

## Preserving WAN Bandwidth

As you expand your company's network to include more servers, workstations, and WAN links, network performance can become a problem. To ensure that you are not wasting bandwidth, you should examine the type of communications that are being sent across the network. For example, if your company's network includes a dial-on-demand WAN link, such as an Integrated Services Digital Network (ISDN) line between two offices, you need to eliminate unnecessary communications that initiate this WAN link.

Because IntranetWare and NetWare devices perform several processes to maintain connectivity, these devices may be sending unnecessary communications over your company's WAN link. This article examines how processes such as NetWare serialization, NetWare Core Protocol (NCP) watchdog, SPX keep-alive, and queue sampling affect a WAN link. This article then explains how to prevent these processes from creating network traffic across a WAN link.

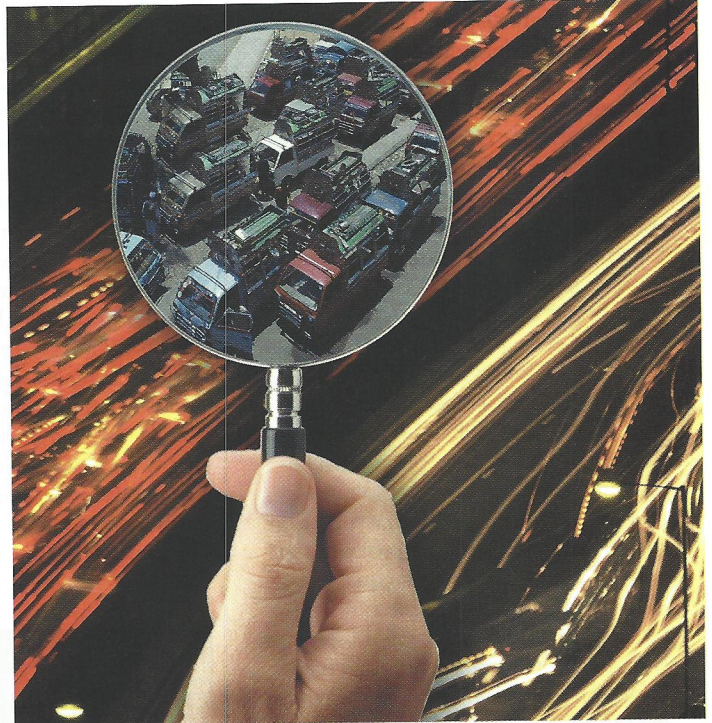
### NETWARE SERIALIZATION

Like many products, IntranetWare, NetWare 4, and NetWare 3 use a serialization process to detect copyright violations. Approximately every 66 seconds, each IntranetWare or NetWare server sends five serialization packets to other IntranetWare or NetWare servers on the network. These serialization packets are IPX packets that are addressed to serialization socket 0x0457 and contain the serial number of the transmitting server. (See Figure 1.) Although serialization packets provide only copy-protection information, they can consume bandwidth on your WAN link. If your company has a dial-on-demand WAN link, serialization packets can even establish this link between two servers.

Despite what you may have heard, you can use routers on each side of the WAN link to filter out serialization packets without affecting the way IntranetWare and NetWare servers communicate. In fact, many routers, such as Novell's NetWare MultiProtocol Router (MPR) 3.1, filter out serialization packets across a dial-on-demand WAN link by default.

### NCP WATCHDOG

When you log in to an IntranetWare or NetWare server, the server begins to monitor your workstation's connection for activity. If you log out of a server, the Novell client on your workstation sends a Destroy Connection NCP request to the server, which clears your workstation's connection ID number. If you simply



turn off your workstation without logging out of the network, however, the Novell client on your workstation cannot send a Destroy Connection NCP request to the server. As a result, the server does not clear your workstation's connection ID number.

IntranetWare and NetWare use the NCP watchdog process to identify and terminate invalid connections. If you log in to a server and do not communicate with this server within a specified amount of time, the server sends your workstation an NCP watchdog request to determine if your workstation's connection is still valid. (See Figure 2 on p. 34.)

If the Novell client is loaded on your workstation, this client sends an NCP watchdog reply to ensure that the server does not clear your workstation's connection. If the Novell client on your workstation does not send an NCP watchdog reply (because you shut off your workstation, for example), the server sends another NCP watchdog request. The server repeats this process the number of times specified by the Number of Watchdog Packets SET parameter. After reaching this number, the server assumes that the workstation's connection is invalid and clears the connection.

By default, an IntranetWare or NetWare server sends an NCP watchdog request after your workstation's connection has been inactive for five minutes. If your company has a dial-on-demand WAN link and no user is accessing this link, you certainly don't want the NCP watchdog process to establish this link because the connection has been idle five minutes.

To avoid establishing a WAN link for the sole purpose of sending and receiving NCP watchdog packets, some routers perform NCP watchdog spoofing: If the server and your



workstation are separated by a dial-on-demand WAN link, the local router replies to the NCP watchdog request on behalf of your workstation. As a result, a WAN link is not established. NetWare MPR 3.1 provides an NCP watchdog spoofing option, and Cisco's IOS software includes an IPX watchdog spoofing command that performs the same function.

Because these routers perform NCP watchdog spoofing, your workstation's connection remains intact unless you log out of the network. If you want to periodically clear connections on your server, you can have this server force every workstation to log out at a predetermined time, such as 9 p.m. In this way, all connections are available the next day.

If you do not have a router that performs NCP watchdog spoofing, you can reduce the traffic sent across the WAN link by increasing the values for three SET parameters:

- Delay Before First Watchdog Packet (default: five minutes)

No.	Source	Destination	Layer	Summary	Error	Size	Interpacket	Absolute Time	Relative Time
1	0080C767A093	COMPAQ-FS3	rip	Req network=BA 5E BA 11		64	0 µs	4:15:34 PM	0 µs
2	COMPAQ-FS3	0080C767A093	rip	Resp network=BA 5E BA 11, 1hop		64	522 µs	4:15:34 PM	522 µs
3	FS2	Broadcast	nisp	LAN Level 1NLSIP Hello Packet		100	3 s	4:15:38 PM	3 s
4	COMPAQ-FS3	FS2	ser	Novell Serialization (Copy Protection)		80	260 ms	4:15:38 PM	4 s
5	COMPAQ-FS3	FS2	ser	Novell Serialization (Copy Protection)		64	100 µs	4:15:38 PM	4 s
6	COMPAQ-FS3	FS2	ser	Novell Serialization (Copy Protection)		64	94 µs	4:15:38 PM	4 s
7	COMPAQ-FS3	FS2	ser	Novell Serialization (Copy Protection)		64	91 µs	4:15:38 PM	4 s
8	COMPAQ-FS3	FS2	ser	Novell Serialization (Copy Protection)		64	91 µs	4:15:38 PM	4 s
9	COMPAQ-FS3	0080C767A093	wdog	Poll inactive station, Conn=4		64	36 µs	4:15:38 PM	4 s
10	0080C767A093	COMPAQ-FS3	wdog	Session is valid, Conn=4		64	391 µs	4:15:38 PM	4 s
11	FS2	Broadcast	nisp	LAN Level 1NLSIP Hello Packet		102	1 s	4:15:38 PM	5 s
12	COMPAQ-FS3	Broadcast	nisp	LAN Level 1NLSIP Hello Packet		102	2 s	4:15:41 PM	7 s
13	COMPAQ-FS3	Broadcast	nisp	LAN Level 1NLSIP Hello Packet		100	373 ms	4:15:41 PM	7 s

```

Packet Number : 4          4:15:38 PM
Length : 64 bytes
802.3 : ----- IEEE 802.3 Datalink Layer -----
Station: COMPAQ-FS3 -----> FS2
Length: 36
ipx : ----- Internetwork Packet Exchange -----
Checksum: 0xFFFF
Length: 36
Hop Count: 1
Packet Type: 4(IPX)
Network: 00 00 00 33 -----> 00 00 00 22
Node: 00-00-00-00-00-01 -----> 00-00-00-00-01
Socket: 0x0000 -----> Serialize
ser : ----- Novell Serialization (Copy Protection) Packet -----
Serialization Data: 0 4 32 48 40 55
    
```

Figure 1. IntranetWare and NetWare serialization occurs approximately every 66 seconds.

- Delay Between Watchdog Packets (default: one minute)
- Number of Watchdog Packets (default: 10 watchdog packets)

The default values apply to IntranetWare, NetWare 4, and NetWare 3. You can use the SET utility to change these parameters on your server. For Intranet-

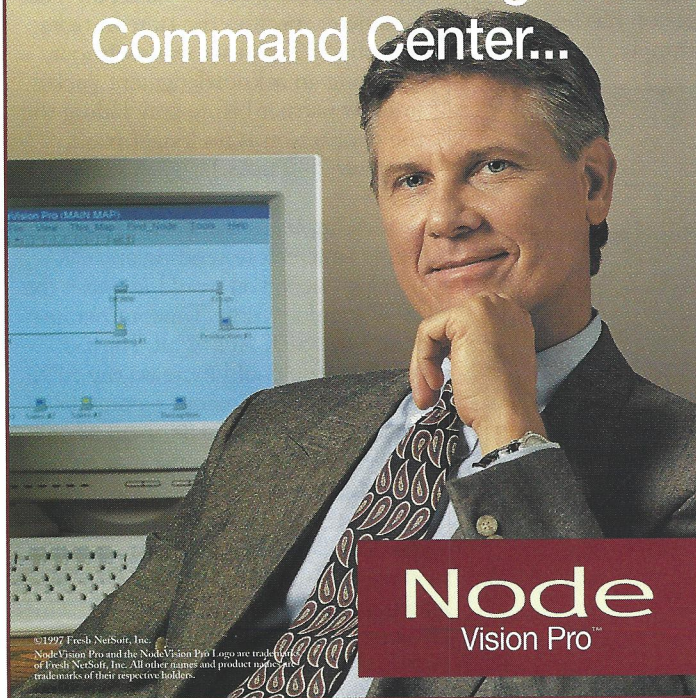
Ware and NetWare 4, you can also use the SERVMAN utility.

### SPX KEEP-ALIVE

Because SPX applications are connection oriented, each SPX application performs an SPX "handshake" with its partner before transferring data. Each side of an SPX connection is called a

Free  
30 Day Trial

## I've Finally Found the Ultimate Network Manager's Command Center...



# Node

## Vision Pro™



©1997 Fresh NetSoft, Inc. NodeVision Pro and the NodeVision Pro Logo are trademarks of Fresh NetSoft, Inc. All other names and product names are trademarks of their respective holders.

## And I'll Tell You This About NodeVision Pro™ ...

- It is easy to install, learn, and operate.
- It makes troubleshooting at the node level a breeze.
- It finds and highlights changes made in any text file.
- It doesn't have TSR's or NLM's that contend for network resources.
- It maps network segments automatically.
- It has color coded alarms.
- It has an outstanding Software Distribution module.
- It meters software on network, local drives, and CD-ROMs without an NLM.
- It has great remote file management.
- It allows me to snap in my favorite applications into the Management Console.
- It doesn't cost me an arm and a leg to buy.

Download NodeVision Pro for a **FREE 30 day trial** and compare it to SMS, ManageWise, LANDesk Manager, The Norton Administrator, and any other network management suite...

You'll be glad I told you about it!

<http://www.freshnetsoft.com>



Or call today, toll-free:  
**1-800-793-7374**

**fresh NetSoft**  
THE AFFORDABLE VISION FOR GROWING NETWORKS



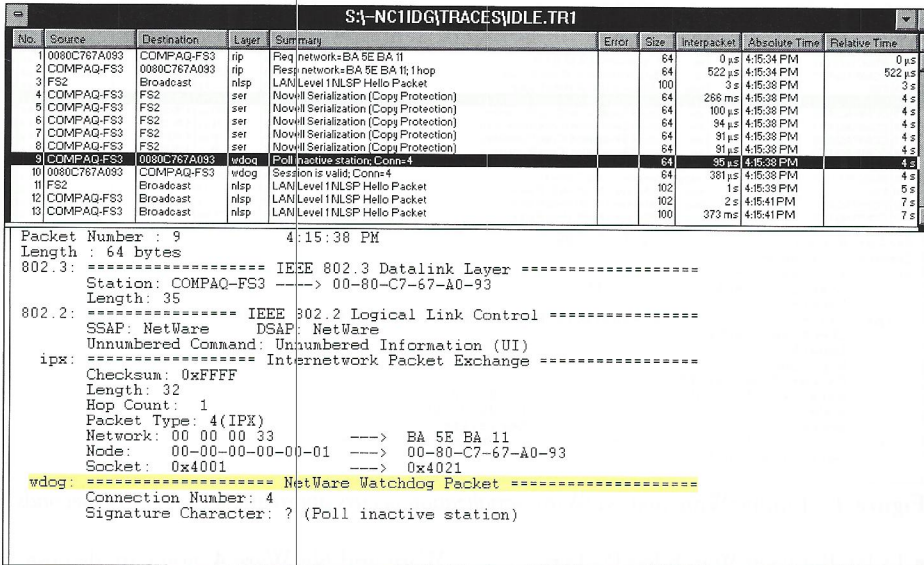


Figure 2. An IntranetWare or NetWare server sends NCP watchdog packets to identify valid connections.

partner. For example, if you were to use Novell's RCONSOLE utility, this utility would instruct the Novell client on your workstation to initiate a connection with the server that supports the RSPX and REMOTE NetWare Loadable Modules (NLMs). The SPX partners in this case are the Novell client (acting on behalf of the SPX application) and the server.

Because an SPX application sends an acknowledgment request with the data being transmitted, the SPX partner sends an acknowledgment packet after receiving this data. The following are common SPX applications:

- NetWare for SAA Gateway
- Btrieve
- Print server applications such as Novell's PSERVER utility and Hewlett-Packard's JetDirect
- Backup applications such as Cheyenne's ARCserve and Seagate's Backup Exec for NetWare

SPX applications such as the ones listed above use a keep-alive, or watchdog, process that is similar to the NCP watchdog process: By default, the SPX partners send watchdog packets to each other after their connection has been idle six seconds. For example, Figure 3

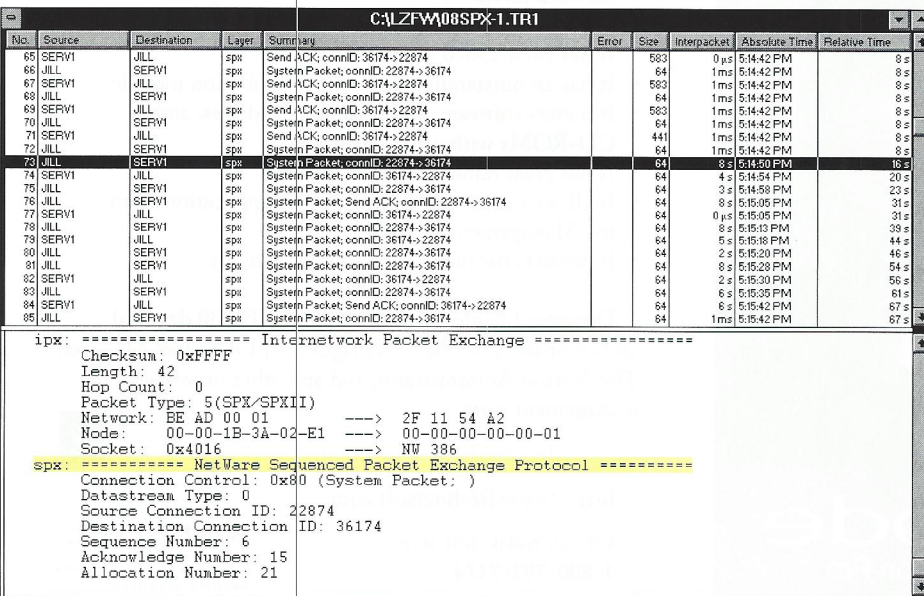


Figure 3. An idle RCONSOLE session initiates the SPX watchdog process.

shows SPX watchdog traffic from an idle RCONSOLE session.

You can decrease SPX watchdog traffic in the following ways:

- Increase the time before the SPX watchdog process begins, and increase the interval between the SPX watchdog packets.
- Disable the SPX watchdog process at the workstation to stop the Novell client from sending SPX watchdog requests to the server. (However, the client will still answer SPX watchdog requests from the server.)
- Purchase a router that can perform SPX watchdog spoofing.

### Increase Time Before the SPX Process Begins

To decrease the number of SPX watchdog packets sent over a WAN link, you can change the following SPX parameters.

- **SPX Watchdog Verify Timeout.** This parameter specifies the time in ticks that an SPX partner waits before requesting a watchdog packet from its SPX partner. (A tick is approximately 1/18 of a second. Default: 108 ticks.)
- **SPX Ack Wait Timeout.** This parameter specifies the time in ticks that an SPX partner waits for an acknowledgment packet before resending an SPX watchdog packet. (Default: 54 ticks.)
- **SPX Watchdog Abort Timeout.** This parameter specifies the time in ticks that the SPX partner waits without receiving an acknowledgment packet from its partner before concluding that the connection is no longer valid. (Default: 540 ticks.)

For example, to make the server wait a longer time before sending an SPX watchdog query, you would increase the SPX Watchdog Verify Timeout parameter and the SPX Ack Wait Timeout parameter. You could increase the SPX Watchdog Verify Timeout parameter to 14 seconds, and you could increase the SPX Ack Wait Timeout parameter to three minutes.

On an IntranetWare or NetWare 4 server, you can use the INETCFG utility to change the SPX parameters. (You must load the INETCFG utility at the IntranetWare or NetWare 4 server console.)

You can also change the SPX parameters at the workstation level. If you are



using Novell's NETX shell or Virtual Loadable Module (VLM) client, you can change SPX watchdog parameters in the NET.CFG file. If you are using Novell's IntranetWare client or NetWare Client 32, you can change the SPX parameters by accessing your Windows 95 Control Panel. Then you select Network, IPX 32-bit Protocol for Novell NetWare Client 32, and SPX.

Changing these parameters can significantly reduce the overhead on a WAN link. If you have a dial-on-demand WAN link, however, you should disable the SPX watchdog process or purchase a router that performs SPX spoofing.

#### Disable the SPX Watchdog Process

You can also prevent an SPX application on your workstation from using the SPX watchdog process to periodically validate SPX connections. If you are using Novell's NETX shell or VLM client, you can disable the SPX watchdog process by entering SPX WATCHDOGS = OFF under the PROTOCOL IPX heading in the NET.CFG file.

Of course, the Off setting specifies that the workstation cannot use the watchdog process. However, using the Off setting does not disable the SPX watchdog process at the server. If the server sends an SPX watchdog request to your workstation, the Novell client still answers this request.

If you are using the IntranetWare client or the NetWare Client 32, you can disable the SPX watchdog process by accessing your Windows 95 Control Panel. Then select Network, IPX 32-bit Protocol for Novell NetWare Client 32, and SPX. You must then deselect the Allow Connection Watchdogging option.

If you want to disable the SPX watchdog process at the server, you can use the SPXWDOG NLM. You can download this NLM from the Novell Support Connection World-Wide Web (WWW) site at <http://support.novell.com>. (Use the search engine to find the STRTL5.EXE file.)

#### Purchase a Router That Performs SPX Watchdog Spoofing

To eliminate SPX watchdog traffic across a WAN link, you can use a router

that performs SPX watchdog spoofing. For example, Cisco's IOS Software 11.1 includes an IPX/SPX spoofing parameter that enables the router to respond to SPX watchdog packets on behalf of your workstation. (For more information about Cisco's IOS Software 11.1, see <http://www.cisco.com/warp/public/732/Releases.1>.)

#### QUEUE SAMPLING

Your printer configuration can also generate unnecessary traffic if you assign a print server to a remote printer that is located on the other side of a WAN link. When a printer is idle, the print server assigned to that printer queries its print queue at regular intervals. This process is called *queue sampling*, or *queue polling*.

IntranetWare and NetWare 4 have a default queue sampling interval of five seconds; NetWare 3 and NetWare 2 have a default queue sampling interval of 15 seconds. (The *queue sampling interval* is the number of seconds between each query.) Unless you have changed the default setting, the print server looks for jobs in the print queue every five to 15 seconds,

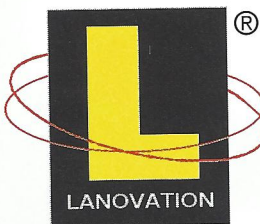
Windows 95  Windows NT  Windows 3.1  Windows for Workgroups









Heads Above  
Competition  
*InfoWorld*  
April 1997

## The World's Easiest Enterprise Software Distribution!

And Now... LAN Escort's Pictures provide  
the most powerful and flexible Windows  
management available!



LAN Escort Pictures Let You:

-  Distribute software
-  Take a Picture of any user's desktop
-  Control entire Windows environments
-  Maintain a database of workstation registry configurations
-  Troubleshoot Windows problems
-  Restore deleted shortcuts

How LAN Escort Works:



LAN Escort takes a picture.



You install an application.



LAN Escort detects ALL modifications. You don't struggle with creating a distribution package.

LAN Escort delivers!

1313 Fifth St. SE Minneapolis, MN 55414 612-379-3805 Fax: 612-378-3818 [sales@lanovation.com](mailto:sales@lanovation.com) [www.lanovation.com](http://www.lanovation.com)

Download a FREE evaluation copy of LAN Escort: [www.lanovation.com](http://www.lanovation.com) or call 800-747-4487

Circle 119 on the reader service card.



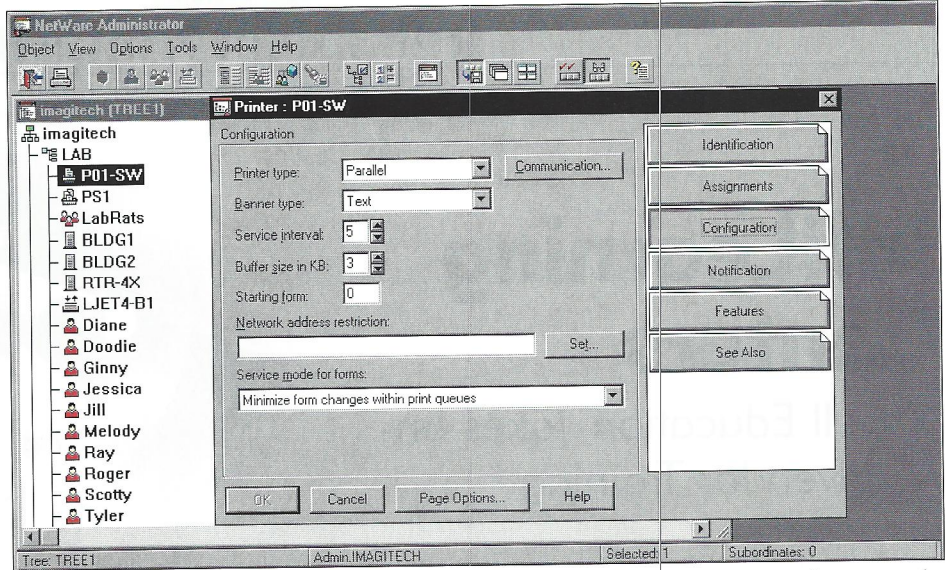
depending on which version of the operating system you are running. This queue sampling is a nightmare for WAN links.

You can solve this problem in one of two ways:

- Do not configure a print server to service print queues that are located on the other side of a WAN link.
- Use Novell's NetWare Administrator (NWADMIN) utility or Novell's PCONSOLE utility to increase the queue sampling interval to the maximum setting, which is 255 seconds. (See Figure 4.)

**CONCLUSION**

Analyzing the communications sent across your company's network is essential—what you don't know can hurt you. If network devices are sending serialization packets, NCP watchdog packets, SPX watchdog packets, and queue sampling packets across a WAN link, you should prevent these packets from crossing the WAN link or reduce the number of packets being sent. Taking these steps will im-



**Figure 4.** You can use the NWADMIN utility to configure a higher queue sampling interval.

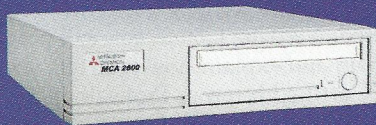
prove performance and even reduce costs if your company has a dial-on-demand WAN link and pays for this link on a per-packet basis.

Laura Chappell researches, writes, and lectures on NetWare protocol performance,

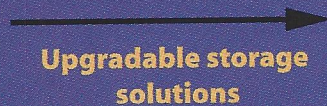
troubleshooting, and optimization. She speaks at NetWare Conferences and presents customized training courses on network analysis. You can reach Laura at [lchappell@imagitech.com](mailto:lchappell@imagitech.com), and you can view her trace files and presentation notes at [www.imagitech.com](http://www.imagitech.com).

**No more growing pains when expanding your business...  
Rely on Mitsubishi's complete storage solution for**

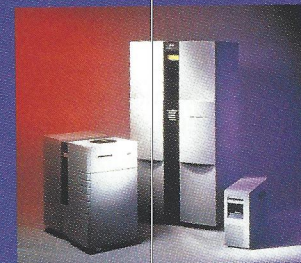
• Document Imaging • Medical Imaging • Backup • Graphics / Prepress • Audio / Video •



**5.25" Magneto-Optical Drive**



**Upgradable storage solutions**



**5.25" Magneto-Optical Jukeboxes**



**Drive A.I.D.**

**Drive A.I.D./Juke A.I.D.**

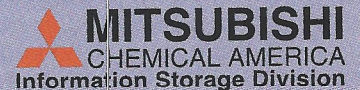
**Management Software for Stand-alone Drives and Optical Jukeboxes**



**Juke A.I.D.**



**For more information call  
1-800-DISKS-24**



[www.mitsubishi-infostorage.com](http://www.mitsubishi-infostorage.com)

©1997 Mitsubishi Chemical America, Inc. Juke AID is a registered trademark of Mitsubishi Chemical

Circle 120 on the reader service card.