chapter 3

Improving Speed and Security on Your Workstation

Chapter Overview

This chapter explains how you can improve workstation speed by using the Packet Burst protocol and Large Internet Packets (LIP). It also explains how you can protect information on your DOS and Windows workstations. The following topics are in this chapter:

Using Packet Burst to Increase Speed

The Packet Burst protocol is designed to transmit multipacket messages efficiently over the internetwork. Packet Burst is enabled automatically in the DOS Requester

Requirement for Packet Burst

The Packet Burst protocol code requires about 6 K of memory. However, as a default, the DOS Requester uses ODI for Packet Burst and doesn't require additional workstation memory.

How Packet Burst Works

At connection time, maximum burst sizes are negotiated with each server. Since Packet Burst is established with each connection, it's possible to "burst" with one server but not with another.

Once you establish a Packet Burst connection between a workstation and a NetWare server, the workstation automatically uses the Packet Burst service whenever an application requests to write more than one physical packet of data.

Disabling Packet Burst

Packet Burst is enabled by default in the DOS Requester.

To disable Packet Burst at the workstation, add this line to the workstation's NET.CFG file under the "NetWare DOS Requester" section heading:

```
PB BUFFERS= 0
```

Using Large Internet Packets (LIP) to Increase Speed

Large Internet Packet (LIP) functionality allows the packet size to be increased from the default of 576 bytes.

Previously, the size of packets that cross bridges or routers on NetWare networks was limited to 576 total bytes. Some network architectures (Ethernet and Token-Ring™) allow larger packets to be sent over the network.

By allowing the NetWare packet size to be increased, LIP enhances the throughput over bridges and routers if the routers aren't limited to the smaller packet size.

How LIP Works

In NetWare versions earlier than NetWare v4.0, the workstation initiated a negotiation with the NetWare server to determine an acceptable packet size.

If the NetWare server detected a router between it and the workstation, the server returned a maximum packet size of 576 bytes to the workstation.

In NetWare v4.0, the workstation still initiates packet size negotiation. However, the NetWare server doesn't return a packet size of 576 bytes when a router is detected.

Instead, the workstation negotiates with the NetWare server to agree upon a packet size.

Disabling LIP

LIP is enabled by default in the NetWare DOS Requester

To disable LIP functionality in the workstation, enter the following line in the configuration file (NET.CFG) under the "NetWare DOS Requester" section heading:

```
LARGE INTERNET PACKETS = OFF
```

Using NCP Packet Signature to Improve Security

NCP packet signature is an enhanced security feature that protects servers and clients using the NetWare Core Protocol by preventing packet forgery.

NCP packet signature is optional because the packet signature process consumes CPU resources and slows performance, both for the client and the NetWare server.

Without the NCP packet signature installed, a knowledgeable network client can pose as a more privileged client to send a forged NCP request to a NetWare server. By forging the proper NCP request packet, an intruder could gain rights to access all network resources.

How NCP Packet Signature Works

NCP packet signature prevents forgery by requiring the server and the client to “sign” each NCP packet. The packet signature changes with every packet.

NCP packets with incorrect signatures are discarded without breaking the client’s connection with the server. However, an alert message about the source of the invalid packet is sent to the error log, the affected client, and the NetWare server console.

If NCP packet signature is installed on the server and all its clients, it is virtually impossible to forge a valid NCP packet.

When to Use NCP Packet Signature

NCP packet signature is not required for every installation. Some network supervisors may choose not to use NCP packet signature because they can tolerate certain security risks.

Tolerable Security Risks

The following situations are examples of network situations that may not need NCP packet signature:

- Only executable programs reside on the server.
- All workstation users on the network are known and trusted by the supervisor.
- Data on the NetWare server is not sensitive; loss or corruption of this data will not impact operations.

Serious Security Risks

NCP packet signature is recommended for security risks such as these:

- Unauthorized users on a workstation on the network.
- Easy physical access to the network cabling system.
- An unattended, publicly accessible workstation.

NCP Packet Signature Options

Several signature options are available, ranging from never signing NCP packets to always signing NCP packets. NetWare servers and network clients both have four signature levels.

The default NCP packet signature level is 1 for both clients and NetWare servers. In general, this setting provides the most flexibility while still offering protection from forged packets.

The signature options for servers and clients combine to determine the level of NCP packet signature on the network.

Note Some combinations of server and client packet signature levels may slow performance. However, low CPU-demand systems may not show any performance degradation. Network supervisors can choose the packet signature level that meets both their performance needs and their security requirements.

Client Packet Signature Options

Client signature levels are assigned by a new NET.CFG parameter:

```
signature level = number
```

Replace *number* with 0, 1, 2, or 3. The default is 1.

Number	Explanation
0	Client doesn’t sign packets.
1	Client signs packets *only* if the server requests it (server option is 2 or higher).
2	Client signs packets if the server is capable of signing (server option is 1 or higher).
3	Client signs packets and requires the server to sign packets (or logging in will fail).

Effective Packet Signature Level

The packet signature levels for the server and the client interact to create the “effective” packet signature. Some combinations of server and client levels don’t allow logging in.

Table 3-1 shows the interactive relationship between the server packet signature levels and the client signature levels.

Table 3-1
Effective Packet Signature of Server and Client

IF	Server = 0	Server = 1	Server = 2	Server = 3
Client = 0	No packet signature	No packet signature	No packet signature	*No logging in*
Client = 1	No packet signature	No packet signature	Packet signature	Packet signature
Client = 2	No packet signature	Packet signature	Packet signature	Packet signature
Client = 3	*No logging in*	Packet signature	Packet signature	Packet signature

Examples of Packet Signature Levels

This section includes some examples of when you would use different signature levels.

All Information on the Server Is Sensitive

If an intruder gains access to *any* information on the NetWare server, it could damage the company.

The network supervisor sets the server to level 3 and all clients to level 3 for maximum protection.

Sensitive and Nonsensitive Information Reside on the Same Server

The NetWare server has a directory for executable programs and a separate directory for corporate finances (such as accounts receivable).

The network supervisor sets the server to level 2, and the clients that need access to accounts receivable to level 3. All other clients remain at level 1.

Users Often Change Locations and Workstations

The network supervisor is uncertain which employees will be using which workstations, and the NetWare server contains some sensitive data.

The network supervisor sets the server to level 3. Clients remain at level 1.

Workstation Is Publicly Accessible

An unattended workstation is set up for public access to non-sensitive information, but another server on the network contains sensitive information.

The network supervisor sets the sensitive server to level 3 and the unattended client to level 0.

Installing NCP Packet Signature

To install NCP packet signature on a DOS or Windows workstation, add the following parameter, under the "NetWare DOS Requester" heading, to the NET.CFG file of each workstation:

```
SIGNATURE LEVEL= number
```

Replace *number* with 0, 1, 2, or 3. The default is 1.

See Table 3-1, "Effective Packet Signature of Server and Client," on page 17 for a chart of the levels.

Troubleshooting NCP Packet Signature

This section describes some solutions to problems that may be associated with using NCP packet signature.

Clients Are Not Signing Packets

SECURITY.VLM isn't loaded. SECURITY.VLM loads by default when client signature is set to 1.

Clients Cannot Log In

SECURITY.VLM isn't loaded. SECURITY.VLM loads by default when client signature is set to 1.

Make sure the packet signature levels on the server and the client are correct. See "Effective Packet Signature Level" on page 16.

The following situations do not allow logging in:

- Server packet signature = 3, client signature = 0
- Server packet signature = 0, client signature = 3
- The LOGIN utility is an older version and doesn't support packet signature
- The Requester or shell is an older version and doesn't support packet signature.

"Error Receiving From the NetWork" Appears

The client is using a version of LOGIN.EXE file that doesn't include NCP packet signature. Make sure the new LOGIN.EXE and other new utilities are installed on all servers on the network.

Third-party NLMs Do Not Work

If the SET parameter "Allow Change to Client Rights" is set to OFF, some third-party NLMs may not function. Set this parameter to ON.

Unsecure Clients Log In to Secure Server

The clients are using an old LOGIN.EXE file that does not include NCP packet signature. Make sure the new LOGIN.EXE and other new utilities are installed on all servers on the network.

Add a preferred server statement to the NET.CFG file for all clients that have access to secure servers (level 3).

Using Other Workstation Security Guidelines

In addition to installing NCP packet signature, network supervisors can use other NetWare security features and protective measures to keep their workstation secure.

We suggest the following security guidelines for workstations:

- Use only the most current versions of system software, client software, and patches.
- Regularly check for viruses.
- Use the SECURITY utility to detect vulnerable access points to the server.
- Enable intruder detection and lockout.
- Advise users to log out when their workstations are unattended.
- Secure unattended workstations.
- Require passwords of at least five characters on all accounts.
- Force password changes at least every three months.
- Require unique passwords.
- Limit the number of grace logins.
- Limit concurrent connections.
- Enforce LOGIN time restrictions and station restrictions.