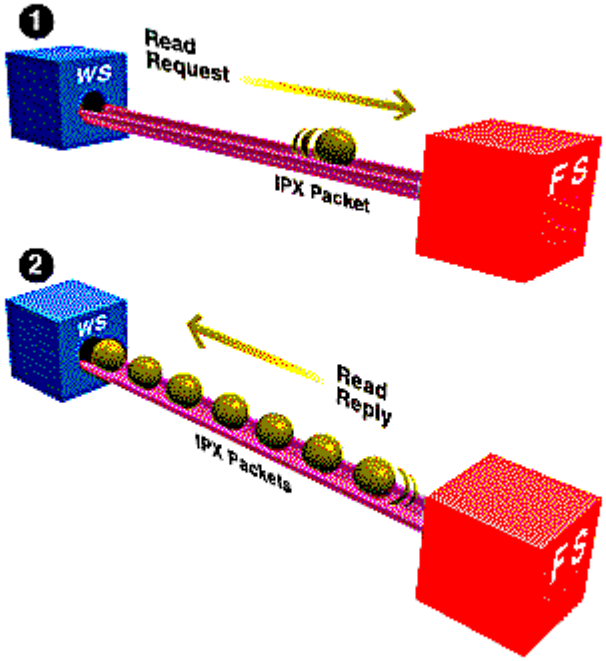
Packet Burst Support

Packet Burst is a protocol built on top of IPX that speeds the transfer of multiple-packet NCP (NetWare Core Protocol) file reads and writes.

When a client makes an NCP read or write request without the benefit of Packet Burst (as in previous versions of NetWare), each packet of the request is followed by an acknowledgment. This one-request/one-response method of communication is inefficient, especially when the requested data requires more than one packet.

Packet Burst protocol enables clients and servers to communicate more efficiently by speeding the transfer of multiple packet NCP (NetWare Core Protocol) read and write requests, thereby reducing network traffic. This protocol is built into the NetWare 3.12 operating system code and the client connection software.

Packet Burst allows a client read request to be made without an acknowledgment. The server returns the requested data in a burst, or series of packets. A write request is sent to the server in burst mode and only one acknowledgment is returned from the server for the complete burst to the client, as shown in Figure 1.



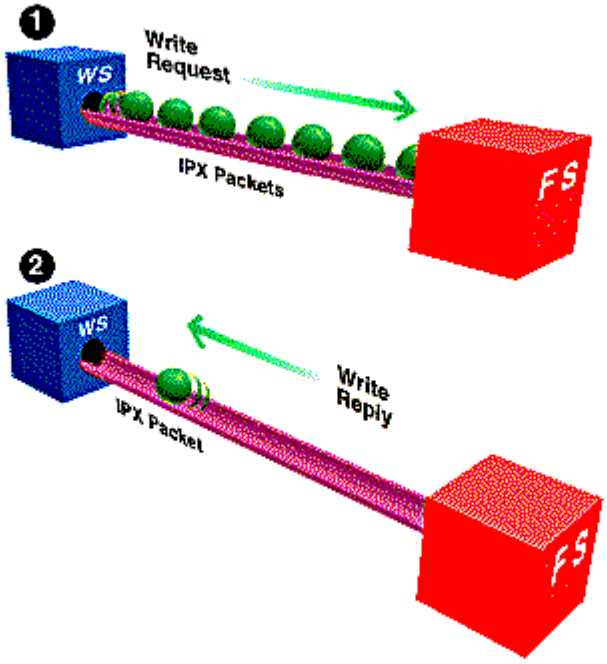


Figure 1: With Packet Burst, clients can have the server read or write large blocks of data comprising multiple packets.

Packet Burst is self-adjusting to a network's characteristics. If a network is experiencing heavy traffic, Packet Burst will adjust the number of packets within the burst. Packet Burst also has built-in correction schemes to watch for missing or dropped packets. If packets are missing, a request is issued for only the missing packets.

To control the flow of data, Packet Burst uses a dual volume-throttling mechanism that employs (1) an expanding and contracting window size algorithm and (2) a packet-transmission metering value.

The actual values for these two parameters are determined individually by each client on the network. To arrive at appropriate values, the client shell executes a complex transmission rate control algorithm.

Note: When Packet Burst is enabled at a server and it is communicating with a client where Packet Burst is not enabled, the server will communicate with this client in the one-request/one-response mode.

Packet Burst protocol increases the speed at which packets are distributed on the network. It is particularly useful within networks where high bandwidth exists on the media and wide area links are used, such as the following:

- Fast links (T-1)
- Multiple routes (X.25)

- Multiple hops over routers/bridges

An increase in performance on local Ethernet or Token-Ring networks can also be experienced because packets are transmitted as a unit.

Packet Burst may actually appear to function more slowly on networks that are heavily loaded or where no extra bandwidth is available on the media. Keep in mind that many factors contribute to the tuning of a network, and you must observe all of the factors when considering performance.

Enabling Packet Burst

Packet Burst is enabled at the server and the client by default in NetWare 3.12.

NetWare 3.11 required the PBURST.NLM and the BNETX.COM shell for Packet Burst to be enabled. This NLM and shell are not supported on a NetWare 3.12 server because Packet Burst support is already included in the operating system and the VLMs.

Existing clients using BNETX.COM will need to be updated to the new VLM client software to communicate with the new NetWare 3.12 server.

Large Internet Packet (LIP)

Large Internet Packet (LIP) is another factor in enhancing the network environment. It works to increase the speed of data transmission when communication occurs through a router.

Clients and servers always negotiate packet size when a client attaches to a server. Previously, if a server identified a router between itself and the client, packet size was set to 576 bytes. (The data portion of the packet is 512 bytes, with 64 bytes of header information.) LIP allows the client and server to negotiate the packet size used when communication occurs through a router, as shown in Figure 2. With LIP, the packets can be set to a maximum of 4202 bytes. The negotiated packet size will depend on the maximum physical packet size of the server.

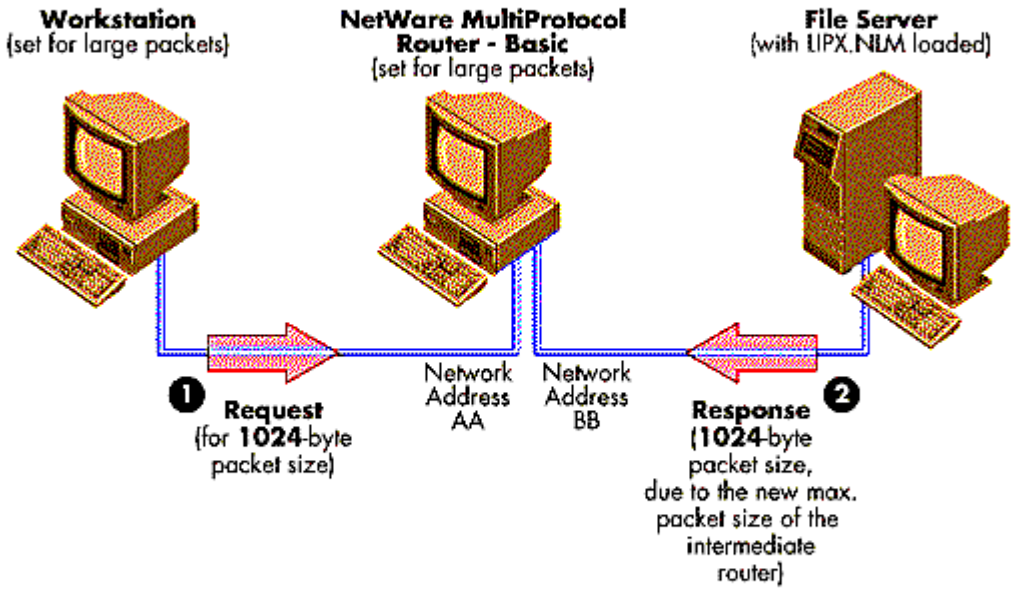


Figure 2: By allowing the NetWare packet size to be increased, LIP enhances the throughput over bridges and routers.

Note: Like Packet Burst, LIP is included in the operating system code of NetWare 3.12 and in the client connection software. LIP is enabled by default at both the server and the client. In some cases, packet size is hard-coded in the router. LIP will not be effective in these instances.

Ethernet Frame Type Changes

The default Ethernet frame type for NetWare 3.12 has changed to IEEE 802.2. (This is also true for NetWare 4.x.)

In previous versions of NetWare, the default Ethernet frame type was set to 802.3 Raw, which is nonstandard with the IEEE and ISO standards. Ethernet 802.3 Raw has the limitation of only supporting the IPX protocol. Figure 3 displays the Ethernet 802.3 Raw frame and its protocol identifier. This header includes a code that identifies the packet as an IPX packet.

Figure 3: Ethernet 802.3 Raw frame.

Ethernet 802.2 frames provide the advantage of supporting multiple protocols within a network. Figure 4 displays the Ethernet 802.2 frame type. Note the Logical Link Control (LLC) header. It identifies the protocols.

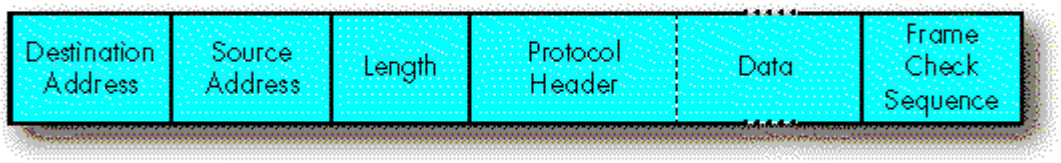


Figure 4: Ethernet 802.2 frame.

The default Ethernet frame type was changed to better accommodate planned future enhancements to network security and to better integrate NetWare into diverse environments.

The following factors also influenced the decision to change the default:

- Adherence to standards

  IPX on 802.3 Raw is not a standard. The standards bodies only recognize 802.2 and 802.2 SNAP frames.

- IPX checksums

  802.3 Raw headers do not have any Protocol Identifier (PID) field defined. As a result, all drivers (ODI, NDIS, etc.) use the 0xFFFF value found in the checksum field of the IPX header in the packet to determine if the packet is IPX on 802.3 Raw. When this field is used to insert valid checksums, these packets will not run on 802.3 Raw.

- OSI 802.2 diagnostics

  In 1992 it was pointed out that 802.2 headers with DSAP and SSAP values of 0xFF and 0xFF respectively are valid for certain OSI diagnostic response packets. These packets thus collide with IPX packets on 802.3 Raw because both look identical.

- MAC (Media Access Control) Layer Bridging

  When bridging Ethernet to Token-Ring (which is all 802.2), bridges cannot handle 802.3 Raw packets. Most bridge vendors have created bridge/routers to deal with this situationþthese devices use an IPX router to handle the 802.3 Raw IPX packets, and they bridge other packets. Other vendors have required users to use ODI drivers and switch to 802.2 to remove all 802.3 Raw IPX frames from the system.

Making the Change

If you add a server set to the frame type of Ethernet 802.2 to an existing Ethernet 802.3 Raw network, the clients will not be able to see the new server.

It is recommended that you update your existing servers and clients to the Ethernet 802.2 frame type.

You can gradually shift to the new default by providing access to both frame types at the server. Here are some suggested implementations that will allow all clients (connected by Ethernet connections) access to the new server:

- Add both frame types to the new server. In this way, the server will be able to support both old clients using Ethernet 802.3 and new clients using Ethernet 802.2.
- Change Ethernet 802.3 clients and servers to Ethernet 802.2 frame type.
- Set the new server to the Ethernet 802.3 frame type instead of the Ethernet 802.2 frame type. You will also need to adjust any new clients.

As NetWare continues to grow into large-scale networks, using industry standards will make integration into large networks easier to perform.

Modifying the Server AUTOEXEC.NCF File. If your current network uses the Ethernet 802.2 frame type, you can leave the frame type option of the LOAD LAN driver statement in place. However, if your network uses the Ethernet 802.3 frame type, you will need to add the frame type option to the LOAD LAN driver command.

The following example (using the NE2000 LAN driver) displays the commands used to load and bind both frame types to a single LAN driver in the AUTOEXEC.NCF file.

```
load NE2000 int=3 port=300 frame=Ethernet_802.2
        bind IPX to NE2000 net=ABCD
        load NE2000 int=3 port=300 frame=Ethernet_802.3
        bind IPX to NE2000 [int=3 port=300 frame=Ethernet_802.3 ]
          net =1234
```

Note the brackets surrounding the interrupt, port, and frame information.

The extra LOAD and BIND commands can be executed from the server console as well. The console will prompt you as you add the additional LAN driver and will allow you to select options.

Remember that to make the change permanent, you will need to add the statements to the AUTOEXEC.NCF file.

Modifying the Client NET.CFG File. Alter the current client NET.CFG file to support Ethernet 802.2 by adding the FRAME statement under the LINK DRIVER heading. For new clients, the client installation utility will create the NET.CFG file with the correct statement. See the following example:

```
LINK DRIVER NE2000
```

INT 3

PORT 300

FRAME Ethernet_802.2

If you have used SHELL.CFG files with previous versions of NetWare, you will need to convert these to NET.CFG files.

(For more information on frame types, see Migrating Ethernet Frame Types from 802.3 Raw to IEEE 802.2 in the September 1993 NetWare Application Notes, p. 71.)

NCP Packet Signature

NCP Packet Signature is an enhanced security feature that protects servers and workstations using NCP (NetWare Core Protocol) by preventing packet forgery.

Packet Signature prevents packet forgery by requiring the server and the workstation to sign each NCP packet. The packet signature changes with each packet. NCP packets with incorrect signatures are discarded without breaking the workstation's connection to the server. However, an alert message--containing the login name and station address of the affected workstation--is sent to the error log.

With NCP Packet Signature installed on the server and all workstations, forging a valid NCP packet is virtually impossible.

How NCP Packet Signature Works

The following list describes the steps that occur between a client and server using NCP Packet Signature:

- As a client logs in to a NetWare 3.12 server, the server and the client determine a shared key referred to as the session key. This key is unique for each client logged in to a given server.
- When the client requests services from the server, the client appends a unique signature to the packet before it sends the packet to the server.
- When the server receives the request, it checks the packet signature to see if it is correct for the client that sent it. If it is correct, the server processes the request and attaches a new signature to the reply packet.

If the client's packet signature is incorrect or if the client does not have packet signature activated, the packet is discarded and an alert message is sent to the server console and the server error log file. The offending client station will receive an error message indicating that an error occurred during the attachment to the server.

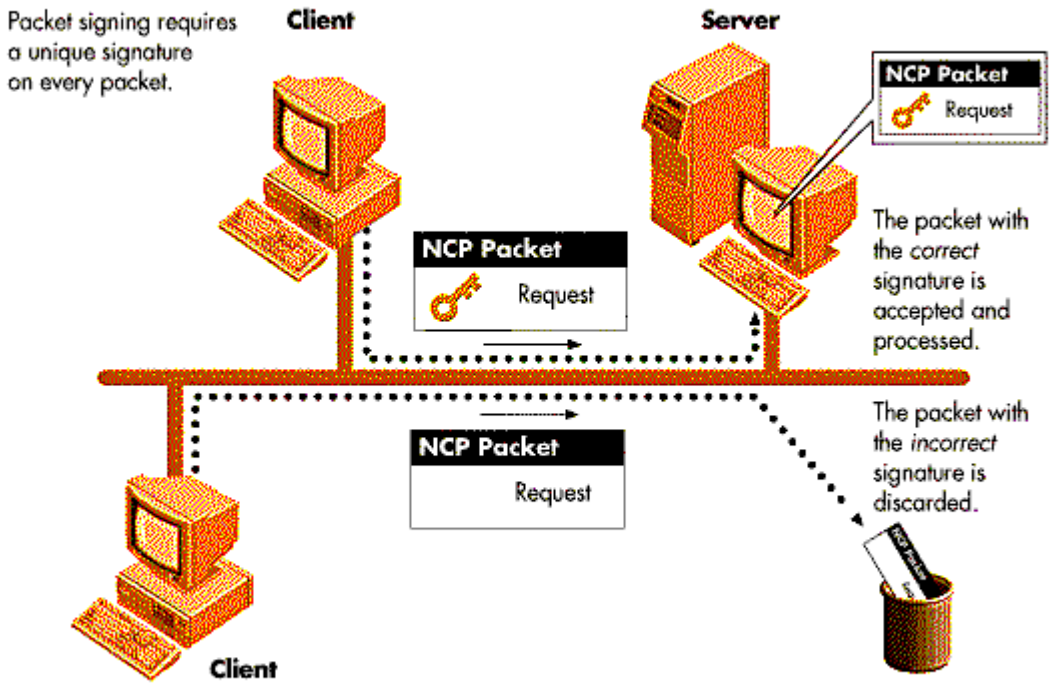


Figure 5: NCP Packet Signature prevents packet forging by requiring the client and server to sign each packet.

NCP Packet Signature is not required for every installation. Some may choose not to use Packet Signature because they can tolerate certain security risks. Calculating the NCP packet signature does consume CPU resources at both the client and the server. This overhead can slow performance in certain configurations. NCP Packet Signature is therefore optional.

Performance Considerations

NCP Packet Signature determination may cause some degradation of performance. However, many factors, including network traffic and CPU speed, also affect network performance. The type of services used will also affect the client's performance when using NCP Packet Signature, as listed below:

- Clients performing lighter tasks, such as word processing or spreadsheet creation, should not experience any slowdown.
- Clients requesting database queries, large file transfers, report generation, or similar load-intensive tasks will experience slowdowns.

You will notice less change in performance (while using NCP Packet Signature) if you do the following:

- Move to a server using a 486/50 CPU or better.

- Use client stations that have a 386 or better CPU. (Older clients with 286 or 8088 CPUs will experience the greatest slowdown.)

Additionally, if you have a mixed network with pre-NetWare 3.12 servers and NetWare 3.12 servers, problems may occur from using the pre-3.12 utilities. This is especially true with LOGIN and ATTACH.

NCP Packet Signature Levels

As Table 1 shows, a number of Packet Signature configurations are possible. In most instances, the default settings (server level=2 and client level=1) provide the most flexibility while still offering protection from forged packets. To implement a greater level of protection, you can change either the server level, the client level, or both.

Table 1: Packet Signature options.

Server Level->	0	1	2 DEFAULT	3
Client Level	not sign packets (regardless of client level)	Server does not sign packets (client requests it (client level = 2 or 3)	Server signs if client is capable of signing (client level = 1,2 or 3)	Server always signs and requires all clients to sign (or login will fail)
0	Client does not sign packets	No packet signature	No packet signature	No packet signature	No logging in
1 DEFAULT	Client signs only if server requests it (server option = 2 or 3)	No packet signature	No packet signature	PACKET SIGNATURE	PACKET SIGNATURE
2	Client signs if server is capable of signing (server option = 1,2 or 3)	No packet signature	PACKET SIGNATURE	PACKET SIGNATURE	PACKET SIGNATURE
3	Client always signs and requires server to sign (or login will fail)	No logging in	PACKET SIGNATURE	PACKET SIGNATURE	PACKET SIGNATURE (maximum protection)

Enabling NCP Packet Signature

If you want to disable packet signing or increase the level of security, issue the following commands.

At the server console or using the server's AUTOEXEC.NCF file, add the following statement:

SET NCP PACKET SIGNATURE OPTION = number

Using the client NET.CFG file, add the following statement under the NetWare DOS Requester heading:

SIGNATURE LEVEL = number

(For more information on NCP Packet Signature, see NCP Packet Signature Performance Considerations in the December 1992 NetWare Application Notes, p. 73.)

Routing Enhancements

NetWare 3.12 operating system code has been enhanced to provide improved handling of routing information. In previous versions of NetWare, routing information was searched in a linear fashion. When a route request was received, the routing table was searched from the beginning of the table until the information needed was located. In NetWare 3.12, a hashing algorithm has been added to increase the efficiency of the table search.

Consider a network with 200 servers. Any time a route request was received at a given server, the table with all of the addresses of the servers and routers was searched until the correct address was located. Hashing the table makes the search faster by narrowing the number of addresses that has to be checked.

This intelligent hashing of routing information allows the server CPU to spend less time on routing.

Memory Pool Enhancement

Memory allocation is the process of reserving specific memory locations in RAM for processes, instructions, and data. Alloc memory makes memory available for short-term needs, such as mapping drives, providing user-connection information, and locking files. Figure 6 illustrates NetWare 3.12's use of memory.

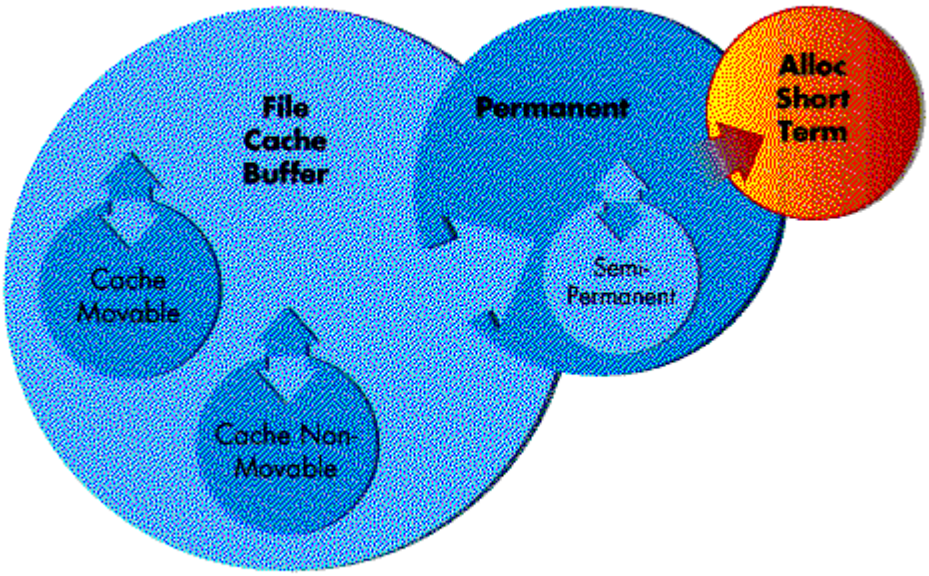


Figure 6: NetWare 3.12 memory pools.

NetWare 3.12 uses the same memory architecture as earlier versions of NetWare 3.x. However, changes to the core operating system require greater use of the Alloc Short Term Memory pool.

NetWare 3.12 commonly needs more than 2 MB in its alloc memory pool. Other demands--such as users not logging out, clients using MS-Windows and OS/2, and some disk drivers--cause the Alloc Short Term memory pool to reach its maximum value quickly.

Therefore, the default value and the range of values available have been increased. The default value for the Alloc Short Term Memory pool has changed to 8 MB (from 2 MB in NetWare 3.11). The maximum value has increased to 32 MB (from 16 MB in NetWare 3.11).

You can use the following SET memory parameter to change this value:

SET MAXIMUM ALLOC SHORT TERM MEMORY = value

The range of values is 50000 to 33554432 (32 MB).

You can verify the amount of memory being used by the Alloc Short Term memory pool by viewing the Server Memory Statistics window in the MONITOR.NLM under the Resource Utilization option.

Adjusting the Alloc Short Term Memory

Allow the server to self-adjust over three or four days and then view the Server Memory Statistics screen. Based on the information shown, you may want to adjust the Alloc Short Term Memory value.

You may want to decrease the value if your server does not use the allotted memory. Or, you may want to increase the value if the server issues warnings that an operation cannot be completed because this memory pool has reached its limit.

File System Enhancements

File system enhancements in NetWare 3.12 include:

- Cache read-ahead
- Enhanced extended attribute support for OS/2 2.1
- A module for CD-ROM use

Cache Read-Ahead

Cache read-ahead allows the server to read more into the cache buffer when the server is performing a sequential file read. This allows for faster file access. Cache read-ahead is controlled with the SET parameter READ AHEAD ENABLED. The default value is ON.

Enhanced Extended Attribute Support for OS/2

NetWare 3.12 supports OS/2 clients. The OS/2 Requester 2.01 and OS/2 utilities are available in NetWare 3.12.

OS/2 remote printing support uses NPRINTER.EXE rather than RPRINTER.EXE. (NetWare 4.x also uses NPRINTER.)

In addition, the NetWare 3.12 file system provides more complete support for the extended attributes of OS/2 2.1 than NetWare 3.11 did.

CD-ROM Module

NetWare 3.12 allows for the use of CD-ROM volumes through the CDROM NLM. The advantage you gain is support for read-only volumes on the network. Several server console utilities are available to control the device after CDROM is loaded.

With the CDROM-related server console utilities, you can perform these tasks:

- Change media
- List devices
- List volumes
- Mount and dismount volumes
- View the root directory of the volume

SET Parameter Changes

Modifications have been made to the default values of some of the SET parameters. Generally, these changes are made to provide more support for the clients or to enhance the server's capabilities. New SET parameters have also been added to work with Packet Burst and Large Internet Packet (LIP) and

other processes.

You may consider using these parameters to increase the capabilities of your server. Some of the parameters only work when placed in the STARTUP.NCF file, while others work in either the STARTUP.NCF or the AUTOEXEC.NCF file. Be careful to place the statements in the proper file.

Table 2 displays the modified and new parameters. The default values are displayed with the parameter.

Table 2: New and modified SET parameters.

Category	Parameter and Default Value	Limits	Description
Communication	Maximum Physical Receive Packet Buffers = 400	618 to 24682	The default packet size was changed from 1130 to 1514
	Maximum Packet Receive Buffers = 400	50 to 2000	The default value was changed from 100 to 400.
	NCP Packet Signature Option = 2	0 to 3	Sets the level of packet signature security at server.
	Enable Packet Burst Statistics Screen = OFF	ON, OFF	Determines whether to display the statistics screen.
	Enable IPX Checksums = 1	0 to 2	0 = No checksums performed 1 = Checksums performed if enabled at the client 2 = Checksums required
	Allow LIP = ON	ON, OFF	Determines whether Large Internet Packet is enabled.
File Caching	Read-Ahead Enabled = ON	ON, OFF	When set to ON and a sequential read is performed, background reads are done to retrieve needed file blocks.
	Read-Ahead LRU Sitting Time Threshold = 10 seconds	0 seconds to 1 hour	Determines the time after which read-ahead will occur.
	Reserved Buffers Below 16 MB = 16	8 to 300	Determines the number of cache buffers reserved for devices that cannot access memory above 16 MB. Set only in STARTUP.NCF.
File System	Maximum Extended Attributes per File or Path = 8	4 to 512	The default value changed from 32 to 8.

Disk	Concurrent Remirror Requests = 4	2 to 30	Determines the number of remirror requests per logical partition. Set only in STARTUP.NCF.
	Enable Disk Read After Write Verify = ON	ON, OFF	Default is set to ON.
Miscellaneous	Display Incomplete IPX Packet Alerts = ON	ON, OFF	Determines if alert messages are displayed when IPX receives incomplete packets. Set only in STARTUP.NCF.
	Replace Console Prompt with Server Name = ON	ON, OFF	Determines whether the console prompt will include the server's name.
	Allow Change to Client Rights = ON	ON, OFF	Determines whether a server can assume the rights of a client. Some third-party applications may not be able to function properly if this is set to OFF.

New VLM DOS Client Architecture

Novell's VLM technology is packaged as the preferred shell in NetWare 3.12. To provide full backward compatibility with existing DOS and MS-Windows applications, however, NETX, XMSNETX, and EMSNETX are also included.

NetWare 3.12 uses the DOS Requester as a replacement for the shell, NETX.EXE. The DOS Requester takes advantage of DOS redirection to provide file and print services. It also uses technology to add features to DOS and provide compatibility with NETX. The DOS Requester works with extended memory, expanded memory, and conventional memory.

The DOS Requester is required for use with NetWare 4.x NetWare Directory Services (NDS). The DOS Requester provides the following for NetWare 3.12 clients:

- Employs memory swapping technology and DOS redirection capabilities
- Includes Packet Burst and Large Internet Packet support
- Supports installed base of NetWare users by providing backward compatibility with NETX
- Provides support for MS-Windows clients

Additionally, the new design incorporates modularity that ensures that the Requester is equipped for future functionality when necessary.

In the NetWare 3.x shell, NETX works as a front end for DOS, intercepting user and application requests before they reach DOS. NETX determines whether to handle the request or pass it to DOS.

The DOS Requester works with DOS. The Requester and DOS share table information, reducing memory use. DOS also makes requests to the Requester for file and print services.

NetWare DOS Requester Components

The DOS Requester is a set of files loaded into the client station's memory. The Requester has two components:

- Manager (VLM.EXE)
- Virtual Loadable Modules (VLMs)

Manager (VLM.EXE). VLM.EXE loads and subsequently manages the Virtual Loadable Modules (VLMs). Its major responsibilities include the following:

- Handling requests from applications and routing them to the proper VLM
- Managing communication between modules
- Controlling memory services, allocation, and management

VLM.EXE replaces the NETX.EXE file. The ODI files (LSL.COM, the LAN driver, and IPXODI.COM) must be loaded before loading the DOS Requester.

Virtual Loadable Modules (VLMs). The DOS Requester is composed of Virtual Loadable Modules (VLMs). These files have a .VLM filename extension.

Each VLM provides a specific function. For example, the PRINT.VLM controls printing functions.

VLMs are of two types:

- Child VLMs
- Multiplexers (parent VLMs)

Child VLMs handle a specific function. Multiplexers route requests to the proper child. For example, TRAN.VLM is a multiplexer (parent) with two child VLMs.

VLMs are loaded into client memory by the manager, VLM.EXE. The client installation utility places the appropriate commands in the proper order in the NET.CFG file to load the VLMs. You can add other VLMs by modifying this file. If you choose to specify the load files, child VLMs must be loaded before their associated multiplexers.

(For complete information on the default VLMs that VLM.EXE loads, see Section 4 of the NetWare 3.11 to 3.12 Update Seminar Student Manual --#507.)

VLM Services. VLM functions fall into one of three service categories:

- DOS redirection
- Service protocol
- Transport protocol

DOS redirection services are handled through REDIR.VLM. DOS uses the redirector VLM to request file and print services from a server.

Service protocols handle requests for specific services. Connection establishment, broadcast messages, file reads and writes, and print redirection are supported at this layer. The principal modules are

NWP.VLM (the NetWare Protocol multiplexer), FIO.VLM (the file input/output VLM), and PRINT.VLM (the print redirector).

Transport protocols are responsible for maintaining server connections and providing packet transmissions and other transport-related services. The multiplexer at this level is TRAN.VLM.

Connection Manager. Another major portion of the DOS Requester is the Connection table manager (CONN.VLM), which provides support for all the service layers. It handles connection table entries and provides a common point of access to the table. The table tracks what service and transport protocols are being used for a given client connection.

Compatibility. NETX.VLM provides backward compatibility with existing NetWare applications by intercepting DOS calls.

Note: NETX.EXE conflicts with REDIR.VLM. Do not load NETX.EXE with the DOS Requester. Use the NETX.VLM.

The BIND.VLM maintains compatibility with non-NDS based servers, allowing you to view bindery information.

NetWare 3.12 Shell Files

The NetWare DOS Requester is the preferred DOS client connection software. NETX.EXE, EMSNETX.EXE, and XMSNETX.EXE are copied to the SYS:LOGIN directory during installation. You will need to copy the appropriate file to the client if you use the shell files.

You can also copy the shell files directly from the NetWare diskettes. They are located on the SYSTEM_3 diskette in the LOGIN subdirectory.

The shell files will work with the client configuration file, NET.CFG. If your current clients are using the older SHELL.CFG, you will need to update these to NET.CFG.

DOS Client Configuration File Modifications

During the client installation process, the install utility copies the VLM manager and modules to a directory named NWCLIENT (unless you specify otherwise). The install utility will also modify the CONFIG.SYS and AUTOEXEC.BAT files to incorporate the required statements if you allow the utility to perform this step. If you do not want the files modified, the utility will place copies of CONFIG.NEW and AUTOEXEC.NEW in the NWCLIENT directory.

DOS client configuration files are modified as follows:

CONFIG.SYS. Because DOS and the Requester share drive table information, LASTDRIVE must be set to Z. Include the following command in your CONFIG.SYS file:

LASTDRIVE=Z

The first NetWare drive you see depends upon the drives in the workstation and any substitute drive assignments. The client installation utility will set the first network drive to F in the NET.CFG file.

AUTOEXEC.BAT. You can create your own AUTOEXEC.BAT file to load the ODI and DOS Requester, or you can use the changes that are added by the client installation utility. The utility creates another batch file, called STARTNET.BAT, to load the networking files and adds the following statement to the AUTOEXEC.BAT file:

CALL C:\NWCLIENT\STARTNET

STARTNET.BAT. Although the commands listed below can be placed in AUTOEXEC.BAT, a network

startup batch file is created for them. It will load the ODI environment and load VLM.EXE. The commands include the following:

```
ECHO OFF
        C:
        CD \NWCLIENT
        SET NWLANGUAGE=ENGLISH
        LSL
        NE2000
        IPXODI
        VLM
```

SET NWLANGUAGE is used to set a variable for the Novell ElectroText.

VLM.EXE has options that can place VLM.EXE in the type of memory you want to use. If your workstation has extended memory, VLM.EXE will load part of the file there by default. The options include /MC for Conventional, /MX for eXtended, and /ME for Expanded.

NET.CFG. NET.CFG is the configuration file that provides information to the network startup files. LAN drivers are configured by the information contained in this file. Many parameters can be placed in this file to customize the client environment.

The following example shows the NET.CFG file after the client installation utility has been executed. The example shows an NE2000 driver.

```
Link Driver NE2000

    INT 3

    PORT 300

    MEM D0000

    FRAME Ethernet_802.2

NetWare DOS Requester

    FIRST NETWORK DRIVE = F

    USE DEFAULTS = OFF

    VLM = CONN.VLM

    VLM = IPXNCP.VLM

    VLM = TRAN.VLM

    VLM = SECURITY.VLM
      ;         VLM = NDS.VLM

    VLM = BIND.VLM

    VLM = NWP.VLM

    VLM = FIO.VLM

    VLM = GENERAL.VLM

    VLM = REDIR.VLM
```

VLM = PRINT.VLM

VLM = NETX.VLM

The above example displays the commands used to specify the load order of the VLMs. NDS.VLM has been commented out (with the semicolon) so that it will not load automatically. This makes the login process faster for clients only using NetWare 3.12. If the client also needs access to NetWare 4.x and NetWare Directory Services, simply remove the semicolon. Without the USE DEFAULTS = OFF and VLM = VLM filename lines, VLM.EXE loads all VLMs found in the client directory, thus slowing down the login process.

Following are some of the parameters used in NET.CFG. These parameters are used by various VLMs and are placed under the heading NETWARE DOS REQUESTER.

To specify the first network drive a user sees, use the following:

FIRST NETWORK DRIVE = drive pointer

Without this statement, the first network drive at a client with a local hard disk would default to D.

To change Packet Burst capability at a client, include the following:

PB BUFFERS = number

The default value is 3 (0 = off; values 1 through 10 enable Packet Burst and specify the number of buffers).

If you are using MS Windows, include the following:

SHOW DOTS = ON

The default value is OFF.

As stated earlier, the default Ethernet frame type has changed to 802.2. If you are using an existing network with 802.3 frames, include the following statement under the LINK DRIVER heading:

FRAME Ethernet_802.3

You may need to include specifics regarding your LAN driver. Check the documentation for your network boards.

New NLMs

NetWare 3.12 introduces new NLMs that help manage connections and increase capabilities for developers and future enhancements. CDROM.NLM has already been discussed; other NLMs are described below:

- NLICLEAR.NLM (Not Logged In Clear) can be used to clear connections held by unauthenticated user connections. Unauthenticated connections cannot be reused until they are cleared. This NLM is used primarily by NetWare Runtime.

  The syntax is as follows:

  LOAD NLICLEAR parameter

  Parameters can be added to specify the following:

  - Whether to notify the server console (NOTIFY)

- How often the server should search the connection table

  (POLL = number)

- How many connections to watch (CONN = number)

- KEYB.NLM can be used to specify the keyboard language type of the server console. The syntax is as follows:

  LOAD KEYB language

  Replace language with one of the following:

  - United States (default)

  - Germany

  - France

  - Italy

  - Spain

- RPL.NLM (remote program load) works with boot programs to provide support for remote booting of IBM diskless clients. You will still need to create the diskless client boot files and place them in the LOGIN directories of your servers. The syntax is as follows:

  LOAD RPL

- TSM modules. TSM is defined as Topology Support Module. ETHERTSM, FDDITSM, PCN2LTSM, RXNETTSM, and TOKENTSM provide additional support for the LAN drivers and the ODI environment. These modules will autoload with the respective LAN drivers.

- MSM31X.NLM is defined as Media Support Module. It provides additional support for the ODI environment and is autoloaded when the LAN driver is loaded.

- NWSNUT.NLM (Utility User Interface) provides a library of functions for NLMs that were written for NetWare 4.x. Generally, it is automatically loaded by the NLM that requires the set of functions. NWSNUT provides the same function that NUT.NLM does for NLMs written for use with NetWare 3.11.

- AFTER311.NLM provides developers with tools to create NLMs that will work with both NetWare 3.12 and 4.x. It is autoloaded by the NLMs that require its services. By using AFTER311 in conjunction with the 4.x OS library (NWSNUT.NLM), a developer can write an NLM that will work on both NetWare 3.x and NetWare 4.x.