disclaimer

This manual and the software it describes are protected by copyright. The manual and software as presented are the object of a license agreement and may be used only in accordance with the license conditions. The licensee bears all risk in regard to hazards and impairments of quality which may arise in connection with the use of this product.

This manual and the software programs it describes may not be transmitted, reproduced or altered in whole or in part, in any form, by any means, nor may they be translated into any other natural or computer language. The creation of a backup copy for personal use is excepted. The information herewith made available to the licensee may be communicated to third parties only with the written permission of AVM Berlin.

All software and the manual have been produced with all due care and inspected for correctness in accordance with the best available technology. AVM Berlin disclaims all liability and warranties, whether express or implied, relating to this product's quality, performance or suitability for a particular purpose which deviates from the performance specifications contained in the product description.

AVM Berlin will not be liable for damages arising directly or indirectly from the use of the manual or related software, nor for incidental or consequential damages, except in case of intent or gross negligence. AVM expressly disclaims all liability for loss of or damage to hardware, software or data as a result of direct or indirect errors or destruction and for any costs, including ISDN connection charges, related to the software and manual supplied and due to incorrect installations not performed by AVM itself.

The information contained in this manual and the software it describes are subject to change without notice for the purpose of technical improvement.

**AVM Audiovisuelles Marketing
und Computersysteme GmbH
Alt-Moabit 95
D-10559 Berlin
Tel.: +49-(0)30-399 76-0
Fax.: +49-(0)30-399 76-299**

**AVM Computersysteme
Vertriebs-GmbH
Alt-Moabit 95
D-10559 Berlin
Tel.: +49-(0)30-399 76-0
Fax.: +49-(0)30-399 76-299**

**NetWare MultiProtocol Router for ISDN 3.1
Installation and ISDN Configuration Guide
June 1996
Printed in Germany.**

Trademarks

NetWAYS/ISDN is a registered trademark of AVM GmbH.

Novell, NetWare, the N-Design, DR DOS, LANalyzer, and LAN WorkPlace, are registered trademarks of Novell, Inc.

The following are trademarks of Novell, Inc.: The NetWare Logotype (teeth logo), HSM, IPX, IPXWAN, LSL, MLID, MSM, MacIPX, NCP, NDR, NDS, NLM, NLSP, NMS, NPA, ODI, SPX, TSM, VLM, ElectroText, Hardware Specific Module, Internetwork Packet Exchange, Link Support Layer, Media Support Module, Multiple Link Interface Driver, NetExplorer, NetWare 3, NetWare 4, NetWare 4.1, NetWare Client, NetWare Connect, NetWare Core Protocol, NetWare Directory Services, NetWare DOS Requester, NetWare IPX Router, NetWare Link Services Protocol, NetWare Link/Frame Relay, NetWare Link/PPP, NetWare Link/SNA, NetWare Link/X.25, NetWare Loadable Module, NetWare MHS, NetWare Management Agent, NetWare Management System, NetWare MultiProtocol Router, NetWare MultiProtocol Router Plus, NetWare Peripheral Architecture, NetWare Ready, NetWare Runtime, NetWare WAN Links, Novell DOS, Novell Labs, Open Data-Link Interface, Packet Burst, Personal NetWare, Red Box, Sequenced Packet Exchange, Streams, System Fault Tolerant, Topology Specific Module, and Virtual Loadable Module.

The following are registered service marks of Novell, Inc.: NetWire.

The following are service marks of Novell, Inc.: Novell Network Registry, NSE Pro, Network Support Encyclopedia Professional Volume.

The following are collective marks of Novell, Inc.: Novell Authorized Reseller.

4.3BSD is a trademark of the Regents of University of California, Berkeley.

Apple, AppleTalk, EtherTalk, LocalTalk, Macintosh, and are registered trademarks of Apple Computer, Inc.

ARCNET is a registered trademark of Datapoint Corporation.

AS400, DOS, IBM, OS/2, Micro Channel, NetView, and PAL are registered trademarks and AFP, SAA, and VTAM are trademarks of International Business Machines Corporation.

AST is a registered trademark of AST Research, Inc.

AT&T is a registered trademark of American Telephone & Telegraph.

MS-DOS, Microsoft, and Word are registered trademarks of Microsoft Corporation.

NFS, Network File System, and Sun are registered trademarks and SunNet Manager is a trademark of Sun Microsystems, Inc.

All other trademarks, service marks, certification marks, and collective marks - registered or not - are the property of their respective owners.

Contents

About This Guide

This guide is written for the network administrator responsible for installing and configuring NetWare® software and NetWare® MultiProtocol Router™ for ISDN 3.1 software. It is not intended to provide detailed information about LAN media, WAN media, or network protocols.

As the administrator, you must plan and implement the connection of the router to the physical internetwork. This task involves laying the network cables, installing network interface boards, installing ISDN-Controllers, adding and removing nodes, and placing routers. To perform these tasks, you should have technical knowledge of protocols, network addressing, routing, and operational issues.

There are four basic steps to getting your NetWare MultiProtocol Router for ISDN installed and operating on your network:

- First, install one or more AVM ISDN-Controllers.
- Second, upgrade to or install new NetWare 3.12 (or NetWare 4.1) operating system software.
- Third, upgrade to or install the new NetWare MultiProtocol Router 3.1 software.
- Fourth, configure the network interfaces and protocols, then bind the appropriate protocols to the appropriate interfaces.

Chapter Summaries

This section briefly summarizes each chapter in this guide. Use these summaries to help you locate specific topics, or to help you decide which portions of this guide contain new information.

Chapter 1, "Introduction to NetWare MultiProtocol Router for ISDN 3.1," provides a detailed overview of the multiple features of the product.

Chapter 2, "Preparing to Install," describes site preparation and equipment setup tasks that must be completed prior to installing your NetWare operating system and NetWare MultiProtocol Router for ISDN software.

Chapter 3, "Installing NetWare MultiProtocol Router for ISDN 3.1," provides specific procedures for installing the NetWare MultiProtocol Router for ISDN 3.1 software on a local and a remote server.

Chapter 4, "Basic Design of ISDN-WANs and Configuration Overview," provides information on design and configuration issues for setting up WANs over ISDN, lists the configuration tasks to be performed and describes where to go for specific configuration instructions.

Chapter 5, "Configuring Boards," provides specific procedures for configuring your ISDN-Controllers used in the router.

Chapter 6, "Configuring ISDN Interfaces," provides specific procedures for configuring the ISDN interfaces and, due to INETCFG restrictions, specific parameters for each ISDN-Controller.

Chapter 7, "Configuring ISDN Call Destinations," provides specific procedures for configuring ISDN Call Destinations.

Chapter 8, "Configuring Global Parameters," describes configuration of parameters that apply for the router as a whole such as the ISDN Trap Propagation, global parameters for remote nodes and describes completion of the Call Acceptance Database.

Chapter 9, "Configuring IPX," describes different configuration possibilities for IPX over ISDN.

Chapter 10, "Configuring TCP/IP," describes different configuration possibilities for IPX over ISDN.

Chapter 11, "Configuring AppleTalk," describes configuration of AppleTalk over ISDN.

Chapter 12, "Configuring Source Route Bridge," describes configuration of a source route bridge over ISDN.

Chapter 13, "Advanced Configuration," discusses configuration of special ISDN connection types such as leased lines and semi-permanent connections,and provides specific information on configuring backup calls.

Chapter 14, "Configuration Interdependencies," provides specific information on interdependencies between configuration parameters.

Chapter 15, "Configuring Remote Node Access," provides specific procedures to configure the NetWare MultiProtocol Router for ISDN 3.1 for remote node access from NetWAYS/ISDN or PPP-compatible clients.

Chapter 16, "Utilities," describes special NetWare MultiProtocol Router for ISDN 3.1 utilities which consist of console commands, NetWare Loadable Module™ (NLM™) and configuration files.

Chapter 17, "Testing the Configuration," provides specific procedures for testing and troubleshooting the configurations associated with NetWare MultiProtocol Router for ISDN 3.1.

Chapter 18, "Monitoring ISDN Connections," gives detailed information on monitoring ISDN interfaces and ISDN connections and shows how you can limit connections to save charges.

Appendix A, "System and Error Messages," describes the causes and solutions of the system and error messages for the NetWare MultiProtocol Router for ISDN 3.1 product.

Appendix B, "AVM Data Call Center," provides specific access information for the AVM Data Call Center.

Conventions Used

The *NetWare MultiProtocol Router for ISDN 3.1 Installation and ISDN Configuration Guide* uses the documentation conventions described in this section.

The following typographical conventions are used:

- Highlighted monospaced character strings represent user input, which must be entered exactly as shown; for example:

  `LOAD TCPIP` <Enter> **`or Load tcpip`** <Enter>

- Highlighted and lowercase character strings show descriptive names for items that you must replace with appropriate values. For example, in the following NetWare console command, you replace driver with the specific name of a driver:

  `UNBIND IP FROM` `driver` <Enter>

- Regular (nonboldface, nonitalic) monospaced character strings represent system prompts or responses; for example:

```
message example
```

This symbol identifies the first step of a procedure. To accomplish a specific task, follow the steps in the procedure.

Graphic Symbols

Procedure

This symbol indicates lists of key points or elements that require attention.

Checklist

This symbol indicates sidelights, discussions, and general points of interest related to the current subject.

Note

This symbol points out key concepts or facts about the product.

Important

This symbol alerts you to situations that can produce critical or irreversible errors if you do not follow instructions carefully.

Warning

This symbol points out hints, tips, or helpful information that you should know.

Suggestion

The following AVM publications provide additional information and should therefore be at your hand:

Related Publications

- Technical Note on NetWare MultiProtocol Router for ISDN 3.1
- NetWare MultiProtocol Router for ISDN 3.1 Quick Installation and Configuration manual
- NetWare MultiProtocol Router for ISDN 3.1 Upgrade manual
- NetWare MultiProtocol Router for ISDN Solutions Guide

The following Novell publications provide additional information and should therefore be at your hand:

- NetWare MultiProtocol Router 3.1 Installation

- NetWare MultiProtocol Router 3.1 Configuration
- NetWare MultiProtocol Router 3.1 Management and Troubleshooting
- NetWare MultiProtocol Router 3.1 Release Notes
- NetWare MultiProtocol Router 3.1 Rules of Thumb
- NetWare MultiProtocol Router 3.1 Readme
- NetWare MultiProtocol Router 3.1 NetWare Link / SNA Host Programmer´s Guide
- NetWare MultiProtocol Router 3.1 Glossary (delivered on CD-ROM)
- Novell´s Guide to NLSP Migration (delivered on CD-ROM)
- NetWare MultiProtocol Router 3.1 Concepts (delivered on CD-ROM)
- NetWare MultiProtocol Router 3.1 System Messages (delivered on CD-ROM)

chapter

1 *Introduction to NetWare MultiProtocol Router for ISDN 3.1*

NetWare®MultiProtocol Router™ for ISDN 3.1 lets you build global networks over ISDN on the basis of proven NetWare, PC and ISDN technology. Through its powerful combination of PC-based routing and source-route bridging software with digital ISDN, the NetWare MultiProtocol Router for ISDN permits modular, cost-efficient integration of geographically distributed LANs and stand-alone PCs and provides synergy from the expertise of Novell® in NetWare-based routing and AVM in ISDN and Mobile ISDN technology to form global corporate networks over ISDN.

Routing Features

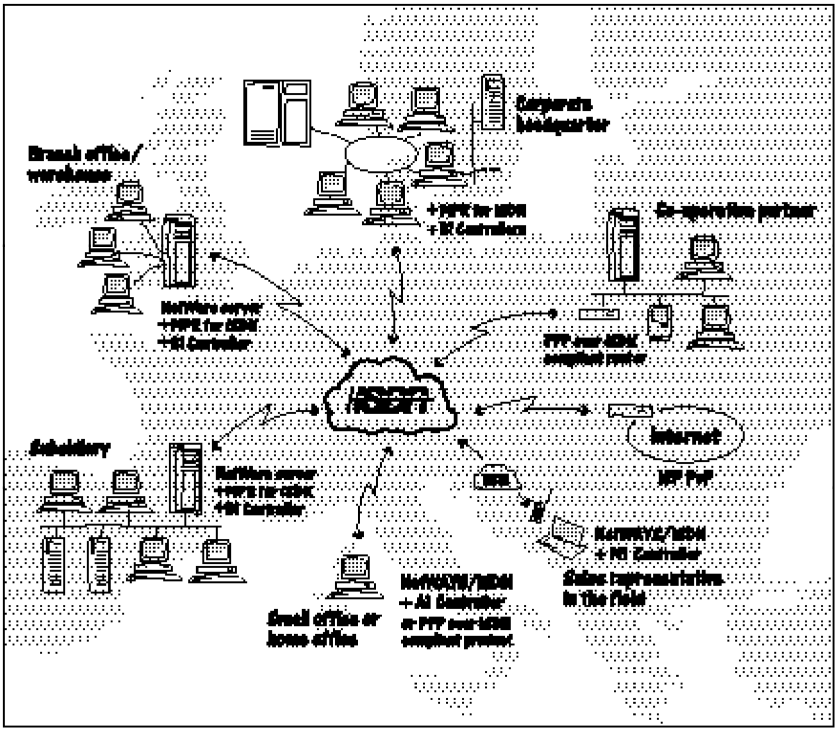
NetWare MultiProtocol Router for ISDN 3.1 provides IPX, TCP/IP and AppleTalk routing as well as Source Route Bridging over ISDN Basic Rate as well as ISDN Primary Rate Interfaces (BRI and PRI). LAN interfaces use Novell´s Open Data-Link Interface™ (ODI) specification; therefore, you can choose LAN boards for many media types, whether Arcnet, Ethernet, Token Ring or FDDI for example.

For ISDN access, NetWare MultiProtocol Router for ISDN uses AVM´s ISDN-Controllers, which support a wide range of ISDN access features for international deployment, including internationally and nationally standardized D channel protocols such as the ISDN signaling protocols DSS1, 1TR6, VN3/VN4, NI-1, 5ESS or TS 03. On the B channel, two different protocols are supported - AVM Proprietary and PPP over ISDN. AVM´s market-proven proprietary protocol has been in practical use for more than four years, offering more powerful features than defined for PPP so far, such as data compression (according to V.42bis), various line management features and access over GSM-based cellular networks. PPP over ISDN is an international standard intended to provide interoperability between remote access products of different manufacturers over ISDN. A further option, called Auto-Framing, enables the

NetWare MultiProtocol Router for ISDN to automatically detect whether an incoming call uses AVM Proprietary or PPP over ISDN.

The NetWare MultiProtocol Router for ISDN can be used as a dedicated router, which is the common set-up in larger networks, at the central sites and when PRI is used. It can also be installed on an existing NetWare file server, which is the common set-up in smaller networks and at branch offices. The following figure shows a sample scenario of LANs and stand-alone PCs interconnected over ISDN:

Figure 1-1:
LANs and Stand-Alone PCs Interconnected via ISDN



Besides interconnecting LANs and PCs over ISDN and GSM-based cellular networks to form company-wide networks, NetWare MultiProtocol Router for ISDN can be used for Internet access or to provide dial-up access to specific company-owned resources for other companies over ISDN, for example access to information or database services. For existing solutions with the NetWare Multi-

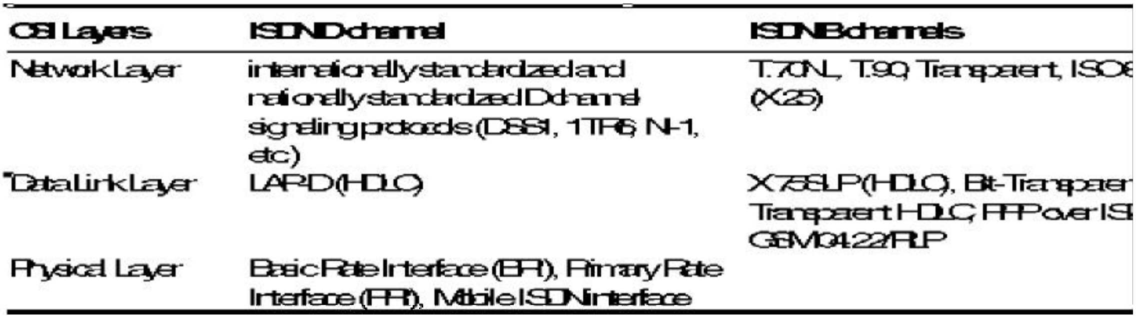
Protocol Router for ISDN in a number of companies, refer to the *NetWare MultiProtocol Router for ISDN Solutions Guide* by AVM.

Supported ISDN Protocols and Access Types

This section covers ISDN specific protocols and ISDN access types supported by the NetWare MultiProtocol Router for ISDN. A detailed survey on the supported networking protocols is given in the *NetWare MultiProtocol Router 3.1 Rules of Thumb*, pp. 4-7, and therefore not repeated here.

NetWare MultiProtocol Router for ISDN supports access from terrestrial ISDN BRIs (Basic Rate Interface) and PRIs (Primary Rate Interface) as well as access over GSM-based cellular networks from remote nodes equipped with AVM´s Mobile ISDN-Controller M1 and a mobile phone. A number of ISDN D and B channel protocols are supported. The ISDN protocols are software-implemented and can be loaded as required; thus, future enhancements and protocol changes can be effected through software without the need to replace ISDN hardware components. Additionally, NetWare MultiProtocol Router for ISDN 3.1 can also be equipped with an AVM Mobile ISDN-Controller M1 and a mobile phone for direct mobile-to-mobile links over GSM-based cellular networks. In Germany, for example, mobile-to-mobile links cost half as much as standard ISDN links.

Table 1-1:
Overview of ISDN Standards



OSI Layers	ISDN D channel	ISDN B channels
Network Layer	internationally standardized and nationally standardized D channel signaling protocols (DSS1, 1TR6, NI-1, etc)	T.70NL, T.90, Transparent, ISO (X.25)
Data Link Layer	LAPD (HDLC)	X.75 SLP (HDLC), Bit-Transparen Transparent HDLC, PPP over IS GSM 04.22 RLP
Physical Layer	Basic Rate Interface (BRI), Primary Rate Interface (PRI), Mobile ISDN interface	

ISDN D Channel Protocols

An overview of the important ISDN standards and their position in the OSI Reference Model is given in Table 1-1.

ISDN D channel signaling protocols are used for negotiations and connection set-up between the ISDN device, i.e. the router/ISDN-Controller and the public ISDN switches of the respective PTTs. The following D channel signaling protocols are supported:

- DSS1 (Euro-ISDN)
- 1TR6 (Germany, support for "Vorbestellte Dauerwählverbindungen" supported at BRI and PRI)
- DS01, DS02 (leased line types offered by the German PTT; DS01 offers one B channel and the D channel; DS02 offers two B channels and the D channel)
- D64S (leased line type offered by the German PTT, offering one B channel and no D channel)
- CT1 (Belgium, Norway)
- VN3/VN4 (France)
- NI-1 (USA)
- 5ESS (AT&T custom ISDN, USA)
- TS 013, AUSTEL (Australia, support for "Semi Permanent Connections" at BRI)

Depending on the PTTs offerings, different options are available. The following options are supported:

♦ Multipoint Access and MSNs/EAZs and SPIDs - BRI

Multipoint access is most commonly available at your Basic Rate Access. This access type includes a set of predefined numbers assigned to your access by your PTT and allows to set up a bus structure to connect and address different devices. These predefined numbers are, depending on the D channel protocol, called Multiple Subscriber Numbers (MSN) or "Endgeräteauswahlziffern" (EAZ). MSNs are supported by the NetWare MultiProtocol Router for ISDN within DSS1, VN3/VN4, NI-1, 5ESS and TS 013 (AUSTEL). EAZs are only used within 1TR6 and are also supported. Configuring an MSN or EAZ for a device tells this device to listen exclusively to this MSN or EAZ when a call comes in on the bus and to only react to incoming calls addressed to this number. Within the NetWare MultiProtocol Router for ISDN, you can and sometimes must configure an MSN or EAZ for each of the two ISDN interfaces (see Chapter 14, "Configuration Interdependencies").

SPIDs are Service Profile Identifiers which are used at NI-1 and AT&T custom ISDN switches in the USA to identify what sort of services and features the switch provides to the ISDN device. When a new subscriber is added, the service representative will allocate a SPID just as they allocate a directory number. The subscriber needs to input the SPIDs into their terminal device before they will be able to connect to the central office switch (this is referred to as initializing the device).

♦ Point-to-Point Access - PRI, BRI

Point-to-Point access is common with Primary Rate Accesses. But if you have more than one Basic Rate access, you may apply for this option (see "Hunt Groups" below). The NetWare MultiProtocol Router for ISDN supports Point-to Point accesses for PRI and with all BRI D channel protocols except for D64S, DS01, DS02 and GSM.

♦ DDI (Direct Dial In), an option for Point-to-Point access - PRI, BRI

At Primary Rate Interfaces and at Basic Rate Interfaces, you can apply for direct dial-in numbers from your PTT. Direct dial-in numbers can be compared with MSNs or EAZs. At PRI accesses, this is the only possibility to direct calls to a specific interface and can be compared to MSNs and EAZs at BRI accesses.

♦ Hunt Groups, an option for Point-to-Point access - BRI

If you applied for Hunt Group Numbers, you receive a single number for different physical Basic Rate Accesses. The NetWare MultiProtocol Router for ISDN supports Hunt Group Numbers at Point-to Point accesses with all D channel protocols except for D64S, DS01, DS02 and GSM.

ISDN B Channel Protocols and Options

ISDN B channel protocols are used for negotiations and connection set-up between the ISDN devices, i.e. the routers/ISDN-Controllers at each site, and to transmit network data. The following protocols are supported on the ISDN B channel:

- AVM Proprietary

  AVM´s market-proven proprietary ISDN protocol has been in practical use for more than four years. It is based on X.75SLP, which is standardized in ISDN. Since it offers more powerful features than PPP over ISDN such as data compression (according to V.42bis) and various line management features, it is the recommended protocol to be used for connections between AVM´s NetWare MultiProtocol Routers for ISDN and NetWare MultiProtocol Router for ISDN and AVM´s remote node product NetWAYS/ISDN.

- PPP over ISDN

  PPP over ISDN is an international standard intended to provide interoperability between remote access products of different manufacturers over ISDN. Since existing RFCs do not yet cover all features implemented in the NetWare MultiProtocol Router for ISDN, only those features can be used with PPP over ISDN that are already standardized through RFCs and are supported by the respective remote device. For a list of RFCs supported with the NetWare MultiProtocol Router for ISDN 3.1, refer to Chapter 9, "Configuring PPP over ISDN."

- Auto-Framing

  The Auto-Framing option enables the NetWare MultiProtocol to automatically detect whether an incoming call uses the AVM Proprietary protocol or PPP over ISDN.

The following options are supported on the B channel:

♦ ISDN connections with 64 Kbps and with 56 Kbps

Some public switches, mostly in the USA, do not offer 64 Kbps, but only 56 Kbps on the B channel. To decrease bandwidth to 56 Kbps, a signaling character is used on the D channel ("r" for restricted) in this case, which is added to the number dialed.

♦ GSM 04.22 (ISDN over GSM - Mobile ISDN)

This is not an option, but a protocol implementation on layer 1 of the B channel that is supported by the NetWare MultiProtocol Router for ISDN for remote node access with NetWAYS/ISDN and direct mobile-to-mobile LAN links over GSM-based cellular networks. It allows remote clients to use cellular mobile networks instead of terrestrial ISDN lines when dialing in to the LAN via NetWare MultiProtocol Router for ISDN. At the ISDN access of the LAN side, nothing changes and no special or additional option has to be applied for for mobile-to-ISDN links. However, use of this option depends on whether providers of GSM-based cellular networks offer access to ISDN from their networks and whether Unrestricted Digital Information (UDI) is enabled on the switches, allowing the service "data transmission" to be used in addition to voice transmission. This implementation is included in the NetWare MultiProtocol Router for ISDN drivers for DSS1 and 1TR6.

Direct Acess and Access through PBXs

AVM´s ISDN-Controllers for both, BRI and PRI can be installed directly at public ISDN accesses as well as at any PBX offering internal BRI or PRI access and uses one of the standardized ISDN D channel signaling protocols supported by the NetWare MultiProtocol Router for ISDN.

Survey of Important ISDN-Specific Features

NetWare MultiProtocol Router for ISDN is dedicated to ISDN and offers a large number of features especially designed for optimum use of ISDN. The following sections give a survey and explanations on important features and discuss conceptional issues on ISDN use and functions that you should keep in mind.

Toll-Saving Features

ISDN is a circuit-switched public network. ISDN connections are dialed up and charged by the PTT by the duration of the connection from the first set-up of a B channel until the last B channel is cleared down. This can be compared with making a phone call: you pick up the phone and dial a number. As soon as the call is answered by the remote site, charges accrue.

Some PTTs also charge call set-up over the D channel, disregarding whether the B channel was set up or not. When compared with a phone call, this means that as soon as the phone at the remote site rings, a charge unit accrues.

Thus, all features that save charges are important. In the following, toll-saving features are classified according to how they work, whether they save charges by generally optimizing ISDN use for internetworking via ISDN-specific timers, by optimizing network, protocol or application-specific behavior through filters and spoofings or by avoiding critical situtations, configuration errors, undesired or too frequent use of B channels by functions that disable a B channel for any physical action.

♦ Features clearing down the physical connection on the B channel

Inactivity Timeout and Self-Learning Inactivity Timeout clear down a B channel and are features that optimize ISDN generally for internetworking. In other words, they are indispensable for using ISDN in a cost-efficient way. Another timer, the Disconnect Timeout, plays a more specialized role, but is also described in this category.

The Inactivity Timeout functions exclusively clear down the physical B channel, so that no further charges accrue until the B channel is set up again physically. But it does not "touch" the logical ISDN B channel connection. This means that everything that has been negotiated once during an initial set-up of a B channel with the remote site over an ISDN interface for this connection remains active, and the interface itself is logically reserved for this connection. For remote node access, however, the interface reservation can be disabled to allow more than one remote node access to a single interface. The negotiated connection parameters nevertheless remain valid until the Disconnect Timeout expires.

The Disconnect Timeout can also clear down a physical connection, depending on how it is configured in relation to the Inactivity Timeout, but its main purpose and function is to clear down the logical ISDN connection on the B channel. This means that everything that has been negotiated once during an initial set-up of a B channel with the remote site over an ISDN interface for this connection is deactivated and the interface itself is logically released and available for any following dial-up operation to negotiate and set up a connection. Since it releases an ISDN interface, the Disconnect Timeout is one of the functions that can be used if an interface is not to be used to maintain a classic WAN link to a remote site, but is to be used dynamically to negotiate and set up different connections to remote sites.

♦ Features preventing set-up of a physically idle B channel

For this purpose, the NetWare MultiProtocol Router for ISDN 3.1 provides a number of filter and spoofing mechanisms. They prevent data packets addressed to a remote site from causing an idle B channel to be set up in order to transmit the packets over ISDN.

Besides their toll saving function, most of the filters are also used for security purposes, i.e. to prevent access from remote sites to servers or services. The NetWare MultiProtocol Router for ISDN implements filters and spoofings on the ISDN level as well as on the network level. The ISDN-specific toll-saving filters and spoofings are listed below:

- Watchdog Spoofing
- SPX Spoofing
- NCP Spoofing
- NW4/NDS Spoofing
- WAN LSP Hello Spoofing
- ARP Spoofing (only for IP remote nodes; always enabled)
- NetWare serialization packets filter
- NetBIOS (IPX packet type 20) broadcast filtering
- IPX Message Waiting Filter
- SNMP Over IPX filter
- SNMP Over IP filter
- NW4/NDS Filter
- Timesync Filter
- IPX Broadcast Filter (only for IPX remote nodes)
- IP Broadcast Filter (only for IP remote nodes)

Please note that filters, such as the Packet Forwarding Filter (FILTCFG.NLM) and several configurable timers that are very important to save tolls, such as the RIP/SAP Periodic Update Time-out or the NLSP Hello Timeout, are provided on the network level. You should check all filters, spoofings, and timers provided on the network level in any case when configuring your router. Further especially check the filters, when you use static routes instead of a routing protocol to a remote site and you use the Disconnect Time-out for this connection, since all ISDN specific filters and spoofings are negotiated during an initial set-up of a B channel and are only activated after a B channel has been set up. They are deactivated when the B channel is logically cleared down by the Disconnect Timeout. After that, any packet not filtered on the network level will initiate another physical and logical ISDN connection set-up over the B channel.

Note on bridging and NetWare for SAA:

Since NetWare MultiProtocol Router for ISDN provides SPX Spoofing, it is much more cost-efficient to set up the NetWare for SAA software at the site where the mainframes are located and let your clients use IPX/SPX over ISDN up to the NetWare for SAA software if you use NetWare for SAA for client-to-host access. The pollings of the NetWare for SAA software to reassure that the session with the clients is still alive are spoofed by the NetWare MultiProtocol Router for ISDN. In general, you should only bridge traffic over ISDN if you really have to, for example if you have two mainframes at two remote sites that have to exchange data. Whenever routing is possible, use routing, since it is much more flexible and, as explained above, can be more cost-effective.

♦ Features disabling B channels on the ISDN-Controller itself for any action

The following features avoid that critical situations, configuration errors, undesired or too frequent use of B channels cause undesired tolls:

- Time Restrictions for use of ISDN interfaces.
- Disabling of Outbound Call Processing on ISDN interfaces.
- ISDN Connection Monitor to configure thresholds on ISDN interfaces. When one of the thresholds is reached, the interface is barred for outgoing and incoming calls. To be on the safe side, defaults are given for the parameters.

To treat B channels of an ISDN-Controller differently, MSNs, EAZs or DDIs are required (see "Multipoint Access and MSNs/EAZs and SPIDs - BRI" above). For more information, refer to Chapter 14, "Configuration Interdependencies."

♦ Features disabling an ISDN call destination for any action

- ISDN Budget Manager to configure a daily, weekly and monthly budget for a call destination. When the maximum value is reached, the call destination is barred for incoming and outgoing calls.

- Time Restrictions for use of specific call destinations.

♦ **Reverse charging features**

COSO (Charge One Site Only) lets you allocate the connection charges either to your site or to the remote site or bar all outgoing calls to a call destination.

Watch Your ISDN Links

This section is intended to sensitize network administrators responsible for the WAN for the most important task that comes after the initial set up of the WAN itself: monitoring WAN links on a regular, daily, basis. The NetWare MultiProtocol Router for ISDN behaves exactly the way it has been configured, and dials up remote sites whenever a packet in a LAN is to be transferred to a remote site. In order to keep ISDN links physically down as long as possible, it provides a number of features - most of them have been described or mentioned in the above sections - that can be customized according to the networking needs and allow you to optimize your WAN traffic.

♦ **What can cause an ISDN link to become inefficient?**

During the set up of a WAN over ISDN, but also, probably more often, after the initial set-up, situations may appear that may very rapidly turn formerly efficient ISDN links into a very expensive affair. The causes for unnecessarily frequent call set-ups over ISDN may be very diverse. It may happen that, due to incorrect configuration, the router endlessly attempts to set up a connection to a remote site, if you configured the link to be set up automatically each time the connection fails, but did not make sure that the interface on the remote site is really available all the time. Other likely causes for unnecessarily frequent call set-ups over ISDN are components added to or already installed in the local networks themselves, for example an antivirus program installed only on one LAN, which automatically scans all servers of the WAN at very short intervals, a Windows for Workgroups client that has been added to one network and is sending NetBIOS broadcasts over IPX type 20 packets at regular, very short intervals, causing all ISDN links to all other remote sites to be set up in order to transmit such a broadcast packet, or an e-mail software that is configured to poll the status of remote "post-office boxes".

♦ The only way out - monitoring!

Monitoring of WANs is in general important, but it should be performed especially carefully when using ISDN as the wide area transport medium. Monitoring the WAN and all ISDN links maintained is extremely important and indispensable for keeping connection charges as low as possible. Only monitoring your WAN links will give you information on the number of ISDN connections established each day and allow to immediately detect "abnormal" situations, i.e. extremely frequent call set-ups or an extremely long physical up-time of an ISDN connection. Once you have detected the critical situation, you can manage the WAN, check whether you used all mechanisms provided by the NetWare MultiProtocol Router for ISDN to optimize WAN traffic, sort out the node in the LAN producing the packets that cause an ISDN connection to be set up too often, etc.

It is advisable in any case to make use of the ISDN Connection Monitor and the ISDN Budget Manager. Cutting down an existing ISDN link is a drastic measure, but they can be "there" also if you are absent, and, even if you may have to sort out problems that appeared due to the cut-down of the WAN connection afterwards, it will prevent high charges from accruing at your ISDN access.

Performance-Enhancing Features

ISDN provides 64 Kbps per B channel (except for some ISDN switches in the USA with 56 Kbps). The NetWare MultiProtocol Router for ISDN fully uses the given bandwidth on ISDN, i.e. it reaches a net throughput of 60 to 62 Kbps out of the theoretical rate of 64 Kbps. In addition, it offers various features to enhance throughput over ISDN.

♦ Compression

The NetWare MultiProtocol Router for ISDN implements software data compression according to V.42bis, but compression is completely downloaded and processed on the ISDN-Controllers. Thus - especially important when installing the router on a NetWare file server to offer file, print and routing services - the server is not burdened with the task of compressing and decompressing data, which would require a considerable amount of power and could slow down the file and print services. With compression according to V.42bis, ratios of 4:1 can be achieved, depending on the type of data transferred. V.42bis works perfectly with ASCII files, but worse with already compressed files, for example.

In addition to data compression, header compression is implemented for IPX (CIPX) and TCP/IP (van Jacobsen), also downloaded and processed on the ISDN-Controllers.

Third, the NetWare MultiProtocol Router for ISDN supports packet sizes of up to 4530 bytes. By joining or splitting packets depending on their size before transmitting them over ISDN, throughput is further optimized.

The performance-enhancing features described above could be regarded at as "toll-saving" features too: the faster data is transferred over a link, the less time it takes and the less you pay, since ISDN is charged by the duration of a connection.

♦ Bandwidth aggregation

Performance-enhancing features also include both Static Bundling and Channel On Demand. Static Bundling defines the number B channels to be set up additionally whenever data is to be transmitted, whereas Channel On Demand only sets up additional B channels dynamically when the configured load threshold is reached. With BRIs, up to 8 data channels can be bundled over several ISDN-Controllers. With PRIs, up to 16 data channels can be bundled.

NetWare MultiProtocol Router for ISDN 3.1 also supports the PPP Multilink protocol (PPP MP), which was developed by the Internet Engineering Task Force (IETF) as an extension to PPP. PPP MP extends PPP so that it can split and combine packets over multiple parallel links in order to create a higher aggregate data rate. It can be used to combine the two B channels in an ISDN Basic Rate Interface line to provide an effective wire speed up to 128 Kbps.

Another method is routing protocol-based load balancing over parallel links using NLSP; regarding ISDN B channel set-up, this bandwidth expansion method can be compared with Static Bundling.

Note

AVM is continuously working to enhance products and develope new products, such as compression and support for Mobile ISDN on the ISDN-Controller T1, encryption on the ISDN-Controllers B1 and T1, etc. As soon as future enhancements to the NetWare MultiProtocol Router for ISDN are available, a release note will be placed on the AVM Data Call Center (see

Appendix B for phone numbers and access information) and the new features will be described in a Technical Note.

Classic and Dynamic ISDN Interface Use

The NetWare MultiProtocol Router for ISDN allows you to set up classic WANs over ISDN, for example to interconnect three remote LANs permanently to form a company-wide WAN over ISDN. Permanently of course does not mean that the physical ISDN connection is permanently up (Inactivity Timeout controls the physical connection), but permanently available to be dialed and set up whenever needed, since a basic assumption for classic WANs is that all servers and services at all sites must be available all the time to run any networking tasks over the WAN the same way as it is done within the LAN.

But, since ISDN offers fast call set-up, new, additional requirements come up that can be accomplished as well with the NetWare MultiProtocol Router for ISDN and are not common with classic routing and classic WAN media: So-called dial-around tasks, where connections to remote sites are not required permanently but only needed temporarily, for example twice a week to perform tasks such as distributing software updates, e-mail or collating databases, as well as to offer dial-up access to services or specific company-owned resources over ISDN for other LANs and stand-alones, for example access to information or database services.

Classic WANs Involve Classic ISDN Interface Use

When setting up classic WANs, you use the ISDN interfaces in this classic way. When accomplishing dial-around scenarios, you use ISDN interfaces and underlying B channels dynamically to connect to multiple remote sites. You can mix both concepts with the NetWare MultiProtocol Router for ISDN, for example use three ISDN interfaces and underlying B channels for classic WAN links and use a fourth ISDN interface and underlying B channel to accomplish dial-around tasks. The two are described in detail in the following.

Classic WANs over ISDN are set up by dedicating one ISDN interface to each destination. This guarantees that the underlying physical B channel (or B channels) is (are) always available for the respective connection, the same way a leased line or a LAN media is.

- **Initial call set-up**

These classic WAN links are set up only once, mostly manually by using CALLMGR, or, if static routes/services have been configured, they are set up by a request from the respective network protocol each time a packet is addressed to a remote destination.

- **Physical clear-down**

For control of all underlying physical ISDN connections over the B channels, you configure the Inactivity Timeout for each destination. It will clear down B channels physically when no packets are to be transmitted to a destination. The B channel is always set up again automatically within 1 to 2 seconds if data is to be transferred. Thus, this process of underlying connection set-up is completely transparent to users or applications.

- **ISDN interface stays reserved for the connection**

Whereas you configure an Inactivity Timeout in this case, you do not configure a Disconnect Timeout. Thus, although the Inactivity Timeout clears down the B channel physically, the ISDN interface, which has been assigned by the network administrator to handle the link and treats one or more underlying B channels according to the configuration for the specific connection, stays logically connected and reserves underlying B channels for the connection. This means that, even in times when the B channel is physically idle and could theoretically be used for any other connection, the ISDN interface will reject any call set-up request coming from either site of this interface: If a call set-up request is issued from within the LAN using another call destination over the same ISDN interface, manually through CALLMGR or by a data packet for example, the request will be rejected by this ISDN interface. If a remote site dials in and addresses this ISDN interface, the call will "reach" the ISDN-Controller this interface belongs to, the physical B channel will be set up to negotiate connection parameters (whenever a B channel is physically idle, it is available and will listen to any call-set up request if not configured differently) and, since the information on which ISDN interface is addressed is transmitted over the B channel (AVM Proprietary: by the Destination Subaddress; for PPP over ISDN, this is different), the ISDN interface will then immediately reject the call set-up request and clear down the physical B channel. Thus, in any case as long as the ISDN connection is not logically cleared by another method than the Disconnect Timeout, the ISDN interface remains reserved for the connection once set up over this interface.

For remote nodes, interface reservation can be achieved by setting the parameter "Remote Node Usage" in the *Expert Configuration for Interface <Interface Name>* to "Exclusive Interface Reservation".

This is the basic set-up of a classic WAN link over ISDN, disregarding whether you route and/or bridge and disregarding whether you use routing protocols, such as RIP/SAP, NLSP or OSPF, or configure static routes/services for IPX, IP or AppleTalk. Setting up WANs this way guarantees that the physical link is always available when needed, because the ISDN interface reserves the B channels for the configured destinations.

Dial-Around Scenarios Involve Dynamic ISDN Interface Use

For dial-around scenarios, ISDN interfaces are not dedicated, but used dynamically for multiple destinations. In these scenarios, it is not guaranteed that a physical B channel (or B channels) is (are) always available for a connection, since it may already be in use for another connection that has been configured to be set up over the same ISDN interface.

♦ Initial call set-up

Such dial-around links are set up on demand, rarely manually by using CALLMGR, for IPX further by using CICC (rarely manually from a client, but in most cases with the help of batch routines), and, most commonly with TCP/IP but also possibly for IPX and AppleTalk, by configuring static routes/services for set-up by a request from the respective network protocol each time a packet is addressed for a remote destination.

♦ Physical clear-down

For control of all underlying physical ISDN connections over the B channels, you configure the Inactivity Timeout for each destination the same way you do it for classic WAN links.

- **ISDN interface is released for any other connection**

In addition to the Inactivity Timeout, you configure the Disconnect Timeout for each destination. Both Timeouts are either set to the same value for one destination or the Disconnect Timeout is set to a significantly higher value. Whenever a connection is set up by one of the above described mechanisms, the ISDN interface that has been assigned by the network administrator to handle the link is activated and the B channel is set up according to the configuration for the specific connection. The B channel is cleared down physically by the Inactivity Timeout and the ISDN interface stays logically connected and reserves the underlying B channels for the specific connection until the Disconnect Timeout expires. This may happen either at the same time or two hours later for example, depending on what you configured. During the logical up-time (if there is one), an underlying B channel would always be set up automatically to the same destination and all ISDN line management and other ISDN specific parameters configured by the network administrator for the specific connection would be active. As soon as the Disconnect Timeout expires, the logical ISDN connection is cleared, the ISDN interface is released and all parameters negotiated during the initial call set-up and assigned for the specific connection as well as all information about this connection is "given up". The ISDN interface is then available for any further connection set-up initiated by any of the methods described above. Be aware that any following initial connection set-up over the ISDN interface will cause the B channel to be set up and all ISDN specific features to be negotiated with the remote site before they are activated, i.e. basically everything configured in the ISDN Network Interface Configuration and everything configured in the Call Destination Configuration.

This is the basic set up of dial-around links over ISDN. In contrast to the classic WAN set-up, this set-up cannot be used with bridging, but it can be applied irrespective of whether you use routing protocols such as IPX RIP / SAP, NLSP or OSPF or configure static routes / services for IPX, IP or AppleTalk. The two major differences to classic WANs and interface usage are:

- When setting up dial-around scenarios, it can never be guaranteed that the physical link is always available when needed, because the ISDN interface only reserves the B channels for the configured destinations until the Disconnect Timeout expires or another method is used for clear down such as CICC for IPX or CALLMGR.

- When setting up dial-around scenarios, all ISDN-specific configurations and parameters to handle a connection will not only be negotiated once for each destination and then be active over months or years, but will be negotiated as often as a logical ISDN connection set-up to each destination is initiated by any method and will be released as soon as the logical ISDN connection is cleared down by any method.

Be More Careful When Using ISDN Interfaces Dynamically

When using ISDN interfaces dynamically, you have to be more careful when designing your networks and configuring the ISDN specifics and take a closer look at all configuration interdependencies arising from network and ISDN behavior.

♦ Networking processes corrupted

First, you must take care that no networking process is corrupted because a physical link to a remote site is required for this process to work, but is not available at that time since the ISDN interface and the underlying B channel is already set up to another destination.

♦ Frequent call set-up due to packets not filtered or spoofed on the network level

Second, and especially when using static routes/services instead of any kind of "controlled" connection set-up (CALLMGR or CICC), any packet addressed to a remote site results in a network request processed to the ISDN interface. If the ISDN interface is available at that time, i.e. not yet logically connected to any destination, it does not know about any of the configured ISDN-related connection specifics for the destination it is requested to set up the call to, since all ISDN-specific parameters such as filters and spoofings are not active to any remote site until the logical ISDN connection has been negotiated and set up but do only apply afterwards until this logical ISDN connection is cleared down again. Thus, for any packets you do not want to have an ISDN line to be set up for, you must set the appropriate filter already on the network level by using FILTCFG. With static routes/services, further make sure that you only configured those remote servers/services on your router that are required for the networking processes that shall run over ISDN with the remote site. This is an additional important method you can apply on the network level to decrease the possibility of unnecessary packets to be generated for a remote server/service.

- **Frequent call set-up due to ISDN security features and "training" time required for other features to get active**

Third, due to the fact that all ISDN Interface and ISDN Call Destination Configurations are always negotiated first with the respective remote site during initial logical ISDN connection set-up, Security Call-Back is for example consequently performed each time a remote site initially dials up the respective ISDN interface on your router to set up a connection, the B channel is cleared and the remote site is dialed back, resulting in charges accruing at your site for the call back. Besides, some features require a training time to get active. For example Recall Request does not apply for initial call set-up. Thus, when your router initially dials up a remote site and you configured Recall Request to have the remote site dial you back and assume the charges for the connection, the remote site will not do so for this first incoming call from your site but only for all subsequent incoming calls from your site. Other features that require "training time" and are only advantageous if a logical ISDN connection to a remote site is up are Self-Learning Inactivity Timeout or SPX Spoofing.

- **Two configurations that may increase the possibility of critical situations**

First, the more call destinations you configure to different remote sites over a single ISDN interface without taking care about the network and ISDN-specific behavior, the higher the possibility that a networking process gets interrupted because the data cannot be transfered to all sites and the higher the possibility of frequent call set-ups. Second, setting Disconnect Timeout to the same value as Inactivity Timeout has the advantage of a high ISDN interface availability for multiple connections, but without taking care about the network and ISDN-specific behavior, the chance of frequent call set-ups increases as well, since all the ISDN-specific features especially implemented with NetWare MultiProtocol Router for ISDN to keep ISDN lines physically down, such as Watchdog Spoofing, SPX Spoofing and IPX Message Filter, can only be active for a very short time frame or cannot be activated at all.

The NetWare MultiProtocol Router for ISDN supports both, static and dynamic ISDN interface usage for classic WAN set-up and for dial-around scenarios and treats ISDN lines exactly the way you configured your networks and the ISDN-specific features. The above explanations were given here to make you aware of basics on network and ISDN behavior that you have to consider when deciding to use ISDN interfaces dynamically. Keep these specifics in mind when designing your WAN to avoid unnecessary ISDN connection charges, irrespective of whether you use only one or all ISDN interfaces dynamically.

Related Products and Options

The NetWare MultiProtocol Router for ISDN is based on the NetWare operating system. This allows unmatched scalability and flexibility when further networking needs have to be met, since NetWare MultiProtocol Router for ISDN can be installed together with other services on a single NetWare server. A survey on possible networking extensions is given below.

Remote Node Access over ISDN

The NetWare MultiProtocol Router for ISDN allows stand-alone PCs, laptops, notebooks or palmtops to dial into the LAN over terrestrial ISDN or GSM-based cellular networks in order to become remote nodes on the LAN. Remote nodes can use any servers, services and resources of the LAN over ISDN - in the same way as locally connected PCs use them. On the stand-alones, a remote node software and ISDN adapter, for example AVM NetWAYS/ISDN together with an AVM ISDN-Controller or any PPP-compliant product combination for remote nodes, is required.

In addition to providing the server component for remote node access, NetWare MultiProtocol Router for ISDN 3.1 also includes a single-user license of AVM´s remote node product NetWAYS/ISDN in the latest version 3.0 for Windows 95 and Windows NT. NetWAYS/ISDN supports both, IPX and TCP/IP, and together with any of AVM´s ISDN-Controllers for Basic Rate Interface or AVM´s Mobile ISDN-Controller M1 provides full-featured remote node access to the LAN.

But besides NetWAYS/ISDN, you can use any remote node product supporting IPX, TCP/IP or AppleTalk and the PPP over ISDN protocol for dial-up.

Routing Extension

The NetWare MultiProtocol Router for ISDN is dedicated to ISDN and provides extensive ISDN support and features. To extend routing capabilities beyond ISDN, it can also be combined with Novell´s WAN·Extensions 3.1 product, offering X.25, Frame Relay and ATM support, or with Novell´s SNA·Extensions 3.1 product, offering DLSw and multiprotocol routing across SNA backbones.

Communications and Host Connectivity Software

Since the NetWare MultiProtocol Router for ISDN can also be installed on a NetWare file server, it can run along with file and print services as well as with other services, such as Novell´s NetWare for SAA software for example, if client-to-host connectivity is required, or AVM´s NetWare Connect for ISDN software and one or more additional ISDN-Controllers, if access to remote services and resources from clients in or outside the LAN is required.

ISDN Management Software

The NetWare MultiProtocol Router for ISDN itself provides access to extensive ISDN-specific information on the use of ISDN links, ISDN-Controllers, the ISDN network itself over various NetWare-based utilities as well as over any SNMP-based network management consoles. For integrated management of all ISDN activities of the NetWare MultiProtocol Router for ISDN under Novell´s Network Management Software™ (NMS) or the joint Novell/Intel product ManageWise™, AVM´s MPR for ISDN Router Manager software can be used. In this case, the NetWare MultiProtocol Router for ISDN software is extended by the Router Agent software, and the ISDN management console, a so-called snap-in module, is added to the network management console software installed on a client in the LAN.

ADT - A CICC Application

ADT by LANtana, Ahrensburg, Germany, is an application which uses the CICC function of NetWare MultiProtocol Router for ISDN for automatic and time-controlled file transfer. The user defines so-called transfer sources including the required transfer information, such as the transfer time. By defining the transfer time (for example during the night), large amounts of data can be transferred in a cost-efficient way.

At the configured transfer time, ADT first establishes an ISDN connection between your NetWare MultiProtocol Router for ISDN to another NetWare MultiProtocol Router for ISDN. Then, the program logs into a server in the remote LAN and, if login was successful and the server granted respective rights, transfers the selected files. After wards, ADT logs out of the server and clears down the connection between the routers.

Further Product Options

CAPIMGR:

NetWare MultiProtocol Router for ISDN includes the CAPIMGR software, but does not make use of it. It exclusively uses AVM´s ISDN-Controllers and CAPI and provides full-featured ISDN support. Thus, ignore all ISDN descriptions in the *NetWare MultiProtocol Router 3.1* guides coming with the product, since they do not apply for NetWare MultiProtocol Router for ISDN 3.1.

However, the CAPIMGR is included with NetWare MultiProtocol Router for ISDN 3.1 and can be used for network applications running on the same PC but on a different ISDN adapter than the NetWare MultiProtocol Router for ISDN. Note that this option is not actively supported by AVM. If you have any questions, contact the manufacturer of the application you want to use.

PPP X.21-Stack:

Novell´s PPP implementation (X.21) for analog lines is included in NetWare MultiProtocol Router for ISDN 3.1. However, since the NetWare MultiProtocol Router for ISDN is dedicated to ISDN, this PPP implementation not be loaded by default, and support for the use of lines other that ISDN lines with the NetWare MultiProtocol Router for ISDN will be restricted. If you want to use the Novell PPP implementation to connect via one of the interfaces RS.232, V.35, RS.422, X.21, you must use the *NetWare MultiProtocol Router 3.1* manuals (hard copy and on CD) provided with the NetWare Multi-Protocol Router for ISDN 3.1 product for information on interface and line types, configuration and all further issues of usage of synchronous or asynchronous communication lines with the PPP implementation to interconnect LANs.

NetWare Mobile IPX:

Novell´s NetWare Mobile IPX software is also provided with NetWare MultiProtocol Router for ISDN 3.1. It consists of router and mobile client components that work in concert to shield users from the protocol and network-layer interruptions that occur when a user changes network interfaces or locations during a network session.

For information on this option, refer to the *NetWare MultiProtocol Router 3.1* manuals which are provided as a hard copy and on CD-ROM.

Product Versions

The NetWare MultiProtocol Router for ISDN 3.1 is available in the following versions:

- 2 BRI for up to four ISDN ports,
- 4 BRI for up to 8 ISDN ports, and
- PRI for up to 36 ISDN ports

Upgrade products are available for former versions of NetWare MultiProtocol Router for ISDN (v2.0, v2.1, v2.11 and v3.0) as well as within the current version (2 BRI -> 4 BRI; 2 BRI/4BRI -> PRI). For upgrading information, refer to the special note included with your upgrade product.

Configuration and Management

With NetWare MultiProtocol Router for ISDN 3.1, first-time installation and configuration becomes easier for standard WANs. It offers several preconfigured scenarios for both IPX and TCP/IP that should apply for most standard network environments. You simply select the file that most closely fits your network and copy it to the router. Then, you have to enter ISDN and network numbers - and that is it.

For more complex networks and fine-tuning, configuration can be effected as usual through INETCFG. Further information about INETCFG, about configuration and management is provided in the *NetWare MultiProtocol Router 3.1 Configuration* guide and is therefore not repeated here.

The intelligent snap-in helps to prevent critical situations that can be caused by misconfiguration.

To manage the router from an SNMP-based management console, SNMP support for ISDN (MPR4ISDN.MIB) is included as well.

The NetWare-based and menu-assisted ISDN Console (ISDNCON.NLM) provides detailed information on ISDN connections and on ISDN-Controllers and their interfaces. Use ISDN Console instead of MONITOR. ISDN Console offers online 1h and 24h statistics on all ISDN connections established during that period, and allows you to extract ISDN line management information and ISDN error messages and to store such information. For detailed information, refer to Chapter 18, "Monitoring ISDN Connections".

chapter 2 Preparing to Install

This chapter describes the system requirements and installation procedures for NetWare® MultiProtocol Router™ for ISDN 3.1 software.

The NetWare MultiProtocol Router for ISDN 3.1 software can be installed on either of the following platforms:

- NetWare 3.12 or NetWare 4.1, as a combined router and server
- NetWare 3.12 or NetWare 4.1, as a dedicated router

You must install or upgrade to NetWare 3.12 or NetWare 4.1 before you install the router software.

Note

NetWare 3.12 Runtime™ software (a special two-user version) and NetWare 4.1 (also a special two-user version) software are included with the NetWare MultiProtocol Router for ISDN 3.1 software; you do not have to purchase them separately.

Warning

The NetWare 4.1 platform does not provide backward compatibility for NetWare MultiProtocol Router for ISDN 2.x software.

This chapter describes preparations that must be made prior to installing NetWare 3.12 Runtime (or NetWare 4.1) and NetWare MultiProtocol Router for ISDN 3.1 software. It contains the following sections:

- "What you need" on page 43
- "Setting Up the Hardware" on page 51
- "Where to Go from Here" on page 54

What You Need

Hardware Requirements

Checklist

You need the following hardware to install MultiProtocol Router for ISDN 3.1:

- A PC (or PC compatible) with a 386 or 486 (SX or DX) or higher processor.
- The system must have 16 MB of RAM to run NetWare 3.12 Runtime (or NetWare 4.1) and the NetWare MultiProtocol Router for ISDN 3.1 software.
- A hard disk with sufficient storage space for your network. The minimum amount of storage space required is 90 MB: 15 MB for a DOS partition plus 75 MB for a NetWare partition containing the SYS: volume.

  However, if all NetWare file groups are copied to the server, you will need a minimum of 100 MB for the SYS: volume. A larger NetWare partition is therefore recommended.

  For more information on hard disk space requirements, refer to the NetWare MultiProtocol Router 3.1 Release Notes, p. 17.
- At least one network board.
- Network cabling (Ethernet, token ring, FDDI, ARCNET, baseband, and so on).
- A CD-ROM drive that can read ISO 9660 formatted CD-ROM disks.
- At least one ISDN-Controller. Possible are:
  - one to four AVM ISDN-Controllers B1, B1 PCI*, B1-MCA, PCMCIA B, or
  - one to four AVM Mobile ISDN-Controllers M1 or M2*
  - one to four AVM ISDN-Controller T1 or T1-B*, or
  - one AVM ISDN-Controller T1 or T1-B and up to three AVM ISDN-Controllers B1.

Note

If you want to install more than one AVM ISDN-Controller T1 or T1-B*, please contact AVM for more information.

Important

AVM ISDN-Controllers marked with an asterisk (*) were not available as this manual was printed. Release of these products is scheduled for the third quarter of 1996. For more information, contact your distributor or AVM.

Software Requirements

NetWare MultiProtocol Router for ISDN 3.1 is based on the NetWare Network Operating System (NOS) and is compatible with NetWare 3.12 and NetWare 4.1. For your convenience in building standalone routers, NetWare MultiProtocol Router for ISDN 3.1 includes Novell® DOS™ software, NetWare 3.12 Runtime, and NetWare 4.1 (two-user version); however, you can also install NetWare MultiProtocol Router for ISDN 3.1 on a server or router that is already configured with NetWare 3.12 or NetWare 4.1

Important

If the server you are upgrading has a NetWare license of more that two users and you do not want to downgrade the number of users on that server to two, you *must* get a NetWare license with the appropriate number of users for that server before installing NetWare MultiProtocol Router for ISDN 3.1.

If you are upgrading a multi-user version of NetWare 4.0x to NetWare 4.1, once you have a license with the number of users you want, you can use the NetWare 4.1 installation to upgrade your version of NetWare. When the installation program prompts you for a License Disk, insert the License Disk containing the correct number of users.

Warning

In some circumstances, installing to NetWare 4.1 more than once on the same server might cause you to have duplicate binds in the INETCFG database. If when using INETCFG you notice duplicate binds, delete the duplicates. Selecting one of the duplicates might cause the server to abend.

NetWare MultiProtocol Router for ISDN 3.1 can also be used in combination with other NLM files that run on NetWare 3.12 or NetWare 4.1. Some likely combinations include Novell´s WAN•Extensions 3.1 software, Novell´s NetWare for SAA software, AVM´s NetWare Connect for ISDN software and network management products. See section "Integration with Other Products" below for information on what to consider and which problems could arise.

To manage your NetWare MultiProtocol Router for ISDN 3.1, the MPR for ISDN Router Manager software may be purchased from AVM for integration in Novell´s ManageWise™ or NMS™ products.

To operate NetWare and NetWare MultiProtocol Router for ISDN 3.1, your system software should be configured as follows:

Checklist

- The system should start DOS from the hard disk. NetWare is started from DOS before it takes over the system hardware completely.

  It should run DR DOS® 6.0 software (or later) or Novell DOS 7.0 (or later).

  Alternately, it should run MS-DOS version 3.1 (or later) if it has an ISA or EISA bus.

  Alternately, it should run MS-DOS version 3.3 (or later) if it has a Micro Channel bus.

- The system must not load any modules that manage extended memory, such as HIMEM, QEMM, or EMM386.

- The system must not load any modules that compress disk files, such as Disk Doubler.

- The system must not load any terminate-and-stay-resident (TSR) modules.

- The system should have at least 16 MB of RAM available if you plan to run NetWare 3.12 The system should have at least 16 MB of RAM available if you plan to run NetWare 3.12 Runtime (or NetWare 4.1), the NetWare MultiProtocol Router for ISDN 3.1 software, and another networking product.

Supplemental Files

Several supplemental files are included on the NetWare MultiProtocol Router for ISDN 3.1 CD-ROM. These supplemental files provide a variety of updates to non-NetWare MultiProtocol Router for ISDN 3.1 modules that corect problems and improve the performance of NetWare MultiProtocol Router for ISDN 3.1. These files include updates for tine synchronization and NDS synchronization, PBURST updates and IPX and SPX connectivity updates. For more information, refer to the *NetWare MultiProtocol Router 3.1 Release Notes*, pp. 36-41.

Interoperability Information

Compatibility with Other Products

♦ Former Versions of NetWare MultiProtocol Router for ISDN

The NetWare MultiProtocol Router for ISDN was introduced on the market at the end of 1992 with v2.0. NetWare MultiProtocol Router for ISDN 3.1 is compatible with all former version, i.e. NetWare MultiProtocol Router for ISDN v2.0, v2.1, v2.11 and v3.0. Of course, you can only use the features provided in both versions running at each end of the ISDN link.

Known items are for example:

Static routes/services, NLSP or Unnumbered IPX WAN links for an IPX connection or Unnumbered IP WAN links for a TCP/IP connection cannot be used for connections between version 3.1 and versions 2.x.

The OSI protocol is not supported with NetWare MultiProtocol Router for ISDN 3.1.

For D64S connections between version 3.1 and versions 3.0 and 2.x, a special solution is required, which is not inlcuded as standard. For more information, refer to the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*.

For "Vorbestellte Dauerwählverbindungen" (semipermanent connections within 1TR6) between version 3.1 and versions 3.1, 3.0 and 2.x, a special solution is required, which is not inlcuded as standard. For more information, refer to the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*.

♦ AVM NetWAYS/ISDN

AVM´s remote node software NetWAYS/ISDN was introduced to the market in the beginning of 1993 with v2.0. You can use NetWAYS/ISDN v2.0, 2.1 as well as the latest version 3.0, which is included with the NetWare MultiProtocol Router for ISDN 3.1, of NetWAYS/ISDN to dial in to the LAN via NetWare MultiProtocol Router for ISDN 3.1.

♦ NetWare Connect for ISDN / NetWare Connect

AVM´s NetWare Connect for ISDN was introduced to the market at the end of 1994 with version 1.0.

NetWare MultiProtocol Router for ISDN 3.1 can be installed on one server with NetWare Connect for ISDN and NetWare Connect version 1.0 and 2.0.

When installing NetWare MultiProtocol Router for ISDN 3.1 together with NetWare Connect or NetWare Connect for ISDN 1.0, refer to the NetWare MultiProtocol Router 3.1 Release Notes for information on problems with a new version of CSL (p. 28), with the NetWare Link/ X.25 feature of NetWare Connect (p. 31) and with the version of STREAMS.NLM (p. 33).

♦ AVM MPR for ISDN Router Manager

AVM´s MPR for ISDN Router Manager v1.0 can be used to manage NetWare MultiProtocol Router for ISDN 3.1. However, you have to use the latest version of the MPR for ISDN Router Agent. For more information, please contact AVM.

If you are running NetWare MultiProtocol Router for ISDN 3.1 as a combined server and router with other server-based products rather than as a standalone router, several issues must be accounted for .

♦ NetWare OSI Transport for X.400

NetWare MultiProtocol Router for ISDN 3.1 does not work with NetWare OSI Transport for X400, an add-on product to NetWare Global Messaging™ software. Do not install NetWare MultiProtocol Router for ISDN 3.1 software, if NetWare OSI Transport for X400is installed on your system.

♦ NetWare for OS/2

NetWare MultiProtocol Router for ISDN 3.1 software is incompatible with NetWare for OS/2. Do not install NetWare MultiProtocol Router for ISDN 3.1 software on a NetWare for OS/2 server.

♦ NetWare SFT III

NetWare MultiProtocol Router for ISDN 3.1 software does not operate on NetWare SFT III™ servers. Do not install NetWare Multi-Protocol Router for ISDN 3.1 software on a NetWare SFT III server.

- **NetWare for SAA**

For information on problems with NetWare for SAA 1.3b, refer to the NetWare MultiProtocol Router 3.1 Release Notes, pp. 28-29.

For information on problems with NetWare for SAA 2.0 and NetWare MultiProtocol Router for ISDN 3.1 on the same server, refer to the NetWare MultiProtocol Router 3.1 Release Notes, pp. 4-5 and pp. 29-30.

- **NetWare Management System**

The SNMP MIB definitions for IPX are not shipped with NetWare Management System™ (NMS™) 2.0b software. The MIB definition for IPX (in ASN.1 format) and the ISDN-related MIBs are on the NetWare MultiProtocol Router for ISDN 3.1 CD-ROM in the /IPXSERV/SUPP/REFMIBS directory. Install these MIBs to all systems running NMS 2.0b to display full information about any SNMP traps generated by the IPX protocol.

PPP Over ISDN

PPP over ISDN (in the following referred to as PPP) is intended to provide interoperability between routers of different manufacturers over ISDN based on internationally accepted and open standards, described in so-called Requests for Comment (RFCs). RFCs are issued by manufactureres and/or interest groups in the form of RFC drafts or informational RFCs and are ratified by the Internet Engineering Task Force (IETF).

For information on third-party router products that have been tested with NetWare MultiProtocol Router for ISDN 3.1, refer to the Technical Note included with the NetWare MultiProtocol Router for ISDN 3.1.

For information on whether or not your NetWare MultiProtocol Router for ISDN 3.1 will interoperate with a third-party router product, take the list of RFCs in Table 2-1 and check which of the listed RFCs are supported by the third-party product.

The same is true for service providers offering ISDN access via router products to any type of services, such as Internet Service Providers like EUnet in Europe for example. Ask them which router product they are using to provide ISDN access and which RFCs are used by the routers.

The following RFCs are supported by NetWare MultiProtocol Router for ISDN 3.1:

Table 2-1: Supported RFCs

Number	Title
RFC 1144	Compressing TCP/IP Headers
RFC 1332	The PPP Internet Protocol Control Protocol (IPCP)
RFC 1334	PPP Authentication Protocols (PAP and CHAP)
RFC 1378	The PPP AppleTalk Control Protocol (ATCP)
RFC 1552	The PPP Internetwork Packet Exchange Protocol (IPXCP), exclusively for remote node access
RFC 1553	Compressing IPX Headers Over WAN Media (CIPX)
RFC 1570	PPP LCP Extensions (incl. callback option)
RFC 1618	PPP over ISDN
RFC 1634	Novell IPX Over Various WAN Media (IPXWAN)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1662	PPP in HDLC Framing
RFC 1717	The PPP Multilink Protocol (MP)
RFC 1877	IPCP Extensions for Name Server Addresses

Since, as of writing, standards for some of the internetworking features provided by the NetWare MultiProtocol Router for ISDN 3.1 do not yet exist or are still being developed, the following differences to the AVM Proprietary protocol apply:

- Inactivity Timeout and Self-Learning Timeout:

  As of writing, PPP does not include a method to differentiate between logical and underlying pyhsical disconnection of an ISDN link. Thus, when an ISDN connection is cleared due to expiration of the Inactivity Timeout, the physical and logical connection are cleared at the same time. This is why you should set the Disconnect Timeout to "Same as Inactivity Timeout".

- Spoofing mechanisms:

  Since all parameter negotiations are cleared when the logical connection is disestablished, the spoofing mechanisms on the ISDN driver level have no meaning for PPP over ISDN.

However, spoofing mechanisms on the network protocol level, such as Watchdog Spoofing and SPX Spoofing for on-demand IPX connections, can be used with PPP.

- Origination Subaddress and Destination Subaddress:

  They have no meaning for PPP. Per default, they are set to 1.

- Compression (according to V.42bis) cannot be used.
- Security Call-Back cannot be used.
- Encryption cannot be used.

Important

Because of the differences listed above, PPP should never be used for connections between NetWare MultiProtocol Routers for ISDN 3.1 and NetWare MultiProtocol Router for ISDN 3.1 and AVM´s NetWAYS/ISDN. Use PPP over ISDN only for connections to remote routers from other manufacturers.

Setting Up the Hardware

Calculate Memory (RAM) Requirement

Calculate the memory (RAM) requirement for your server /router as follows:

- For each loaded ISDN interface, allow for 2.5 KB of RAM.
- For each active ISDN connection, allow for 2.0 KB of RAM.
- For each active remote node, allow for 6 KB of RAM.

NetWare MultiProtocol Router for ISDN 3.1

- Can be installed directly at public ISDN accesses as well as through any ISDN-compatible PBX that supports BRI (S_0) or PRI (S_{2M}) and one of the supported ISDN D channel protocols .
- Supports ISDN Multipoint access and Point-to-Point access.
- Supports MSNs, EAZs and SPIDs at Multipoint accesses.
- Supports Direct Dial In (DDI) at Point-to-Point accesses.
- Supports Hunt Group Numbers at Point-to Point accesses with all D channel protocols except for D64S, DS01, DS02 and GSM.

Prepare for ISDN Access

Before installing your ISDN-Controller(s), check the following:

Checklist

- Normally, the transfer mode "unrestricted digital information", which stands for data transmission (instead of, e.g. voice transmission) and allows data transmission over ISDN, is provided by standard for every ISDN access. To reassure that this transfer mode has been enabled for your ISDN access, please check your order form for your ISDN access or ISDN accesses, or contact your local PTT's office.
- Check with your local PTT whether Advice On Charge During Call (AOCD) is enabled at your ISDN access. This is required for a number of functions provided with the NetWare MultiProtocol Router for ISDN.

Install ISDN-Controllers

Install, configure and test your AVM ISDN-Controller(s) as described in the respective ISDN-Controller manual.

If you want to install more than one ISDN-Controller, make sure that each ISDN-Controller has a unique I/O base address.

Write down all settings (PC bus parameters, such as I/O addresses and slot numbers) and plug the ISDN-Controllers into the server/router PC. You will have to provide this information when configuring the ISDN-Controllers later.

Important

If you are using AVM ISDN-Controllers PCMCIA B or Mobile ISDN-Controllers M1 or M2, make sure that the card and socket services are enabled. For information on how to do this, refer to your computer manual.

Test Your ISDN-Controllers

Use the test software provided with the AVM ISDN-Controllers to reassure that you installed the ISDN-Controllers properly and that your ISDN access is working:

- Use the test programs to verify that your ISDN-Controller is correctly installed and configured and whether it can be addressed by your PC.

- Use the CONNECT file transfer program to test whether you are able to receive incoming calls and to make outgoing calls, especially when a Private Branch Exchange is used.

  If you have D64S lines, you should use a separate .T4 file for testing with the CONNECT program. This file, B1CBASE.T4, is included on the software CD-ROM in the directory \D64S. Set the following values in the CONNECT.CFG on both sides: EAZ 1 on your local side and EAZ 2 on the remote site. Use these numbers when dialing with the CONNECT software.

For more information, refer to the manual(s) coming with your AVM ISDN-Controller.

Recording Hardware Configuration Information

To avoid hardware conflicts in your networks and to have important configuration information at hand, you should record the following information on a router worksheet:

- ISDN-Controllers: I/O address, interrupt request level (IRQ) for computers with ISA/EISA architecture, slot number for computers with EISA/MCA bus, and the D channel protocol provided at your ISDN access.
- Local numbers: all numbers describing the way the ISDN-Controller(s) is (are) connected to your local ISDN access, i.e. the parameters International Dialing Prefix, Country Code, Area Code, ISDN subscriber number and, when a PBX is used, PBX Extension and PBX Outside Line Access, and, in particular situations, EAZ, MSN or SPIDs.
- Remote numbers: for each remote site you want to set up connections to, you will have to specify the parameters ISDN Number (maximally including PBX Outside Line Access, International Dialing Prefix, Country Code, Area Code, ISDN Number and, if a PBX is used, the PBX Extension to reach the ISDN-Controller at the remote site) and Subaddress.

Also refer to the *NetWare MultiProtocol Router 3.1 Installation guide*, pp. 12-13 for further details on hardware configuration information.

Where to Go from Here

With the initial hardware preparation completed, you are ready to upgrade or install the NetWare operating system, as follows:

Note

For information on upgrading from versions 2.0, 2.1, 2.11 and 3.0 to version 3.1 of the NetWare MultiProtocol Router for ISDN, refer to the special upgrade manual coming with your upgrade product.

Note

If your system already has NetWare 3.12 or NetWare 4.1 software installed, you should go directly to Chapter 3, "Installing NetWare MultiProtocol Router for ISDN 3.1."

Installation of the NetWare operating system is not described in this Guide. You have to refer to the *NetWare MultiProtocol Router 3.1 Installation* guide for information on this topic. **Afterwards, come back to Chapter 3 of this Guide to install NetWare MultiProtocol Router for ISDN 3.1 !**

- If you want to install NetWare 3.12 Runtime for the first time, go to "Installing NetWare 3.12" on p. 99 of the *NetWare MultiProtocol Router 3.1 Installation* guide.

- If you want to upgrade an existing server/router from NetWare 3.x or NetWare 4.x to NetWare 4.1 (two-user version), go to "Upgrading to NetWare 4.1" on p. 117 of the *NetWare MultiProtocol Router 3.1 Installation* guide.

Warning

If your system has NetWare 3.x and NetWare MultiProtocol Router for ISDN 2.x installed, upgrading to NetWare 4.1 will prevent NetWare MultiProtocol Router for ISDN 2.x from functioning. Therefore, you should always upgrade to NetWare 4.1 and upgrade to NetWare MultiProtocol Router for ISDN 3.1 at the same time. Do not terminate the integrated INSTALL program after upgrading to NetWare 4.1. Refer to the special upgrade note coming with your upgrade product for more information on this topic.

- If you want to install NetWare 4.1 (two-user version) for the first time, go to "Installing NetWare 4.1" on p. 113 of the *NetWare MultiProtocol Router 3.1 Installation* guide.

chapter 3

Installing NetWare MultiProtocol Router for ISDN 3.1

This chapter tells you how to install the NetWare® MultiProtocol Router™ for ISDN 3.1 software on a local and on remote servers.

For remote and multiple server installation, see "Remote Installation and Configuration" later in this Chapter.

If you are doing a first-time installation, you must have

Checklist

- ♦ Installed LAN boards

  Refer to your LAN board manual for installation information.

- ♦ Installed one or more ISDN-Controller(s)

  Refer to your ISDN-Controller manual and the information in Chapter 2, "Prepare for ISDN Access", of this Guide.

- ♦ Installed the NetWare operating system

  Refer to "Where to Go from Here" on p. 54 of this Guide for information on where to find installation instructions for the NetWare operating system.

This chapter contains the following sections:

- "Installation Setup" on page 56
- "Installing NetWare MultiProtocol Router for ISDN on a Local Server" on page 59
- "Remote Installation and Configuration" on page 63
- "Deinstallation" on page 70

Important

For information on upgrading from versions 2.0, 2.1, 2.11 and 3.0 to version 3.1 of the NetWare MultiProtocol Router for ISDN, refer to the special upgrading manual coming with your upgrade product.

Important

For information on interoperability with other products and PPP over ISDN, refer to Chapter 2, "Preparing to Install" of this Guide.

If you are installing any other Novell® products, do so before installing the NetWare MultiProtocol Router for ISDN 3.1 software.

If you have the IPX™ Upgrade for NetWare Servers Beta software running NLSP™ (NetWare Link Services Protocol™) software installed anywhere on your network, you must upgrade those servers to IPX Upgrade for NetWare Servers 1.1 . Do this before installing NetWare MultiProtocol Router for ISDN 3.1 or IPX Upgrade for NetWare Servers 1.1 software on any other server on the network.

Installation Setup

There are several options for installing NetWare MultiProtocol Router for ISDN 3.1:

Type of installation:

- Local - Install to the local server.
- Remote - Install from a local server or client to a remote server.

Media type:

You can :

- Copy the NetWare MultiProtocol Router for ISDN 3.1 software to a local DOS partition.

  See below for instructions.
- Copy the NetWare MultiProtocol Router for ISDN 3.1 software to the SYS: volume of a NetWare server.

  See below for instructions.
- Mount the CD-ROM drive as a local DOS device and install directly from CD-ROM.
- Mount the CD-ROM drive as a NetWare volume and install directly from CD-ROM.

  For information on mounting a CD-ROM drive as a NetWare volume, refer to Appendix A of the *NetWare MultiProtocol Router 3.1 Installation* guide, "Mounting a CD-ROM as a NetWare Volume."

Copying the NetWare MultiProtocol Router for ISDN 3.1 Files to a Local DOS Partition

Procedure

1. **Bring down the server by entering the following commands at the system console prompt:**

```
down
exit
```

2. **Copy the NetWare MultiProtocol Router for ISDN software onto the DOS hard disk.**

   You must create directories on the server's hard disk to contain the installation files temporarily.

   2a. **Insert the *NetWare MultiProtocol Router for ISDN 3.1* CD-ROM into the drive.**

   2b. **Create a main directory on the hard disk called *NWMPRI31*.**

   2c. **Copy the files from the CD-ROM to the directory.**

   In the following command example, the NWMPRI31 directory is already created and the CD-ROM drive is designated as drive E:.

```
> xcopy e:\NWMPRI31\*.* c:\NWMPRI31 /s /e /v
```

   Because the files on the installation CD-ROM are located in subdirectories, you must use the XCOPY command with the /s option when copying files to the hard disk.

3. **Complete the rest of the installation by preceding to "Installing NetWare MultiProtocol Router for ISDN on a Local Server" or "Installing NetWare MultiProtocol Router for ISDN on a Remote Server" later in this Chapter.**

Copying the NetWare MultiProtocol Router for ISDN Files to a Local NetWare Volume

To install NetWare MultiProtocol Router for ISDN files from the NetWare volume of your local server's hard disk, complete the following steps:

Procedure

1. **Log in from a workstation (equipped with a CD-ROM drive) that is attached to the server.**

   You must log in as a user with enough privileges to create directories where you want to copy the files.

2. **Create a directory on the server’s hard disk to copy the NetWare MultiProtocol Router for ISDN files.**

   Create a main directory called *NWMPRI31*.

3. **Map a drive to the directory you created.**

   For example, if NWMPRI31 is the product directory you created, and it is located on the SYS: volume at the same level as the SYSTEM directory, use the following command:

   ```
   > map j:=sys:\nwmpri31
   ```

4. **Copy the NetWare MultiProtocol Router for ISDN software.**

   4a. **Insert the *NetWare MultiProtocol Router for ISDN 3.1* CD-ROM into the drive, and copy the contents of the CD-ROM to the NWMPRI31 directory.**

   For example, you would enter the following command at the DOS prompt to copy the contents of the CD-ROM to the NWMPRI31 directory:

   ```
   > ncopy e:\NWMPRI31\*.* J: /s /e /v
   ```

   Because the files on the installation CD-ROM are located in subdirectories, you must use the NCOPY command with the /s option when copying files to the hard disk.

   You can perform the remainder of these steps from the server console, or you can use RCONSOLE from the workstation. Refer to your NetWare documentation for more information about RCONSOLE. However, the license diskette must be physically available at the server’s diskette drive.

5. **Complete the rest of the installation by preceding to “Installing NetWare MultiProtocol Router for ISDN on a Local Server” or "Installing NetWare MultiProtocol Router for ISDN on a Remote Server" later in this Chapter.**

Installing NetWare MultiProtocol Router for ISDN on a Local Server

Complete the steps described in this procedure to install NetWare MultiProtocol Router for ISDN 3.1 on a local server / router. For online help, press <F1>.

Procedure

1. **Load the INSTALL program by typyng the following command at the NetWare server system console prompt:**

   ```
   LOAD INSTALL <Enter>
   ```

   The *Installation Options* menu appears.

2. **From the *Installation Options* menu, select *Product Options*, then press** <Enter>**.**

   If you are installing on an existing NetWare 3.12 server / router, a list of the currently installed products (if any) is displayed.

   If you are installing on an existing NetWare 4.1 server / router, a menu labeled *Other Installation Actions* is displayed. Select the *View/Configure/Remove* installed products option and press <Enter>. A list of currently installed products (if any) is displayed.

3. **To install a new product, press** <Ins>**.**

4. **Specify the correct path from which to load the source files.**

Table 3-1:
Specifying INSTALL path names

If you...	Perform the following...
installed the CD-ROM as a local DOS device	Enter the drive letter corresponding to the CD-ROM, for example e:\NWMPR31\INSTALL.
copied the files to the DOS partition of a hard disk	Enter the letter of the drive and the name of the path where you copied the software; for example, C:\NWMPR31\INSTALL.
installed the CD-ROM as a local NetWare volume	Enter the NetWare path corresponding to the CD-ROM, for example, NWMPR31:NWMPR31\INSTALL.
copied the files to a local NetWare SYS volume	Enter the volume and the path where you've copied the software; for example, SYS:\NWMPR31\INSTALL.

5. **From the *Installation Options* menu, select *Install Product*.**

   An *Install to Servers* menu displays the local server name.

6. **Select *Yes* to begin the installation.**

7. **You are now asked whether you want to install preconfigured files to the local server.**

   If you want to install one of the preconfigurations delivered with the NetWare MultiProtocol Router for ISDN, refer to the *Quick Installation and Setup Guide* for information on the files. Choose one, select *Yes* at this prompt and specify the path to install it.

   If you have some experience with NetWare MultiProtocol Router for ISDN and prepared a configuration you want to install, select *Yes*, insert your site-specific diskette, and specify a drive, if other than the default.

   If you want to install the preconfiguration later, select *No* and proceed to Step 8.

8. **To install the license, load the LICENSE diskette, or enter the location of the license file.**

9. **When the NetWare MultiProtocol Router for ISDN 3.1 source files have been copied, the following message is displayed:**

   ```
   "Installation was successful. Bring down and
   restart each server on which you installed the
   software to ensure that it uses the newest NLM
   files."
   ```

10. **Press** <Enter> **to continue.**

    The list of *Currently Installed Products* is displayed. Verify that the version of the NetWare MultiProtocol Router for ISDN 3.1 software that you just installed is displayed in this list.

11. **From the *Installation Options* menu, select *Exit*, then respond *Yes* to the prompt to exit the product installation.**

12. **For NetWare 4.1, use** <Esc> **to return to the *Other Installation Actions* menu. Select *Return* to the previous menu, then Exit.**

    The newly installed version of NetWare MultiProtocol Router for ISDN 3.1 is displayed in the list of *Currently Installed Products*.

13. **At the server console prompt, type**

```
DOWN <Enter>
EXIT <Enter>
```

14. **Restart NetWare from the DOS prompt by typing**

```
SERVER <Enter>
```

15. **Continue with "Editing the STARTUP.NCF File."**

Editing the STARTUP.NCF File

To edit the STARTUP.NCF file, complete the following steps:

Procedure

1. **At the NetWare server system console prompt, type**

```
LOAD INSTALL <Enter>
```

The *Installation Options* menu appears.

On a NetWare 3.12 server, select *System Options*, then press <Enter>.

On a NetWare 4.x server, select *NCF Files Options*, then press <Enter>.

2. **Select *Edit STARTUP.NCF File*, then press** <Enter>**.**

Warning

Be sure you select Edit, and not Create, because a STARTUP.NCF file already exists. If you select Create, all information in the existing file is lost.

On a NetWare 3.12 server, the full path name of STARTUP.NCF is displayed.

On a NetWare 4.x server, only the drive and directory are displayed.

3. **Press <Enter> to accept the default, or specify a boot path location for the SERVER.EXE file.**

4. **Press** <Enter> **to view the contents of the file.**

Add the following lines to the end of the file:

```
SET MINIMUM PACKET RECEIVE BUFFERS=400

SET MAXIMUM PHYSICAL RECEIVE PACKET SIZE= <value>
```

The value of this parameter should be set to the largest value used by your LAN media or the largest value used by your applications, whichever is smaller. Typical values for different media types are shown in the following table.

Table 3-2:
Typical Values for Differnt Media Types:

Media Type	Value
Ethernet	1518
4 MB token ring	4530
16 MB token ring	4530
FDDI	4530
ARCNET	4202
LocalTalk	600
ISDN	4530

As you can see, ISDN is capable of handling packet sizes of up to 4530 Bytes. However, always enter the maximum value that the weakest link can handle.

Example: Ethernet used with ISDN
-> Enter 1518 for the "maximum physical receive packet size".

5. **Press** <Esc>**, select *Yes* to save your changes, then press** <Enter>**.**

   The *Available NCF Files Options* menu appears.

6. **Press** <Esc> **to return to the *Installation Options* menu.**

7. **From the *Installation Options* menu, select *Exit*, respond *Yes* to the prompt, then press** <Enter> **to exit the installation program.**

8. **At the server console prompt, type**

```
DOWN <Enter>

EXIT <Enter>
```

9. **Restart NetWare from the DOS prompt by typing**

```
SERVER <Enter>
```

The installation is complete. Go to Chapter 4, "Configuration Overview".

Remote Installation and Configuration

Remote installation is required when you want to install NetWare MultiProtocol Router for ISDN 3.1 on more than one server or when the server which you want to install the product on does not have a local CD-ROM or floppy disk drive.

Note

Remote installation over ISDN takes about 30 minutes!

Before performing a remote installation, the RSPAWN.NLM and the SPXS.NLM file must be copied from the CD-ROM directory, SUPPS\ALL, to the SYS:SYSTEM directory of the server from which you are installing and to all remote targets. If these files were previously loaded, you must unload them and reload the newer versions. These files can be loaded locally at the server prompt or remotely using RCONSOLE.

If the target servers are physically accessible, RSPAWN and SPXS can be loaded manually from the server prompt. After copying new versions of RSPAWN and SPXS to the SYS:SYSTEM directory, load the files manually by entering

```
UNLOAD RSPAWN

UNLOAD SPXS

LOAD RSPAWN
```

RSPAWN automatically loads SPXS.

Note

If SPXS does not unload, manually unload any NLM™ (NetWare Loadable Module™) files that depend on SPXS or down and restart the server.

Important

Please keep in mind that for remote installation, the RSPAWN service must not be filtered.

Loading RSPAWN and SPXS from RCONSOLE

To copy and load RSPAWN and SPXS remotely from a local NetWare workstation to a remote server, complete the following steps:

Procedure

1. **Run RCONSOLE.**

   If you are running a local NetWare 4.x server, the *Connection Type* menu appears. Whether you are installing on a remote server over a LAN medium or over ISDN, in either case select *SPX*.

   Important

   The files REMOTE.NLM and RSPX.NLM must be loaded on the remote server before you can open a remote session to it with RCONSOLE. If you are unfamiliar with RCONSOLE and are using NetWare 3.12, see *NetWare 3.12 System Administration*. If you are using NetWare 4.x, see *NetWare 4.0 Supervising the Network*.

   A window displays a list of available servers.

2. **To open a session, select a remote server from the list of available servers, then press** <Enter>**.**

3. **To display the RCONSOLE *Available Options* menu:**

   On a local NetWare 3.12 server, press the asterisk key (*) on the numeric keypad - not <Shift>+<8> - on the main keyboard.

   On a local NetWare 4.x server, press <Alt>+<F1>.

4. **From the *Available Options* menu, select *Transfer Files To Server*, then press** <Enter>**.**

5. **Copy the RSPAWN.NLM and SPXS.NLM files from the CD-ROM SUPPS\ALL directory to the SYS:\SYSTEM directory on the remote server.**

6. **Press** <Esc> **to return to the remote server console prompt.**

7. **From the remote server console prompt, unload old RSPAWN and SPXS files, and load the new versions by entering**

   ```
   UNLOAD RSPAWN

   UNLOAD SPXS

   LOAD RSPAWN
   ```

   RSPAWN automatically loads SPXS.

   Note

   If SPXS does not unload, manually unload any NLM™ (NetWare Loadable Module™) files that depend on SPXS or down and restart the server.

8. **To terminate the remote session:**

   For NetWare 3.x versions of RCONSOLE, press <Shift>+<Esc>, select *Yes* at the prompt, then press <Enter>.

   For NetWare 4.x versions of RCONSOLE, press <Alt>+<F2>, select *Yes* at the prompt, then press <Enter>.

9. **Press** <Esc> **and select *Yes* to exit RCONSOLE.**

10. **Continue the installation as described below.**

Installing NetWare MultiProtocol Router for ISDN 3.1 on a Remote Server

If you want to perform a remote installation on a NetWare 4.1 server from a NetWare 3.12 server, you must set the bindery context on the remote NetWare 4.1 server. If the NetWare 4.1 server does not have a bindery context set, the system will not accept a login attempt by any directory services user.

After loading RSPAWN and SPXS on the remote server, complete the following steps:

Procedure

1. **At the local server console prompt, type**

   ```
   LOAD INSTALL <Enter>
   ```

   The *Installation Options* menu appears.

2. **From the *Installation Options* menu, select *Product Options*, then press** <Enter>**.**

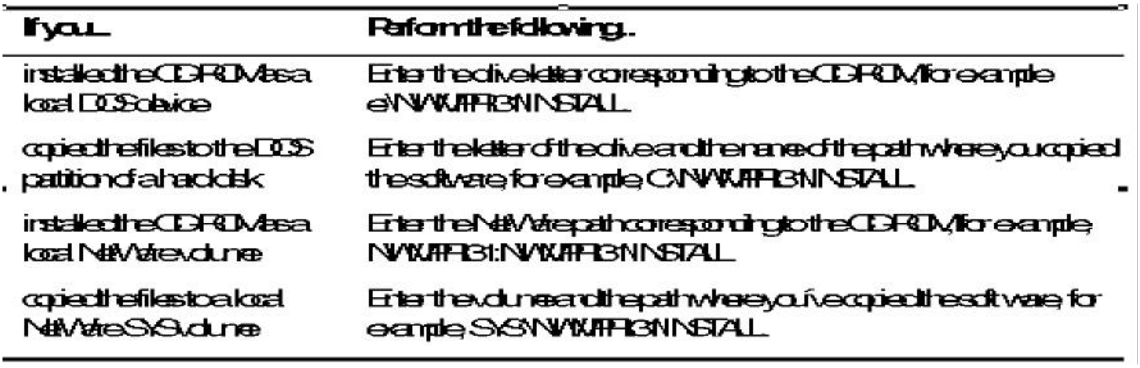
   If you are installing from a NetWare 3.12 server / router, a list of installed products (if any) is displayed.

   If you are installing from a NetWare 4.1 server / router, the *Other Installation Actions* menu appears. Select the View / Configure / Remove installed products option and press <Enter>. A list of currently installed products (if any) is displayed.

3. **To install a new product to install, press** <Ins>**.**

4. **Specify the correct path from which to load the source files.**

Table 3-4:
Specifying INSTALL path names



If you...	Perform the following...
installed the CD-ROM as a local DOS device	Enter the drive letter corresponding to the CD-ROM, for example e:\NWWUPR3\INSTALL
copied the files to the DOS partition of a hard disk	Enter the letter of the drive and the name of the path where you copied the software, for example, C:\NWWUPR3\INSTALL
installed the CD-ROM as a local NetWare volume	Enter the NetWare path corresponding to the CD-ROM, for example, NWWUPR31:NWWUPR3\INSTALL
copied the files to a local NetWare SYS volume	Enter the volume and the path where you´ve copied the software, for example, SYS:\NWWUPR3\INSTALL

5. **From the *Installation Options* menu, select *Install Product*.**

   An *Install to Servers* menu displays the local server name. The value in the title string reflects the number of servers to be installed.

   5a. **To modify the list of servers, press** <Ins> **to launch the *Available File Servers* menu. Edit the list using the following keys:**

   <Del> removes a server.

   <F5> marks a server to be added or removed.

   <Enter> adds marked servers to the list and begins the installation process.

6. **Select *Yes* to begin the installation.**

7. **Enter the Administrator´s name and password for each of the remote servers.**

8. **You are now asked whether you want to install preconfigured files to the remote servers.**

   If you want to install one of the preconfigurations delivered with the NetWare MultiProtocol Router for ISDN, refer to the *Quick Installation and Setup Guide* for information on the files. Choose one, select *Yes* at this prompt and specify the path to install it.

   If you have some experience with NetWare MultiProtocol Router for ISDN and prepared a configuration you want to install, select *Yes*, insert your site-specific diskette, and specify a drive, if other than the default.

If you want to install the preconfiguration later, select *No* and proceed to Step 8.

9. **To install the license, load the LICENSE diskette, or enter the location of the license file.**

10. **When all the NetWare MultiProtocol Router for ISDN 3.1 source files have been copied to the local system, a sequential connection is established to each of the remote servers.**

    If any of the selected servers do not have the correct version of RSPAWN installed, an error message is displayed. To continue, press <Esc>, load the correct version of rspawn on the remote server, and retry. For more information, see "Loading RSPAWN and SPXS from RCONSOLE" above.

11. **When all the NetWare MultiProtocol Router for ISDN 3.1 source files have been copied to all the selected servers, the following message is displayed:**

    ```
    "Installation was successful. Bring down and
    restart each server on which you installed the
    software to ensure that it uses the newest NLM
    files."
    ```

12. **Press** <Enter> **to continue.**

13. **From the *Installation Options* menu, select *Exit*, then respond *Yes* to the prompt to exit the product installation.**

    The newly installed version of NetWare MultiProtocol Router for ISDN 3.1 is displayed in the list of *Currently Installed Products*.

14. **For NetWare 4.1, use** <Esc> **to return to the *Other Installation Actions* menu. Select *Return to the previous* menu, then *Exit*.**

15. **Reboot the remote server. At the NetWare console prompt, type the following commands:**

    ```
    DOWN <Enter>

    EXIT <Enter>
    ```

Suggestion

You can also use a **reboot.ncf** file with the following lines:

```
remove dos
down
exit
```

Make sure, however, that the server is automatically restarted from the DOS prompt, i.e. that the ´server´ command is included in the autoexec.bat file.

16. Continue with "Editing STARTUP.NCF Remotely."

Editing STARTUP.NCF Remotely

Procedure

To edit the STARTUP.NCF file remotely from a local NetWare workstation, complete the following steps:

1. Run RCONSOLE.

If you are running a local NetWare 4.x server, the Connection Type menu appears. Whether you are installing on a remote server over a LAN medium or over ISDN, in either case select *SPX*.

Important

The files REMOTE.NLM and RSPX.NLM must be loaded on the remote server before you can open a remote session to it with RCONSOLE. If you are unfamiliar with RCONSOLE and are using NetWare 3.12, see NetWare 3.12 System Administration. If you are using NetWare 4.x, see NetWare 4.0 Supervising the Network.

A window displays the list of available servers.

2. To open a session, select a remote server from the list of available servers, then press <Enter>**.**

3. At the server or router console prompt, type

```
LOAD INSTALL <Enter>
```

On the remote NetWare 3.12 server, the *Installation Options* menu appears. Select *System Options*, then press <Enter>.

On the remote NetWare 4.x server, select *NCF Files Options*, then press <Enter>.

4. Select *Edit STARTUP.NCF File*, then press <Enter>**.**

Warning

Be sure you select Edit, and not Create, because a STARTUP.NCF file already exists. If you select Create, all information in the existing file is lost.

On the remote NetWare 3.12 server, a new window displays the full path name of STARTUP.NCF.

On the remote NetWare 4.x server, a new window displays the drive and directory.

5. **Press** <Enter> **to view the contents of the file.**

   Add the following lines to the end of the file:

```
SET MINIMUM PACKET RECEIVE BUFFERS=400
SET MAXIMUM PHYSICAL RECEIVE PACKET SIZE=<value>
```

   The value of this parameter should be set to the largest value used by your LAN media or the largest value used by your applications, whichever is less. Typical values for different media types are shown in the following table:

Table 3-5:
Typical Values for Different Media Types

Media Type	Value
Ethernet	1518
4 MB token ring	4530
16 MB token ring	4530
FDDI	4530
ARCNET	4202
LocalTalk	600
ISDN	4530

   As you can see, ISDN is capable of handling packet sizes of up to 4530 Bytes. However, always enter the maximum value that the weakest link can handle.

   Example: Ethernet used with ISDN
   -> Enter 1518 for the "maximum physical receive packet size".

6. **Press** <Esc>**, select *Yes* to save your changes, then press** <Enter> **to return to the *Available System Options* menu.**

7. **Press** <Esc> **to return to the *Installation Options* menu.**

8. **On the remote server, press** <Esc> **two times (on a NetWare 3.12 server) or three times (on a NetWare 4.x server) and select *Yes* to exit INSTALL.**

9. **At the server console prompt, type**

```
REMOVE DOS <Enter>
DOWN <Enter>
EXIT <Enter>
```

Suggestion

You can also use a **reboot.ncf** file with the following lines:
remove dos
down
exit
Make sure, however, that the server is automatically restarted from the DOS prompt, i.e. that the ´server´ command is included in the autoexec.bat file.

10. **To terminate the remote session:**

On a local NetWare 3.12 server, press <Shift>+<Esc>, select *Yes* at the prompt, then press <Enter> to return to the server console prompt.

On a local NetWare 4.x server, press <Alt>+<F2>, select *Yes* at the prompt, then press <Enter> to return to the server console prompt.

The installation is complete.

Go to Chapter 4, "Basic Design of ISDN-WANs and Configuration Overview" for an overview of all required configuration tasks.

Deinstallation

NetWare MultiProtocol Router for ISDN 3.1 can be deinstalled using INSTALL.NLM to remove product entries from the INSTALL.NLM database. Removing the entries does not remove files or rename the configuration. The router remains fully operational, and subsequent installations are not treated as upgrades.

chapter

4 Basic Design of ISDN-WANs and Configuration Overview

In this chapter, design and configuration issues for setting up WANs over ISDN are discussed.

At the end of the chapter, a configuration overview is given that lists all steps that are necessary for configuring the NetWare® Multi-Protocol™ Router for ISDN 3.1 and gives information on where to find the related instructions.

This chapter contains the following sections:

- "Routing Protocol or Static Routes - Basic Considerations" on page 65
- "Possible and Recommended Configurations for IPX" on page 72
- "Configuration Overview" on page 73

Routing Protocol or Static Routes - Basic Considerations

The NetWare MultiProtocol Router for ISDN enables you to decide for all routable protocols, i.e. for IPX, TCP/IP and AppleTalk, whether you want to route them over ISDN by using a routing protocol or by configuring static routes/services.

This decision can be made for each ISDN interface handling a connection. This offers you the flexibility to customize your ISDN connections according to two criteria: First, which applies best for the network protocol you want to route to a remote site, and second, which applies best to cover the nature of the remote site with regard to servers and services available, i.e. if it is of a more static or a more dynamic nature.

In the following, some general recommendations will be given. Afterwards, advantages and drawbacks of each of the two methods, static routes/services and routing protocol, are described and recommendations for the respective protocols and additional notes on when and how to implement classic WAN links and dial-around links will be given.

Important

For the non-routable protocols SNA and NetBIOS you cannot configure static routes, but can only use source route bridging. Therefore, SNA and NetBIOS are not discussed in the following sections.

General Recommendations

Fixed Tariffs

Whenever you use one of the ISDN accesses and line types that have fixed tariffs and are not charged by the duration of a connection, i.e. D64S, DS01, DS02, 1TR6 with "Vorbestellte Dauerwählverbindung" or TS 03 with "Semi Permanent Connection", you may choose whatever applies best in your opinion.

All considerations in this section apply for normal circuit-switched lines that are charged by the duration of each connection. They are intended give you indications for the best way to set up your WAN links in regard to cost-efficiency in this sense.

TPC/IP

When using TCP/IP, the general recommendation is to configure static routes instead of using RIP, RIP II or OSPF, irrespective of whether networks are of a static or dynamic nature. Using static routes is common with TCP/IP, and routing protocols involve exchange of routing information; the most critical is RIP exchanging routing information every 60 seconds.

Static Routes/Services

Using static routes instead of a routing protocol over ISDN always has the advantage that no routing and services information is exchanged over ISDN. The drawback is, that if servers and services that shall be available in the WAN change frequently, i.e. new servers, segments and services are added, removed, or their status changes, these changes have to be reflected in the static routes and services configuration of each router involved.

Choose Static Routes to Link Networks with Static "Nature"

When setting up your WAN links over ISDN, have a look at your LAN and the LANs that you wanto to interconnect over your router and decide whether they are of a more static or dynamic nature. Whenever they are more static, it is recommended to use static routes/service instead of a routing protocol to link them over ISDN, disregarding whether you use IPX, TCP/IP or AppleTalk.

Further recommendations that go together with static routes/services:

- First, configure only those routes/services of your local and of each remote site on your router that are required for your internetworking purposes
- Second, use FILTCFG to filter out single IPX nodes, IP hosts, NICs, packet types and for IP in additon IP services (e.g. telnet, ftp) that are on those routes you configured, but shall not gain access to remote sites over ISDN or be transmitted over ISDN. Note that for servers/services that only need to be available sometimes, it can be more comfortable if you configure the routes/services once and use FILTCFG to filter them out or let them pass through.

Classic and Dynamic ISDN Interface Usage with Static Routes/Services

The recommendation to use static routes/services further applies irrespective of whether you want to set up classic WAN links or use ISDN interfaces dynamically. The only difference is, that with dynamic ISDN interface usage, you will configure more than one Call Destination over an ISDN interface and will set the Disconnect Timeout for each of these Call Destinations to release the ISDN interface. Be aware that first, the Disconnect Timeout is the only method to release an ISDN interface that makes sense with static routes/services, and, further read through the section "Choose Routing Protocols to Link Networks With Dynamic ´Nature´" carefully to know about what you have to consider with dynamic ISDN interface usage.

Routing Protocols

With routing protocols, advantage and drawback are "turned around": Using a routing protocol instead of static routes/services over ISDN has the advantage that you do not have to configure routes/services manually (exchange of routing and services information is the task of routing protocols). Two drawbacks come up with routing protocols. First, routing tables or link stati need to be verified/updated over ISDN and, depending on the routing protocol implementation (distance vector or link state protocol for example), this is done very frequently. Second, the advantage that network changes are transmitted can get a drawback as well, because if servers and services that shall be available in the WAN change very frequently, ISDN lines are set up or kept up to transmit the changes. However, a closer look at the behavior each routing protocol is required, since various mechanisms are implemented with the distinct routing protocols to optimize their behaviour. These are discussed below together with recommendations on which routing protocol to use for which network protocol.

Note

This chapter does not discuss any of the tunneling possibilities, for example transport of IPX or AppleTalk (AURP) encapsulated/tunneled in TCP/IP. Further, the various routing protocols are not described to their full extend, but are only discussed in regard to what is important in conjunction with ISDN use.

Choose Routing Protocols to Link Networks with Dynamic "Nature"

When setting up your WAN links over ISDN, have a look at your LAN and the LANs that you wanto to interconnect over your router and decide whether they are of a more static or dynamic nature. Whenever they are more dynamic, it is more comfortable and therefore recommended to use a routing protocol to link them over ISDN, disregarding whether you use IPX or AppleTalk. For TCP/IP, the general recommendation to use static routes is still valid, but preferences can be made if you choose to use a routing protocol instead of static routes.

Recommendations that go together with the use of any of the routing protocols:

- Use FILTCFG to filter out routes/services, single IPX nodes, IP hosts, NICs, packet types and for IP in additon IP (e.g. telnet, ftp) that shall not gain access to remote sites over ISDN or be transmitted over ISDN.

Routing Protocol to Choose for the Respective Network Protocols

♦ IPX - RIP/SAP, NSLP

For IPX, the routing protocols RIP/SAP and NLSP are supported.

RIP/SAP is a distance vector-based routing protocol implementation. RIP/SAP consistently exchanges routing and services information, i.e. updates routing and services tables in a periodic manner. This is done per default every 60 seconds, whether changes appear or not, and, in addition, exchanges information each time a change occurs. The following mechanisms are implemented to reduce traffic produced by this routing protocol.

- RIP/SAP Periodic Update Timer

  With RIP/SAP Periodic Update Timer you can - and over ISDN you must - change the default of 60 seconds for exchange of routing and services information to a higher value, best to the max. value of 84 hours. However, since this would imply that network changes would as well only be updated every 84 hours and not at the time the change occurs, RIP/SAP on change is implemented as an underlying mechanism.

- RIP/SAP Only On Change mechanism

  This mechanism does not have to be configured, it is always active and guarantees that the network changes are transmitted whenever they occur. It works independend of the update of all routing and services tables defined through RIP/SAP Periodic Update Timer.

NLSP is a link state protocol implementation. NLSP exchanges routing and services information only when network changes occur. NSLP further uses Non Broadcast or WAN LSP Hello packets to reassure that the remote side of the link is available. The following mechanisms are implemented to reduce traffic produced by this routing protocol:

- Non Broadcast Hello Timer Interval

  The Non Broadcast Hello Timer Interval defines the frequency of WAN LSP Hello packets. This timer can be set per router. The default value is 20 seconds, but does not have to be changed if you decide to use NLSP instead of RIP/SAP or static routes, since LSP Hello Spoofing is provided.

- LSP Hello Spoofing

  With LSP Hello Spoofing, LSP Hello packets are not transmitted to the remote end of each NLSP link over ISDN, but are spoofed locally on each router.

NLSP is the more advanced routing protocol implementation, especially when compared in design with distance-vector protocol implementations, which are of older style technology. However, the following restriction must be considered:

- The current version of NLSP does not support interarea (level 2) routing, and routes or services cannot be filtered within a routing area but between areas at the area boundaries.

You can create routing areas by running RIP on the network interfaces that link the areas, and therefore filtering of routes and services over an ISDN link can be applied if NLSP is used in the LAN and RIP / SAP is used over ISDN. Thus, although NLSP is the more advanced routing protocol implementation, it has some drawbacks as of today and the RIP / SAP mechanisms described above overcome the major problem of this distance-vector protocol, i.e. the frequent update of routing tables and services. Therefore, when compared with IPX RIP / SAP, NLSP does not bring advantages over ISDN for most standard internetworking scenarios as of today.

Recommendation

For IPX over ISDN, IPX RIP / SAP is the recommended routing protocol.

♦ TCP/IP - RIP I, RIP II, EGP and OSPF

For TCP / IP, the routing protocols RIP I, RIP II, EGP and OSPF are supported.

RIP is a distance vector-based routing protocol implementation. RIP consistently exchanges routing information, i.e. updates routing tables in a periodic manner. This is done per default every 60 seconds, whether changes appear or not. No mechanisms are implemented to reduce traffic produced by this routing protocol. Thus, do not use RIP over ISDN if your connections are charged by connection time. RIP II is an extension of RIP allowing to transmit subnet information.

OSPF is a link state protocol implementation. OSPF exchanges routing information only when network changes occur. OSPF further uses OSPF Hello packets to reassure the remote side of the link is available. The following mechanism is implemented to reduce traffic produced by this routing protocol:

- OSPF Hello Timer

  The OSPF Hello Timer defines the frequency of OSPF Hello packets. This timer can be set per interface. You can - and over ISDN you must - change the default of 10 seconds to a higher value if you decide to use OSPF instead of static routes. The maximum value is approximatly 18 hours.

Recommendation

For TCP/IP over ISDN, the general recommendation is to use static routes. If you want to use a routing protocol instead, use of OSPF is recommended.

♦ AppleTalk - RTMP

For AppleTalk, the routing protocol RTMP is supported.

RTMP consistently exchanges routing information, i.e. updates routing tables in a periodic manner. This is done per default every 10 seconds, whether changes appear or. The following mechanism is implemented to reduce traffic produced by this routing protocol.

- RTMP Routing Update Timer

  With RTMP Routing Update Timer you can - and over ISDN you must - change the default of 10 seconds for exchange of routing information to a higher value, best to the max. value of 30 minutes.

Recommendation

For AppleTalk over ISDN, the general recommendation is to use static routes. If you want to use RTMP be aware that routing information is at least exchanged every 30 minutes.

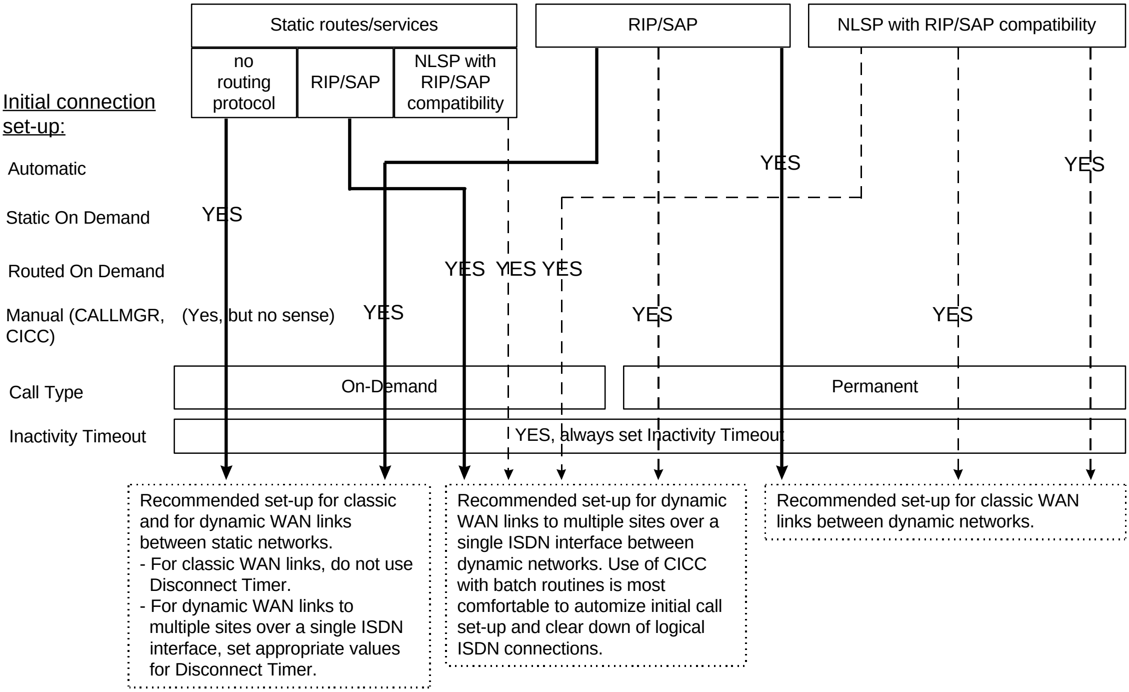
Classic and Dynamic ISDN Interface Usage with Routing Protocols

If you choose a routing protocol instead of static routes/services you can set up classic WAN links, of course. You can also use ISDN interfaces dynamically, but not the same way it can be done with static routes / services. When choosing classic WAN links and classic ISDN interface usage with a routing protocol, you never set a Disconnect Timeout. Besides that, you have different possibilities for configuring your Call Destinations. When choosing dynamic ISDN interface usage with a routing protocol, the methods for call set-up and clear-down are different when compared with the two methods that come with static routes / services, i.e. logical ISDN connection set-up by network protocol request and logical ISDN connection clear-down by Disconnect Timeout. With routing protocols, you use manual methods (CALLMGR on the router or via RCONSOLE) or, for IPX also batch routines (CICC from any IPX client or batch routines) for initial ISDN connection set-up. The remote site is only known to your local site after initial logical ISDN connection set-up, since at that time, routing protocol information is exchanged and tables maintaining routes and services are build the very first time. To clear down a logical ISDN connection and to release the ISDN interface, you can use CALLMGR, CICC or Disconnect Timeout. When the logical ISDN connection is cleared, the remote networks "disappear" as well, i.e. entries about routes and services of the remote network are cleared.

Possible and Recommended Configurations for IPX

Figure 4-1 shows the IPX protocol configuration and connection handling and should help you to get an overview of the configuration possibilities for IPX.

Figure 4-1:
IPX Protocol Configuration and Connection Handling



Recommended set-up for classic and for dynamic WAN links between static networks.
- For classic WAN links, do not use Disconnect Timer.
- For dynamic WAN links to multiple sites over a single ISDN interface, set appropriate values for Disconnect Timer.

Recommended set-up for dynamic WAN links to multiple sites over a single ISDN interface between dynamic networks. Use of CICC with batch routines is most comfortable to automize initial call set-up and clear down of logical ISDN connections.

Recommended set-up for classic WAN links between dynamic networks.

* IPX RIP/SAP is the only configuration possible for connections to NetWare MultiProtocol Router for ISDN v2.0, 2.1 or 2.11

Configuration Overview

Configuration of the NetWare MultiProtocol Router for ISDN 3.1 software involves tasks that are described partly in the *NetWare MultiProtocol Router 3.1* guides and in this NetWare MultiProtocol Router for ISDN 3.1 Installation and ISDN Configuration guide. ISDN-related tasks are only described in the latter.

In the following, all steps that are necessary for configuring the NetWare MultiProtocol Router for ISDN 3.1 are listed and information on where to find the related instructions is given.

Configuring for LAN Support

The steps involved in configuring NetWare MultiProtocol Router for ISDN 3.1 and a LAN adapter board are as follows. They are all described in the *NetWare MultiProtocol Router 3.1* guides:

1. Configure the LAN board´s hardware parameters.

   Refer to the *NetWare MultiProtocol Router 3.1 Configuration guide*, pp. 20-22.

2. Configure the protocol´s software parameters.

   In most of the cases, it should be enough to enable the network protocol and leave the default values.

   If you need more information, refer to the respective chapters of the *NetWare MultiProtocol Router 3.1 Configuration* guide for IPX (8), TCP/IP (11), AppleTalk (12) and Source Route Bridge (14). Ignore all instructions concerning WAN configuration. You will find information on configuring protocols for WAN connections in the *NetWare MultiProtocol Router for ISDN Installation and ISDN Configuration* guide.

3. Bind the configured protocol to the configured LAN interface.

   In most of the cases, you just have to enter your network address (IPX network address for IPX, IP address and subnet mask for TCP/IP) and can leave the default values.

   For additional information, refer to the guide and chapters mentioned in point 2.

Configuring for ISDN Support

The steps involved in configuring NetWare MultiProtocol Router for ISDN 3.1 and an ISDN-Controller are as follows. Since this Guide only describes the ISDN-related tasks, information is given on when to use which Novell documentation to perform the required steps:

1. Configure the ISDN-Controller´s parameters.

   Refer to Chapter 5 "Configuring Boards" of this Guide.

2. Configure network interfaces.

   Refer to Chapter 6 "Configuring ISDN Interfaces" of this Guide.

3. Configure ISDN call destinations.

   Refer to Chapter 7 "Configuring ISDN Call Destinations" of this Guide.

5. Configure global parameters for the NetWare MultiProtocol Router for ISDN.

   Refer to Chapter 8 "Configuring Global Parameters" of this Guide.

4. Configure the protocol´s software parameters.

   Refer to Chapters 9 (IPX), 10 (TCP/IP), 11 (AppleTalk) and 12 (Source Route Bridge) of this Guide.

5. Bind the configured protocol to the configured ISDN interface.

Chapters Containing Further Configuration Information

The following chapter of this Guide provides important additional configuration information and should be read as careful as the other configuration chapters:

- Chapter 14, "Configuration Interdependencies"

The following chapters of this Guide contain information on special configuration scenarios and should be read when required:

- Chapter 9, "Configuring IPX"
- Chapter 10, "Configuring TCP/IP"
- Chapter 11, "Configuring AppleTalk"
- Chapter 12, "Configuring Source Route Bridge"
- Chapter 13, "Advanced Configuration"
- Chapter 15, "Configuring Remote Node Access"

chapter 5 Configuring Boards

When you select and configure a LAN board or an ISDN-Controller, you are actually configuring one or more physical interfaces that correspond to individual connections over which packets are routed. Configuring a board causes the driver associated with the board to load each time you initialize the router.

For information on how to configure your LAN boards, refer to the *NetWare MultiProtocol Router 3.1 Configuration* guide, chapter 2, "Configuring Drivers and Board Parameters."

Due to INETCFG restrictions, ISDN-Controller related parameters must be configured in two separate menus. The parameter paths are as follows: load INETCFG > select *Boards*; load INETCFG > select *Network Interfaces* > select *ISDN-Controller Configuration*. For information on the latter, refer to Chapter 6, section "ISDN-Controller Configuration".

Changes in board parameters can be brought into effect by selecting the Reinitialize System command from the Internetworking Configuration menu or by entering the command manually at the system console prompt. When the system is reinitialized, the boards and all interfaces are unloaded and reloaded again to bring the configuration changes into effect.

This chapter contains the following sections:

- "Configuring an ISDN-Controller" on page 84
- "Enabling / Disabling an ISDN-Controller" on page 89
- "Deleting an ISDN-Controller" on page 89

Important

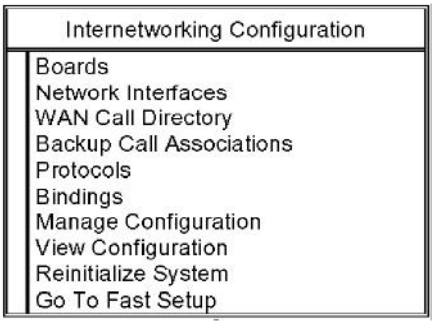
If you are using an AVM ISDN-Controller PCMCIA B or an AVM Mobile ISDN-Controller M1 or M2, make sure that the card and socket services are enabled before you start the server. For information on enabling card and socket services, refer to your computer manual.

To configure or reconfigure an ISDN-Controller, load INETCFG by typing the following command at the server prompt:

```
LOAD INETCFG <Enter>
```

The *Internetworking Configuration* menu is displayed:

**Figure 5-1:
Internetworking Configuration Menu**



Important

It is recommended not to use the Fast Setup option in this menu to configure NetWare MultiProtocol Router for ISDN 3.1. NetWare MultiProtocol Router for ISDN 3.1 provides preconfigured files for standard environments, which are described in the separate Quick Installation and Configuration manual coming with the product.

Configuring an ISDN-Controller

Procedure

1. **From the *Internetworking Configuration* menu, select *Boards*, then press** <Enter>**.**

   The *Configured Boards* window is displayed.

   If you are configuring a new ISDN-Controller, continue with Step 2.

   If you are changing an existing board configuration, select that ISDN-Controller, press <Enter>, then continue with Step 5.

   The *Configured Boards* window displays a list of configured ISDN-Controllers with the following ISDN-Controller relevant information:

   Board Name Name you assign to the ISDN-Controller.

   Driver The driver you selected for the ISDN-Controller.

   Int Interrupt request level (IRQ) used by the ISDN-Controller.

IOAddr I/O Base Address used by the ISDN-Controller.

Slot Slot number, if an AVM ISDN-Controller B1 PCI or B1-MCA is used.

Status Status of the ISDN-Controller, which is enabled by default.

Comment Comment you enter about the ISDN-Controller or its configuration.

2. **Press** <Ins> **to display the list of available drivers.**

3. **Scroll through the list, select the appropriate driver for the first ISDN-Controller installed in your system, then press** <Enter>**.**

   Options: ISDN-BRI, ISDN-PRI, ISDNWAYS.

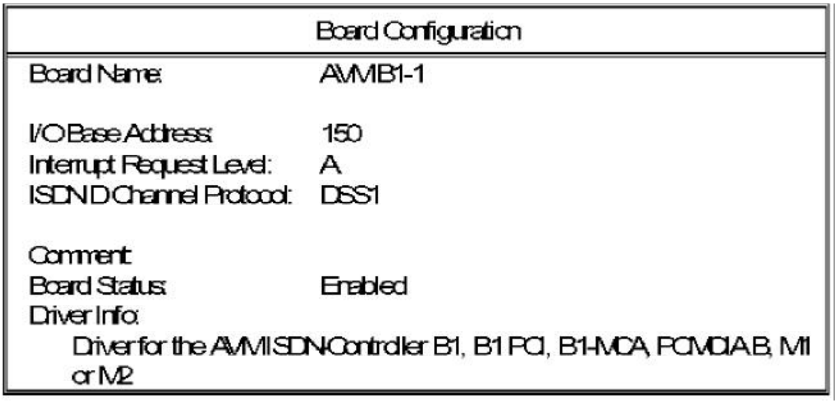
   Select ISDN-BRI, if you are using an AVM ISDN-Controller B1, B1 PCI, B1-MCA, PCMCIA B, M1 or M2.

   Select ISDN-PRI, if you are using an AVM ISDN-Controller T1 or T1-B.

   ISDNWAYS is provided to allow remote access to the NetWare MultiProtocol Router for ISDN from NetWAYS/ISDN and PPP clients. Special configuration information for providing remote access is given in Chapter 15, "Configuring Remote Node Access". Follow the instructions in this chapter to configure boards, then refer to Chapter 15 to configure for remote node access.

   After you selected the ISDN driver, the following menu appears:

Figure 5-2:



```
                      Board Configuration
Board Name:                  AVMB1-1

I/O Base Address:            150
Interrupt Request Level:     A
ISDN D Channel Protocol:     DSS1

Comment:
Board Status:                Enabled
Driver Info:
   Driver for the AVM ISDN-Controller B1, B1 PCI, B1-MCA, PCMCIA B, M1
   or M2
```

Board Configuration menu

4. **Enter a name in the *Board Name* field, then press** <Enter>**.**

You can use up to 10 alphanumeric characters for the board name.

5. **Specify the Controller parameters.**

Highlight each field, press <Enter>, then select the appropriate value for the parameter from the pop-up menu displayed.

6. **Check the *I/O Base Address.***

This parameter selects the base input / output port address used by the ISDN-Controller. Verify that the base I / O address matches what you noted during installation of your ISDN-Controller. Change it, if necessary.

B1, PCMCIA B, M1, M2:	Default: 150; Options: 150, 250, 300, 340
B1 PCI:	see your PCI configuration
T1, T1-B:	Default: 150

Important

If you want to use a different I/O Base Address on your ISDN-Controller T1 or T1-B, please contact AVM for more information.

Note

When the ISDN-Controller B1-MCA is used, INETCFG automatically disables the parameters “I/O Base Address” and “Interrupt Request Level” and prompts the parameter “Slot”, which is typical for configuration of adapters in MicroChannel bus systems. In case you use the ISDN-Controllers B1-MCA, select the MCA slot number appropriate to your configuration. Options: 1 to 8.

7. **Check the *Interrupt Request Level*.**

This parameter specifies the interrupt request level (IRQ) used by the ISDN-Controller configured for the NetWare MultiProtocol Router for ISDN. The Interrupt Level must not be used by other hardware adapter boards, it has to be unique. If the default value is already used by other boards, enter a new value. You do not have to change hardware (jumpers), since this IRQ level is software-configurable.

B1, M1, PCMCIA B:	Default: A; Options: 3, 4, 5, 7, 9, A, B, C, F
B1 PCI:	see your PCI configuration
T1, T1-B:	Default: 5; Options: 3, 4, 5, 7, 9, A, B, C, F

Important

If you want to use other interrupts than the default on your ISDN-Controller T1 or T1-B, please contact AVM for more information.

8. **Check the *ISDN D Channel Protocol*.**

This parameter specifies, which ISDN D channel protocol or protocol stack shall be loaded for this ISDN-Controller to access the ISDN network. The NetWare MultiProtocol Router for ISDN, in conjunction with the corresponding ISDN-Controllers, supports the internationally standardized D channel protocol DSS1, often referred to as "Euro-ISDN", as well as various national D channel protocols.

Make sure that you select the D channel protocol provided at your ISDN access (direct access or via PBX).

B1, B1 PCI, B1-MCA, PCMCIA B:	Default:	DSS1
	Options:	DSS1, 1TR6, VN3, CT1, NI1, 5ESS, AUSTEL, D64S, DS01, DS02, MDSS1, M1TR6
M1, M2:	GSM	
T1, T1-B:	Default:	DSS1T1
	Options:	DSS1T1, 1TR6T1

Table 5-1:
D Channel Protocols and protocol stacks

Protocol / Stack	Description
DSS1 / DSS1T1	internationally standardized ISDN D channel protocol, formerly called Euro-ISDN or E-DSS1. This ISDN D channel protocol is already or will soon be provided by all European countries that agreed to the Memorandum of Understanding in 1989.
1TR6 / 1TR6T1	national ISDN D channel protocol, provided in Germany.
VN3	national ISDN D channel protocol provided in France (also called NUMERIS). Note that this driver also supports VN4!
CT1	national ISDN D channel protocol provided in Belgium (also called ALINE).
NI1	national ISDN D channel protocol in the USA (National ISDN-1).
5ESS	ISDN D channel protocol in the USA, provided at AT&T custom ISDN BRIs.
AUSTEL	national ISDN D channel protocol in Australia (according to TS 013).

DS01 / DS02 / D64S leased line types offered by the German Deutsche Telekom AG. DS01 stands for 1 data channel, one signalling channel, DS02 for 2 data channels, 1 signalling channel. D64S stands for 1 B channel, no D channel.

MDSS1 D channel protocol to be selected if your local ISDN access provides the DSS1 protocol and you want to allow access to your LAN from users over Mobile ISDN.

M1TR6 D channel protocol to be selected if your local ISDN access provides the 1TR6 protocol and you want to allow access to your LAN from users over Mobile ISDN.

GSM protocol stack to be selected if you want to provide direct access to your router over GSM-based cellular networks (Mobile ISDN-Controller M1 or M2 used).

9. (Optional) Enter a *Comment* to this Board Configuration.

10. Check the *Board Status*.

Options: Enabled; Disabled

Default: Enabled

Enabled means that the board driver is loaded each time the router is started.

When a board is disabled, the driver is not loaded and the board cannot be used.

11. Press <Esc>**, select *Yes* to save changes to the board configuration, then press** <Enter>**.**

If there are any conflicts with the configuration parameters of other plug-in boards, one or more messages describe them. You must determine whether the conflict is acceptable or whether it interferes with the operation of the router and, if necessary, resolve it.

The *Configured Boards* window is redisplayed with the board you just configured. Note that the board status is Enabled; you can use the <Tab> key to toggle between *Enabled* and *Disabled*.

12. To configure the remaining boards, if any, repeat Step 2 through Step 11.

After you have configured the LAN boards and ISDN-Controller(s) in your system, you have to configure interface parameters for the ISDN-Controller(s) next. To configure interfaces, go to the next Chapter, "Configuring ISDN Interfaces".

Enabling/Disabling an ISDN-Controller

To enable or disable an ISDN-Controller, complete the following steps:

Procedure

1. **At the server prompt, type**

   ```
   LOAD INETCFG <Enter>
   ```

   The *Internetworking Configuration* menu is displayed.

2. **From the *Internetworking Configuration* menu, select *Boards*, then press** <Enter>**.**

   A new window displays the list of configured boards.

3. **Highlight the ISDN-Controller you want to enable (or disable), then press** <Tab> **.**

   The status of the ISDN-Controller is changed from *Disabled* to *Enabled* (or *Enabled* to *Disabled*). The <Tab> key acts as a toggle switch.

4. **Press** <Esc> **to return to the *Internetworking Configuration* menu.**

Important

After enabling or disabling an ISDN-Controller, select the Reinitialize System command from the Internetworking Configuration to unload and reload boards and their interfaces.

Deleting an ISDN-Controller

To delete an ISDN-Controller, complete the following steps:

Procedure

1. **At the server prompt, type**

   ```
   LOAD INETCFG <Enter>
   ```

   The *Internetworking Configuration* menu is displayed.

2. **From the *Internetworking Configuration* menu, select *Boards*, then press** <Enter>**.**

   A new window displays the list of configured boards.

3. **Highlight the ISDN-Controller you want to delete, then press** <Delete>**.**

   A message is displayed indicating that deleting the board also deletes all existing binds to the ISDN-Controller's interfaces.

   If ISDN Call Destinations are configured, another message is displayed asking whether you want to delete ISDN Call Destinations that refer to this ISDN-Controller. If you answer *No*, the ISDN Call Destinations remain, even though the ISDN-Controller is deleted.

4. **When prompted, select *Yes*, then press** <Enter> **to delete the board.**

   The ISDN-Controller is removed from the list of configured boards.

5. **Press** <Esc> **to return to the *Internetworking Configuration* menu.**

chapter 6 Configuring ISDN Interfaces

This chapter provides basic information on configuring the ISDN interfaces. You should read through this chapter very carefully to learn about the parameters and their configuration options.

Important

Due to INETCFG restrictions, board-related and global parameters are also configured under Network Interfaces. Note that the board-related parameters, if required, only have to be configured once per ISDN-Controller, and the global parameters must be configured only once for the whole NetWare MultiProtocol Router for ISDN 3.1.

This chapter contains the following sections:

- "ISDN Network Interface Configuration" on page 94
- "Expert Configuration of ISDN Interface <*Name*>" on page 99
- "Default Call Destination Configuration" on page 109
- "ISDN-Controller Configuration" on page 111

Special configuration scenarios are described in the following chapters of this Guide:

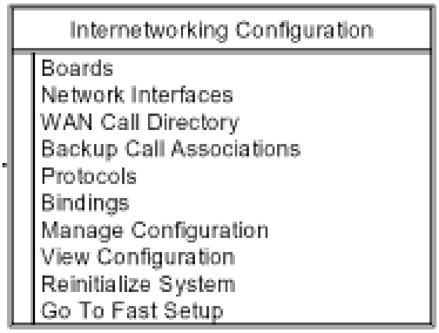
- Chapter 9, "Configuring IPX"
- Chapter 10, "Configuring TCP/IP"
- Chapter 11, "Configuring AppleTalk"
- Chapter 12, "Configuring Source Route Bridge"
- Chapter 13, "Advanced Configuration"
- Chapter 14, "Configuration Interdependencies"
- Chapter 15, "Configuring Remote Node Access"

Since they provide important additional configuration information, you should also read through them very carefully.

To configure ISDN interfaces, INETCFG is required. If INETCFG is not already loaded, load it by typing the following command at the server prompt:

```
LOAD INETCFG <Enter>
```

The Internetworking Configuration menu is displayed:



Internetworking Configuration

Boards
Network Interfaces
WAN Call Directory
Backup Call Associations
Protocols
Bindings
Manage Configuration
View Configuration
Reinitialize System
Go To Fast Setup

Figure 6-1:
Internetworking Configuration Menu

Procedure

1. **From the *Internetworking Configuration* menu, select *Network Interfaces*, then press** <Enter>**.**

   The *Network Interfaces* window is displayed.

   If you are configuring a new interface, ensure that the appropriate ISDN-Controller has been configured (see Chapter 5, "Configuring Boards"), then continue with Step 2.

   The *Network Interfaces* window displays a list of network interfaces associated with each configured ISDN-Controller with the following information:

   Board Name Name you gave to the ISDN-Controller when you configured it.

   Interface Each interface is identified as BoardName_n, where n is the interface number. An AVM ISDN-Controller for BRI has 2 interfaces, an AVM ISDN-Controller for PRI 30 interfaces.

   Group Interface group, if any, that the ISDN interface belongs to.

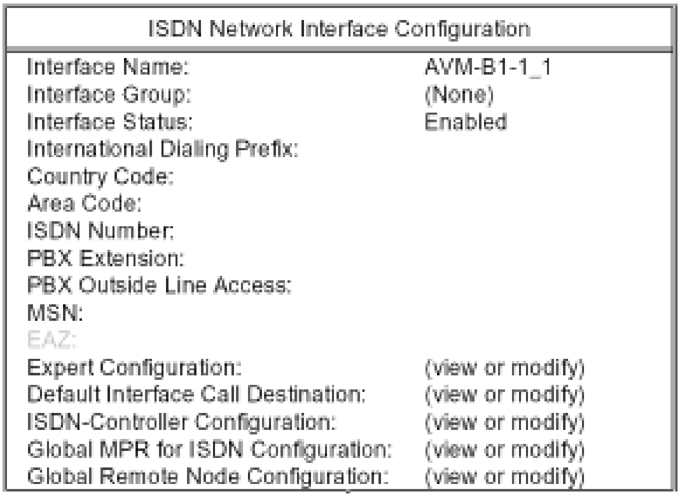
Media Network medium or WAN protocol selected (ISDN-BRI or ISDN-PRI).

Status Current status of the interface.

2. **Scroll to an unconfigured network interface, then press** <Enter> **to select it.**

The *ISDN Network Interface Configuration* window is displayed:

Figure 6-2:
ISDN Network Interface Configuration Menu



ISDN Network Interface Configuration

Interface Name:	AVM-B1-1_1
Interface Group:	(None)
Interface Status:	Enabled
International Dialing Prefix:	
Country Code:	
Area Code:	
ISDN Number:	
PBX Extension:	
PBX Outside Line Access:	
MSN:	
EAZ:	
Expert Configuration:	(view or modify)
Default Interface Call Destination:	(view or modify)
ISDN-Controller Configuration:	(view or modify)
Global MPR for ISDN Configuration:	(view or modify)
Global Remote Node Configuration:	(view or modify)

Interface Name: The name of the interface in the form of BoardName_n, where n is the interface number.

♦ **Expert Configuration:** allows you to set values for more specific interface-related parameters (Subaddress, Interface Usage, Call Acceptance, Security Call-Back, etc.).

♦ **Default Interface Call Destination:** lets you define default values for call parameters that apply on this interface for calls from remote sites which you did not configure a call destination for.

♦ **ISDN-Controller Configuration:** lets you define ISDN-Controller related parameters that only apply in special situations (Hunt Groups, SPIDs, etc.). They have to be configured only once for an ISDN-Controller.

- **Global MPR for ISDN Configuration:** lets you define global parameters that are valid for the NetWare MultiProtocol Router for ISDN as a whole (Logging, Accounting, Traps, etc.). For more information, refer to Chapter 8, "Configuring Global Parameters".

- **Global Remote Node Configuration:** allows configuration of parameters that apply for all remote nodes dialing into the router (Dynamic Address Assignment, etc.). Global parameters for remote nodes are set after configuring remote node access and after binding the network protocol(s) to ISDNWAYS. For more information on this menu, refer to Chapter 17, "Configuring Remote Node Access."

ISDN Network Interface Configuration

The *ISDN Network Interface Configuration* menu contains general interface-related information such as the Interface Status and the address of the ISDN-Controller interface. You should always fill in all required parameters. From this menu, you can then skip to the other configuration menus described above.

Changes in the *ISDN Network Interface Configuration* are brought into effect by selecting the *Reinitialize System* command in the *Internetworking Configuration*. The message "Driver reconfiguration started" is displayed on the system console. The drivers are not unloaded and reloaded unlesss you changed the Interface Status.

Proceed as follows:

Procedure

1. **Select an *Interface Group*.**

   This parameter lets you assign an interface to an existing or a new interface group. An interface group is a grouping of several interfaces with similar characteristics, such as equal ISDN number. A symbolic name identifies an interface group. They can be used interchangeably. Thus, all interfaces belonging to an interface group must have the same values in their Expert Configurations.

   Defining an interface group lets you make and accept on-demand calls on any of several network interfaces without creating an individual ISDN Call Destination for each interface. All you need to do is specify the interface group name instead of the interface name in the ISDN Call Destination. When the call is made or comes in, an available interface, and therefore any free B channel, is selected from the group. Thus, you don't need to dedicate interfaces to specific destinations.

Press <Enter> to display a list of already configured interface groups. Select one and press <Enter> again.

2. **Check the *Interface Status*.**

   The interface status defines whether or not the respective interface is loaded when the router is brought up.

   Default: Enabled

   Options: Enabled, Disabled, Time Restricted

   Enabled means that the interface is loaded into server memory each time the system is started or reinitialized. If this is the first interface of an ISDN-Controller, the controller is also loaded.

   Disabled means that the interface is not loaded.

   If you select "Time Restricted", you can configure the periods during which the interface is enabled and disabled in a separate menu (see Step 11 on page 105). For example, you can disable the Interface Status during the weekends to make sure that no one is able to dial into or out of your LAN. When the Interface Status changes from Enabled to Disabled, all active connections over this interface are cleared.

3. **Enter your *International Dialing Prefix*.**

   Specify the prefix you have to dial in your country to make international calls.

   For a complete configuration, you should always enter the International Dialing Prefix and values for the parameters Country Code, Area Code, ISDN Number and, if necessary, PBX Extension, PBX Outside Line Access (or EAZ or MSN).

   The International Dialing Prefix depends on the country in which you are installing the NetWare MultiProtocol Router for ISDN.

   Example 1: The International Dialing Prefix to dial out of Germany is 00.

Example 2: The International Dialing Prefix to dial out of the UK is 000.

4. **Enter your *Country Code*.**

Specify the number identifying your country when someone calls you from abroad. Enter your Country Code, even if you do not want to make international calls at the moment. The Country Code depends on the country in which you are installing the NetWare MultiProtocol Router for ISDN.

Example 1: The Country Code to reach Germany from abroad is 49.

Example 2: The Country Code to reach the UK from abroad is 44.

5. **Enter your *Area Code*.**

This parameter specifies the number identifying your area when someone calls you from outside your area, but still within your country. Enter your Area Code, even if you do not want to make calls outside your local exchange area at the moment.

Example 1: The Area Code for Munich (Germany) is 089.

Example 2: The Area Code for Inner London is 171.

6. **Enter your *ISDN Number*.**

This parameter specifies the ISDN number of your ISDN access.

If the ISDN-Controller in your router PC is directly connected to the public ISDN, enter the ISDN subscriber number of your ISDN access.

If the ISDN-Controller is connected to a private branch exchange (PBX), enter the ISDN subscriber number of the PBX itself (without the PBX extension).

If you want to use DDI numbering, enter the complete DDI number in this field.

Example for DDI: Your ISDN access is assigned the number range 39925910 to 39925918. Select one of the numbers, for example 39925913, and enter it as ISDN Number.

Note

If you are not sure about your ISDN subscriber number, contact your local PTT or, if a PBX is used, your PBX specialist.

7. If your server/router PC is connected to the public ISDN via a PBX, you have to enter

7a. the *PBX Extension* to reach the server/router PC.

This parameter specifies the concrete extension of the PBX your ISDN-Controller is connected to. It must be dialed in addition to the ISDN subscriber number of the PBX to reach the ISDN-Controller in your router.

7b. your *PBX Outside Line Access*.

This is the number you have to dial to get access to the public ISDN within a PBX.

The most common PBX Outside Line Access digit is "0".

8. Enter the *MSN* (Multiple Subscriber Number), if:

- The server / router PC is connected to an ISDN access with the D channel protocols DSS1, MDSS1, VN3, CT1, NI1, 5ESS or AUSTEL, and
- You have to use MSNs to address the interfaces of your ISDN-Controller and applied for MSNs at your local PTT.

If this applies to your situation, configure the MSN, to which the interface of ISDN-Controller should listen, as follows:

- **MSNs with non-sequential numbers (8885951, 774840, etc.)**

In this case, enter this number in the ISDN Number (see above) and the MSN field.

Example: ISDN Number: 885951, MSN: 885951

- **MSNs where only the final digits differ (885951, 885952, etc.):**

In this case, the complete entry for ISDN Number (see above) contains the whole number, and the final digits are repeated for MSN.

Example: ISDN Number: 885951, MSN: 51.

9. Enter the *EAZ* (Endgeräteauswahlziffer), if

- The router PC is connected to a 1TR6 ISDN access, and
- you have to use EAZs for one of the following reasons: a second piece of terminal equipment using the same Service

Indicator is connected to the same ISDN bus or your router PC is connected to a PBX that requires configuration of EAZs to address the interfaces of an ISDN-Controller.

If this is true for your situation, configure the EAZ, to which the interface of the ISDN-Controller should listen, as follows:

9a. No PBX, ISDN-Controller has direct access to the public ISDN:

Replace the last digit (0) of your ISDN subscriber number with the EAZ and enter the resulting number in the ISDN Number field (see above). Repeat the EAZ here.

Example: EAZ: 7; ISDN subscriber number: 5502150

-> entry for ISDN Number: 5502157; entry for EAZ: 7

9b. ISDN-Controller connected to a PBX:

How EAZs are configured in this case depends on the type of PBX used. Therefore ask your PBX specialist, whether you have to

- replace the last digit of the PBX Extension with the EAZ. The EAZ must be repeated here.

  Example 1: EAZ: 7; PBX Extension: 210
  -> entry for PBX Extension: 217; entry for EAZ: 7

or

- add the EAZ to the PBX Extension. The EAZ must be repeated here as well.

  Example 2: EAZ: 7; PBX Extension: 210
  -> entry for PBX Extension: 2107; entry for EAZ: 7

Possible values for EAZ range from 0 to 9.

10. Press <Enter> **on *Expert Configuration* and continue with "Expert Configuration of ISDN Interface *<Name>*".**

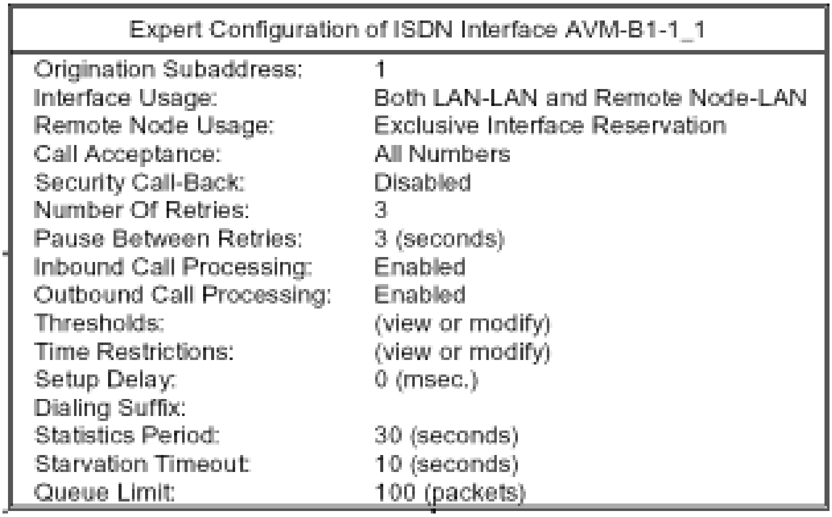
Expert Configuration of ISDN Interface <*Name*>

The Expert Configuration menu allows you to set values for more specific interface-related parameters (Subaddress, Interface Usage, Call Acceptance, Security Call-Back, etc.)

Changes in the Interface Expert Configuration of an ISDN interface are brought into effect by selecting the Reinitialize System command from the Internetworking Configuration menu or by entering REINITIALIZE SYSTEM at the server console prompt. The message "Driver reconfiguration started" will be displayed at the server console.

When you press <Enter> on *Expert Configuration* in the *ISDN Network Interface Configuration* menu, the following window is displayed:

Figure 6-3:
Expert Configuration for ISDN Interface <Name> menu



```
            Expert Configuration of ISDN Interface AVM-B1-1_1
  Origination Subaddress:        1
  Interface Usage:               Both LAN-LAN and Remote Node-LAN
  Remote Node Usage:             Exclusive Interface Reservation
  Call Acceptance:               All Numbers
  Security Call-Back:            Disabled
  Number Of Retries:             3
  Pause Between Retries:         3 (seconds)
  Inbound Call Processing:       Enabled
  Outbound Call Processing:      Enabled
  Thresholds:                    (view or modify)
  Time Restrictions:             (view or modify)
  Setup Delay:                   0 (msec.)
  Dialing Suffix:
  Statistics Period:             30 (seconds)
  Starvation Timeout:            10 (seconds)
  Queue Limit:                   100 (packets)
```

Procedure

1. **Check the *Origination Subaddress*.**

   The Origination Subaddress is a supplement to the number that is dialed to reach the configured ISDN-Controller itself and specifies the concrete address of the currently selected logical interface.

   When you leave this field empty, incoming calls directed to any subaddress will be accepted at this interface.

When you set the Origination Subaddress on all interfaces of an ISDN-Controller to the same value, incoming calls directed to this subaddress will be forwarded to any interface.

For PPP over ISDN, the origination subaddress has no meaning.

2. **Check the *Interface Usage*.**

   This parameter defines whether the respective interface is to be used for connections between LANs only, for remote access by NetWAYS/ISDN and PPP-compatible clients only or whether both type of connections are allowed.

   Default: Both LAN-LAN and Remote Node-LAN

   Options: Both LAN-LAN and Remote Node-LAN, LAN-LAN, Remote Node-LAN

   If you select "LAN-LAN", no connections to remote nodes are allowed over this interface. This means that the interface is reserved for connections between LANs only.

   "Remote Node-LAN" means that this interface can only be used for connections to remote NetWAYS/ISDN and PPP-compatible clients. If you choose this option, you also have to specify the *Remote Node Usage* (see Step 3 below).

   "Both LAN-LAN and Remote Node-LAN" allows both types of connections over this interface. If you have connections with remote PPP nodes, also read the description of "PPP Destination Type" on page 110 of this chapter.

3. **If you chose *Remote Node-LAN* or *Both LAN-LAN and Remote Node-LAN* for *Interface Usage* above, check the *Remote Node Usage*.**

   This parameter describes how NetWare MultiProtocol Router for ISDN interfaces are treated when used for remote node access.

   Default: Exclusive Interface Reservation

   Options: Exclusive Interface Reservation,
   On Demand Interface Acquirement

   "Exclusive Interface Reservation" means that an interface and the underlying ISDN data channel will be reserved for a connection from the first dial-in until the connection is cleared logically. The logical connection between the remote client and the interface will be maintained in case of an Inactivity Timeout (physical connection down), and any incoming call to the interface will be rejected during this period. This guarantees that an ISDN data channel will be physically available whenever data is to be transmitted from or to the remote client, and is the recommended type of remote node usage.

"On Demand Interface Acquirement" means that an interface and the underlying ISDN data channel will not be reserved for one connection, but will be released and become available for any other dial-in or dial-out operation as soon as the underlying physical ISDN data channel between the remote client and the interface is deactivated due to an Inactivity Timeout. This type is more flexible, since it allows more than one remote clients to share a single ISDN data channel. It cannot be guaranteed, however, that an ISDN data channel is available whenever data is to be transferred from or to the remote client, since the physical ISDN data channel might be in use for another remote client communicating with the LAN.

4. **Check the *Call Acceptance*.**

This parameter specifies whether a specific security mechanism is to be placed ahead of the local network security mechanisms (specific NetWare login scripts or TCP/IP based logins for each remote user, for example) when a call is set up from a remote site to this interface of the ISDN-Controller for the first time.

Default:	All Numbers
Options:	All Numbers, Only Registered Numbers: Caller-Specified, Only Registered Numbers: CLI, Only Registered Numbers: CLI and Caller-Specified

If "All Numbers" is selected, no ISDN-specific security check is performed and all incoming calls for the MSN, EAZ or DDI configured for this ISDN interface are accepted.

"Only Registered Numbers" means that all incoming calls for the MSN, EAZ or DDI configured for this ISDN interface are cross-checked by their transmitted number (or numbers), and access is denied to all incoming calls not registered in the Call Acceptance Database. The following options are possible:

- Caller-Specified: the origination address (made up from the components International Dialing Prefix, Country Code, Area

Code, ISDN Number, PBX Outside Line Access and PBX Extension) of the remote site or the Dial-Back Number, if configured, is compared with the number entered in the Call Acceptance Database. This mode provides least security.

- CLI: only the number transmitted over the D channel is compared with that entered in the Call Acceptance Database. CLI (Call Line Identification) is a service of ISDN. To use CLI, make sure that this service is enabled at all remote sites that are allowed access to your router. Otherwise, they are denied access by your router.
- CLI and Caller-Specified: the number transmitted over the D channel and the origination address (made up from the components International Dialing Prefix, Country Code, Area Code, ISDN Number, PBX Outside Line Access and PBX Extension) of the remote site or the Dial-Back Number, if configured, are compared with the entries in the Call Acceptance Database. This security mode provides highest security. Normally, the caller-specifed and the CLI number are identical. However, they can differ in rare cases (e.g. the CLI number transmitted may be incomplete). In either case, you have to make two entries in the Call Acceptance Database for the respective remote site.

5. **Check the *Security Call-Back*.**

NetWare MultiProtocol Router for ISDN 3.1 provides a Security Call-Back to provide highest network security. Call-back is naturally only performed for an initial logical connection set-up request from a remote site, and not for subsequent underlying physical call set-ups from this site.

When one of the call-back modes is selected, the NetWare Multi-Protocol Router for ISDN first disconnects an ISDN connection coming in from a remote site and then dials back.

Default:	Disabled
Options:	Disabled, Force Call-Back to Caller-Specified Number, Force Call-Back to CLI Number

With Force Call-Back to a Caller-Specified Number, the NetWare MultiProtocol Router for ISDN takes the number delivered by the remote site. This is either the origination address (made up from the components International Dialing Prefix, Country

Code, Area Code, ISDN Number, PBX Outside Line Access and PBX Extension) of the remote site or the Dial-Back Number, if configured.

With Force Call-Back to CLI Number, the NetWare MultiProtocol Router for ISDN dials back the number delivered over the D channel of the ISDN network.

6. Check the *Number of Retries*.

This parameter specifies the number of retries the ISDN-Controller will initiate an attempt to establish an ISDN connection.

Default: 3

Range: 0, 1, 2, 3, ... 10 (0=no retry)

Suggestion

If the ISDN network message "Network Congestion" is returned very often (esp. for international calls), you should enter a higher value for this parameter to compensate for short-term congestions in the ISDN network.

7. Check the *Pause Between Retries*.

This field specifies the pause (in seconds) between two attempts to establish an ISDN connection.

Default: 3

Range: 1, 2, 3, ... 30

8. Check the *Inbound Call Processing*.

This parameter specifies whether or not the NetWare MultiProtocol Router for ISDN listens for incoming calls on the configured network interface.

Default: Enabled

Options: Enabled, Disabled, Time Restricted

When Inbound Call Processing is enabled, the NetWare MultiProtocol Router for ISDN listens to incoming calls on the currently configured network interface.

When inbound call processing is disabled, no incoming calls for the MSN, EAZ or DDI configured on this interface are accepted. If Inbound Call Processing is disabled on all interfaces of an ISDN-Controller, no incoming calls will be accepted at the ISDN bus. The ISDN network will return the message "No user responding". This feature is useful for central sites that want to make circular calls to their branch offices and never want to be called themselves.

Time Restricted lets you enable and disable Inbound Call Processing at specific times for security purposes. Time Restrictions are configured in a different menu (see Step 11 below).

When the value changes from Enabled to Disabled, active connections will not be affected.

9. Check the *Outbound Call Processing*.

This parameter defines whether or not outgoing calls are processed on this interface. It is useful for service providers, for example, who offer online services and do not want to have connection charges at their ISDN access. On the NetWare Multi-Protocol Router for ISDN in AVM´s Data Call Center, Outbound Call Processing is disabled, for example.

Default:	Enabled
Options:	Enabled, Disabled, Time Restricted

Enabled means that outgoing calls are allowed over this interface.

When Outbound Call Processing is disabled, no outgoing calls, including underlying call set-ups, are allowed over this interface. It can only be used for incoming calls.

Time Restricted lets you enable and disable Outbound Call Processing at specific times. Time Restrictions are configured in a different menu (see Step 11 below). For example, you can disable Outbound Call Processing during the weekends to make sure that no one is able to dial into or out of your LAN and no charges accrue over the weekend.

When the value changes from Enabled to Disabled, active connections will not be affected.

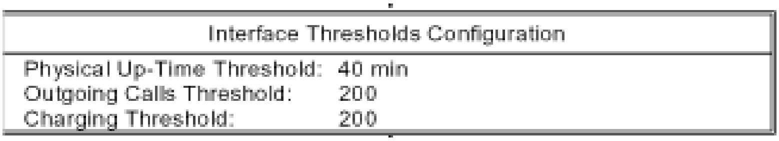
10. Check the*Thresholds* for the ISDN Connection Monitor or enter new values.

The ISDN Connection Monitor lets you configure three different interface-related thresholds on a 24 h basis: the maximum physical up-time per interface, the maximum outgoing calls per interface and the maximum charge units per interface. When one of the thresholds is reached, the interface is barred for incoming and outgoing calls until the bar is removed. For the initial phase, you may take the given default values. For more information and an explanation of how the default values have been calculated, refer to Chapter 18, section "ISDN Connection Monitor".

Later, to find out the appropriate threshold values for your situation, watch the number of ISDN call set-ups, the physical up-time and the charge units accruing daily for three or four weeks. The threshold values then should be slightly higher than the average to allow for deviations at peak times.

To view or modify the thresholds, press <Enter> on the parameter to display the following window:

Figure 6-5:
Thresholds Configuration



```
              Interface Thresholds Configuration
Physical Up-Time Threshold:  40 min
Outgoing Calls Threshold:    200
Charging Threshold:          200
```

Important

To avoid unnecessary charges, you should adapt the defaults on all ISDN interfaces to your situation.

10a. ***Physical Up-Time Threshold*.**

Default: 40 min

Enter the Physical Up-Time Threshold in hours, minutes and seconds.

10b. ***Outgoing Calls Threshold*.**

Default: 200

Enter the Outgoing Calls Threshold.

10c. ***Chargings Threshold*.**

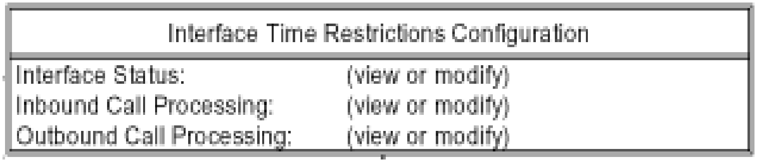
Default: 200

Enter the Chargings Threshold.

11. Check the *Time Restrictions*.

Press <Enter> on this parameter to display the following window:

Figure 6-6:
Interface Time Restrictions Configuration Menu

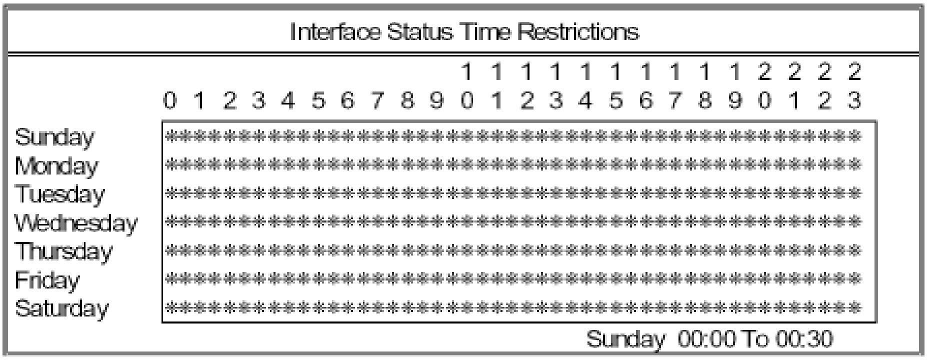


```
                 Interface Time Restrictions Configuration
Interface Status:                (view or modify)
Inbound Call Processing:         (view or modify)
Outbound Call Processing:        (view or modify)
```

If you set the Interface Status, Inbound Call Processing and Outbound Call Processing to "Time Restricted", you can define times during which these parameters are enabled and times during which they are disabled.

To view or modify the times, press <Enter> on the respective parameter.

Figure 6-7:
Interface Status Time Restrictions Menu



```
                      Interface Status Time Restrictions
                                         1 1 1 1 1 1 1 1 1 1 2 2 2 2
                     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
Sunday               ************************************************
Monday               ************************************************
Tuesday              ************************************************
Wednesday            ************************************************
Thursday             ************************************************
Friday               ************************************************
Saturday             ************************************************
                                             Sunday  00:00 To 00:30
```

As you can see, all the input fields are already filled in with asterisks. This means the parameter is enabled each day of the week and every hour of the day.

To disable the parameter at certain times, delete the corresponding asterisks by pressing <Del> or the Space Bar. To restore the asterisks, press <Ins> or *.

The key assigment is similar to that in the SYSCON utility (NetWare 3.12) and NETADMIN / NWADMIN utilities (NetWare 4.x).

Important

If the interfaces of an ISDN-Controller are not identified by a unique MSN, EAZ or DDI, make sure that Time Restrictions are set identically on each interface. For more information, refer to Chapter 14, "Configuration Interdependencies".

11a. Check the time restrictions for the *Interface Status*.

In this window you can determine the days and times during which the given interface can be used. Outside these periods, the interface is barred for outgoing as well as incoming calls. The interface status in the ISDN Console changes from UP to DOWN to indicate that outgoing calls are not possible and incoming calls to this interface are rejected. A connection configured as a backup router would then be activated.

When the Interface Status changes from Enabled to Disabled, all active connections over this interface are cleared.

For example, you can disable the Interface Status during the weekends to make sure that no one is able to dial into or out of your LAN.

11b. Check the time restrictions for *Inbound Call Processing*.

Here you can define the days and times during which Inbound Call Processing is enabled (asterisk) and disabled (no asterisk).

When the value changes from Enabled to Disabled, active connections will not be affected.

11c. Check the time restrictions for *Outbound Call Processing*.

Here you can define the days and times during which Outbound Call Processing is enabled (asterisk) and disabled (no asterisk).

When the value changes from Enabled to Disabled, active connections will not be affected.

12. If you are using an AVM ISDN-Controller for PRI, check the *Setup Delay*.

In some rare cases local exchanges have problems with multiple call set-ups within short intervals at Primary Rate Interfaces.

If this is the case, define the Setup Delay in milliseconds.

Default: 0 (= disabled)

Options: 0 to 2000 (milliseconds)

13. **For international connections, enter the *Dialing Suffix*.**

For certain international connections, a special character is needed to indicate the end of the phone number. This will accelerate call set-up considerably from within about 12 to 15 seconds to 1 to 2 seconds.

Enter the required symbol in this place to accelerate call-set up to abroad sites.

Example: For connections from Belgium to Germany, the character to enter is #.

14. **Check the *Statistics Period*.**

This parameter specifies the rate (in seconds) at which the ISDN-controller updates the statistics gathered.

Default: 30

Range: 5, 6, 7 ... 300

These Statistics can be viewed through the ISDN Console or via the MPR for ISDN Router Manager or any SNMP-based management console by displaying the specified tables as described in MPR4ISDN.MIB.

15. **Check the *Starvation Timeout*.**

This parameter defines the period of time the NetWare MultiProtocol Router for ISDN will wait for replies from remote sites. When a data channel is broken, a signal is sent over the D channel to report the event. Since there is no D channel in D64S lines, this parameter is mainly used with D64S. However, it also applies for other ISDN lines.

Default: 10 (seconds)

Options: 0 to 30 seconds (0=disabled)

16. **Check the *Queue Limit*.**

This parameter specifies the maximum number of outbound data packets that can be queued within the NetWare operating system and on the ISDN-Controller to this interface for transmission. When the limit is exceeded, subsequent outbound data packets will be returned to the service requester instead of being added to the transport queue of the interface. As a consequence, the Dropped Packet counts in the ISDN Console (see Chapter 18) increases.

Default: 100

Range: 0, 1, 2, ... 2000

A value of 0 defines unlimited queues. However, it is recommended not to change the default value.

17. **Press** <Esc> **to return to the *ISDN Network Interface Configuration* menu.**

18. **Press** <Enter> **on *Default Interface Call Destination* and continue with "Default Call Destination Configuration".**

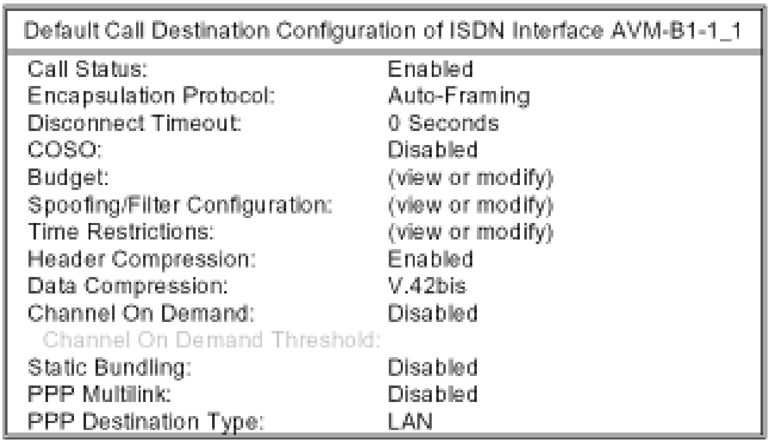
Default Call Destination Configuration

The Default Call Destination Configuration of an interface applies when a call comes in from a remote site which you did not configure a call destination for. In such a case, the router takes the parameter values in the Default Call Destination Configuration of the respective interface to control the connection.

For information on how incoming calls are accepted, refer to Chapter 7, "Configuring ISDN Call Destinations."

When you press <Enter> on *Default Interface Call Destination*, the following menu is displayed:

Figure 6-8:
Default Call Destination Configuration for ISDN Interface *<Interface Name>* menu



```
Default Call Destination Configuration of ISDN Interface AVM-B1-1_1
Call Status:                        Enabled
Encapsulation Protocol:             Auto-Framing
Disconnect Timeout:                 0 Seconds
COSO:                               Disabled
Budget:                             (view or modify)
Spoofing/Filter Configuration:      (view or modify)
Time Restrictions:                  (view or modify)
Header Compression:                 Enabled
Data Compression:                   V.42bis
Channel On Demand:                  Disabled
  Channel On Demand Threshold:
Static Bundling:                    Disabled
PPP Multilink:                      Disabled
PPP Destination Type:               LAN
```

Check all the values in this menu. For detailed information on each of the parameters, refer to Chapter 7, "Configuring ISDN Call Destinations".

Note the following differences to the ISDN Call Destination Configuration:

- Encapsulation Protocol:

  the default value is Auto-Framing to allow automatic detection of the protocol used (AVM Proprietary or PPP over ISDN).

- COSO:

  the option "Local" is not available, since it would not make sense to assume the charges for an unknown caller.

- PPP Destination Type:

  this parameter defines how PPP calls from "unknown" sites are accepted. Options are "LAN" and "Remote-Node".

  LAN means that for incoming PPP calls, parameters are negotiated as defined in RFC 1634 (IPXWAN). In addition, the call is visible through the Call Connection Manager (CALLMGR).

  If you select Remote-Node, parameters will be negotiated as defined in RFC 1552 (IPXCP) or RFC 1332 (IPCP), depending on the network protocol. In addition, the call is visible in the ISDN Console (Remote Nodes).

- You should set the Disconnect Timeout to an appropriate value to make sure that connections to unknown remote sites are disconnected after a specified period of inactivity. Example: On AVM´s Data Call Center, the Disconnect Timeout is set to 5 min.
- To make sure that unknown remote sites are not allowed to use channel bundling, it is recommended to leave the defaults Channel On Demand=Disabled and Static Bundling=Disabled.

ISDN-Controller Configuration

In the ISDN-Controller Configuration you define special parameters that apply for the current ISDN-Controller.

You only have to enter this menu, if

- You have a point-to-point ISDN access.
- You want to accept all incoming calls on this ISDN-Controller as Mobile ISDN calls only.
- You have to use SPIDs (D channel protocols NI-1 and 5ESS).
- You are using an AVM ISDN-Controller for PRI.

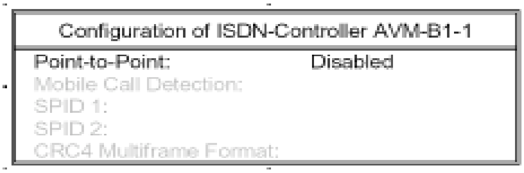
Important

For each ISDN-Controller, you have to configure these parameters only once!

Changes in the *ISDN-Controller Configuration* are brought into effect by selecting the *Reinitialize System* command from the *Internetworking Configuration* menu. The boards are unloaded and reloaded again with the new settings.

When you press <Enter> on *ISDN-Controller Configuration* in the *ISDN Network Interface Configuration* menu, the following menu is displayed:

Figure 6-7:
ISDN-Controller Configuration menu



```
Configuration of ISDN-Controller AVM-B1-1
Point-to-Point:                 Disabled
Mobile Call Detection:
SPID 1:
SPID 2:
CRC4 Multiframe Format:
```

Procedure

1. **If you are using an AVM ISDN-Controller for BRI, check the setting for *Point-to-Point*.**

   If you have a point-to-point ISDN access, you must enable Point-to-Point. At a point-to-point access, only one ISDN terminal device can be operated.

Default:	Disabled
Options:	Disabled, Enabled

   At a point-to-multipoint access, leave the default "Disabled". At point-to-multipoint accesses, up to eight terminal devices can be operated. They can be addressed with the help of MSNs or EAZs.

2. **If you are using MDSS1 or M1TR6 as D Channel Protocol, check the *Mobile Call Detection*.**

   Mobile Call Detection defines how incoming calls are treated when you are using the D channel protocols MDSS1 and M1TR6. These protocols support calls from remote sites over GSM-based cellular networks as well as over terrestrial ISDN lines.

Default:	Auto-Framing
Options:	Auto-Framing, Mobile Calls Only

   When Mobile Call Detection is set to Auto-Framing, both types of calls are accepted on this interface.

   Mobile Calls Only means that only calls from remote sites over GSM-based cellular networks are accepted on this interface. Calls over standard terrestrial ISDN lines are rejected.

3. **If you have an ISDN access with the D channel protocol NI-1 or 5ESS, enter your *SPID1* and *SPID2*.**

   SPIDs are Service Profile Identifiers which are used to identify what sort of services and features the switch provides to the ISDN device. When a new subscriber is added, the service representative will allocate a SPID just as they allocate a directory number. Subscribers must input the SPIDs into their terminal device before they will be able to connect to the central office switch (this is referred to as initializing the device).

   Your ISDN provider should be able to tell you what your SPID is and how many SPIDs are required.

4. **If you are using an AVM ISDN-Controller for PRI, check the *CRC4 Multiframe Format*.**

   Default: Enabled

   Options: Enabled, Disabled

   In some countries, there are two different types of PRI switching stations which use different signalling formats on the D channel. Newer stations use CRC4 Multiframe format, older ones Doubleframe format. Call set-up problems may be the result, which become apparent through the following: The D channel LED on the AVM ISDN-Controller T1 / T1-B flashes and the ISDN network returns the error message 3301 or 3302.

   In such a case, ask your local PTT if CRC4 Multiframe is supported at your local switching station. If not, you should disable *CRC4 Multiframe Format* in this menu.

5. **Press** <Esc> **to return to the *ISDN Network Interface Configuration* menu.**

When you are finished, press <Esc> twice, select *Yes* to save your changes to the Interface Configuration, then press <Enter>.

The *Network Interfaces* menu reappears.

To configure the remaining interfaces, if any, repeat the steps described in the sections "ISDN Network Interface Configuration", "Expert Configuration for ISDN Interface <*Name*>" and "Default Interface Call Destination" above.

Then, proceed to Chapter 7, "Configuring ISDN-Call Destinations" to configure your call destinations.

chapter

7 Configuring ISDN Call Destinations

The WAN Call Directory is a list of ISDN Call Destination Configurations. In general, you have to create one ISDN Call Destination configuration for each destination (LANs and remote nodes) your router will communicate with.

Before you start configuring ISDN call destinations, you should be aware of how the NetWare® MultiProtocol Router™ for ISDN 3.1 identifies and treats outgoing and incoming calls.

Outgoing calls are identified by the unique Call Destination Name of an ISDN call destination. The call destination names are for example used within the protocol bindings and identify the target when calls are set up with CICCON or CALLMGR.

Incoming calls are treated as follows:

- First, the NetWare MultiProtocol Router for ISDN checks whether it can find the CLI number transmitted over the D channel in a call destination´s CLI List.
- If not, it takes the Default Call Destination Configuration of the interface to which the call is directed and switches through the B channel with the parameters defined in the default destination.
- In the next step, it compares the number transmitted over the B channel (caller-specified number) with the entries for ISDN Number in the configured ISDN call destinations.
- If it does not find a corresponding entry, it checks the transmitted system ID with the Remote System IDs configured in the call destinations.
- If this is not successful either, the call is accepted with the parameters defined in the Default Call Destination Configuration for the specified interface.

If one of the checks is successful, the call is accepted with the parameters defined in the corresponding ISDN call destination configuration.

Special configuration scenarios are described in the following chapters of this Guide:

- Chapter 9, "Configuring IPX"
- Chapter 10, "Configuring TCP/IP"
- Chapter 11, "Configuring AppleTalk"
- Chapter 12, "Configuring Source Route Bridge"
- Chapter 13, "Advanced Configuration"
- Chapter 14, "Configuration Interdependencies"
- Chapter 15, "Configuring Remote Node Access"

This chapter contains the following sections:

- "Configuring an ISDN Call Destination" on page 116
- "Changing ISDN Call Destination Parameters" on page 150
- "Deleting an ISDN Call Destination" on page 151

Configuring an ISDN Call Destination

To configure ISDN Call Destinations, INETCFG is required. If INETCFG is not already loaded, load it by typing the following command at the server prompt:

```
LOAD INETCFG <Enter>
```

The *Internetworking Configuration* menu is displayed.

Proceed as follows:

Procedure

1. **From the *Internetworking Configuration* menu, select *WAN Call Directory*, then press** <Enter>**.**

   The *Configured WAN Call Destinations* window is displayed. This window has no entries if no ISDN Call Destinations are configured.

2. **Press** <Ins> **to configure a new ISDN Call Destination.**

   The prompt *New Call Destination Name*: allows you to enter a name of up to 47 alphanumeric characters for the new ISDN Call Destination.

The ISDN Call Destination name entered here is used in several other menu options when an ISDN Call Destination name needs to be identified. You should use a descriptive name, such as the name of the remote destination and whether it is a LAN or a remote node or a branch or store number.

3. **Enter a name for the new ISDN Call Destination, then press** <Enter>**.**

   A list of supported wide area media is displayed. These are media available on previously configured ISDN interfaces. If you have not yet configured such an interface, the respective medium is not displayed in this list.

   Note

   If you have not installed an ISDN-Controller and configured an interface before attempting to configure an ISDN Call Destination, you receive this message:

   ```
    WAN network interfaces must be configured
    before WAN Call Destinations may be created.
   ```

4. **Select a *Wide Area Medium* and press** <Enter>**.**

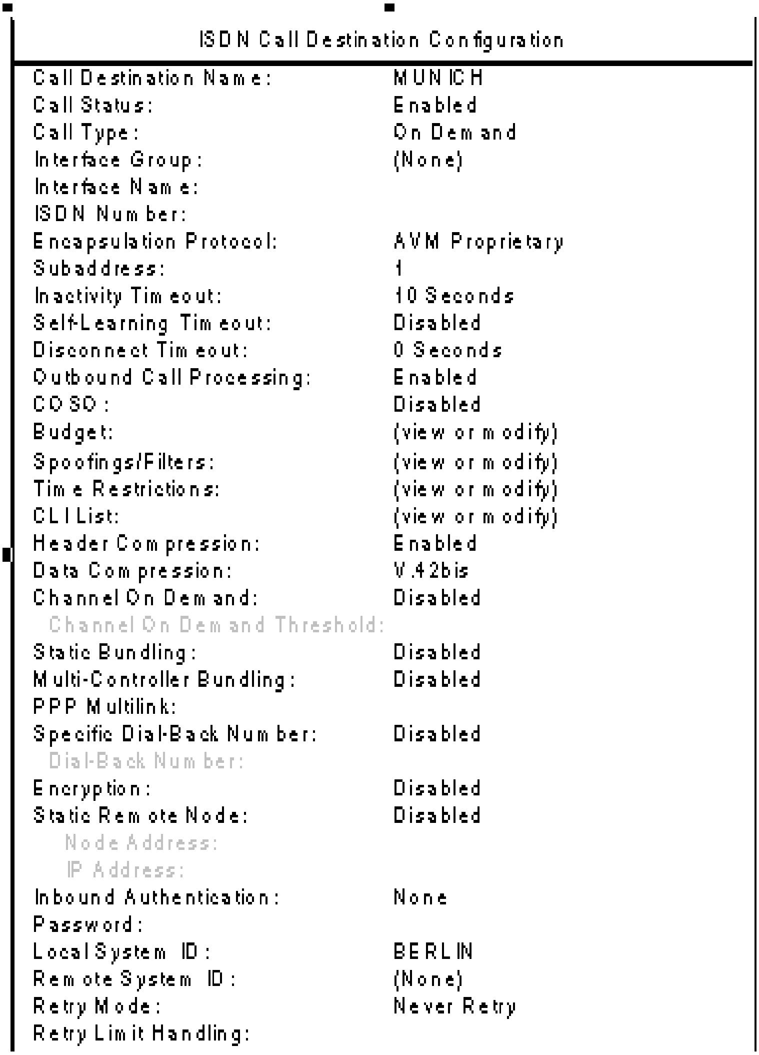
   The wide area media listed depend on which version of the NetWare MultiProtocol Router for ISDN 3.1 you have installled: the BRI version (ISDN-BRI), the PRI version (ISDN-PRI), or both.

   Select ISDN-BRI for AVM ISDN-Controllers for Basic Rate Interfaces (BRI).

   Select ISDN-PRI for AVM ISDN-Controllers for Primary Rate Interfaces (PRI).

   The *ISDN Call Destination Configuration* menu is displayed:

Figure 7-1:
ISDN Call Destination Configuration menu



```
                 ISDN Call Destination Configuration
Call Destination Name:          MUNICH
Call Status:                    Enabled
Call Type:                      On Demand
Interface Group:                (None)
Interface Name:
ISDN Number:
Encapsulation Protocol:         AVM Proprietary
Subaddress:                     1
Inactivity Timeout:             10 Seconds
Self-Learning Timeout:          Disabled
Disconnect Timeout:             0 Seconds
Outbound Call Processing:       Enabled
COSO:                           Disabled
Budget:                         (view or modify)
Spoofings/Filters:              (view or modify)
Time Restrictions:              (view or modify)
CLI List:                       (view or modify)
Header Compression:             Enabled
Data Compression:               V.42bis
Channel On Demand:              Disabled
  Channel On Demand Threshold:
Static Bundling:                Disabled
Multi-Controller Bundling:      Disabled
PPP Multilink:
Specific Dial-Back Number:      Disabled
  Dial-Back Number:
Encryption:                     Disabled
Static Remote Node:             Disabled
    Node Address:
    IP Address:
Inbound Authentication:         None
Password:
Local System ID:                BERLIN
Remote System ID:               (None)
Retry Mode:                     Never Retry
Retry Limit Handling:
```

5. Check the *Call Status.*

The Call Status defines whether or not the call destination may be used for outgoing and incoming calls. It allows you to disable a call destination entry without having to delete it from the WAN Call Directory.

Default: Enabled

Options: Enabled, Disabled, Time Restricted

Enabled means that outgoing and incoming calls to and from this destination are allowed.

Disabled means that no outgoing call can be done using this destination and incoming calls from this call destination are rejected. If this call destination´s CLI number is in the CLI List, incoming calls from this site are rejected on the D channel; i.e. no charges accrue for the caller.

Time Restricted lets you enable and disable the Call Status at specific times. Thus, you can disallow incoming and outgoing calls at the weekends, for example, or configure a call destination for occasional uploads or administration purposes. When a connection to this call destination is active and the Call Status changes to "Disabled", the connection is automatically terminated. A configured backup call destination would then be activated.

For information on configuring Time Restrictions, see Step 29 below.

6. **Check the *Call Type*.**

This parameter lets you specify how the outbound connection is maintained on the network protocol level.

Default: On Demand

Options: On Demand, Permanent

An on-demand connection is activated by data and terminated logically and physically when the Disconnect Timeout is reached. The Inactivity Timeout controls the physical connection. On Demand is the correct setting for circuit-switched lines.

A permanent connection is kept active continuously by reconnecting whenever the link goes down. The underlying physical connection is controlled by the Inactivity Timeout.

For D64S, DS01 and DS02, you have to set the Call Type to Permanent and set the Retry Mode (see Step 45) to an appropriate value.

When configuring backup calls, the Call Type must also be set to *Permanent*.

For detailed information on on-demand and permanent connections and classic and dynamic ISDN interface usage, refer to Chapter 4, "Basic Design of ISDN-WANs and Configuration Overview" in this Guide.

7. **Specify an *Interface Group* or an *Interface Name*.**

Specify the name of the interface or the interface group to initiate an outbound connection. The Interface Name or Interface Group is selected from a list of previously configured ISDN interfaces. You can specify an Interface Name or an Interface Group, but not both.

When you specify an Interface Name, this interface is always used for outgoing and incoming calls to and from this destination. If the interface is already in use for a different connection, the call set-up attempt fails.

When you specify an Interface Group, the system selects any available interface associated with the group for in- and outbound connection attempts.

8. **Specify the *ISDN Number*.**

Enter the complete number to reach the remote site you want to connect to.

Be sure that you enter the complete number. The complete number to enter here depends on how the respective ISDN device is connected to the public ISDN, on the location of the remote site and how the addressed ISDN adapter / device there is connected to the public ISDN. The ISDN Number of the remote site can therefore maximally consist of the following "components":

- PBX Outside Line Access (DO NOT FORGET !)
- International Dialing Prefix
- Country Code
- Area Code

- ISDN subscriber Number of the ISDN adapter / device in the remote router or PC (including PBX Extension, if it is connected to a PBX).

Warning

Entering the numbers here might be compared with dialing a number on the phone: if one digit is wrong you will get a wrong connection or no connection at all. Therefore make sure that you have the correct number of the remote site and that you enter it correctly.

For special connection types such as semipermanent and 56 Kbps connections, refer to Chapter 13, section "Special Connection Types" in this Guide.

9. Check the *Encapsulation Protocol*.

Default: AVM Proprietary

Options: AVM Proprietary, PPP over ISDN

The AVM Proprietary and PPP over ISDN protocols are different encapsulating methods for transferring network protocols over the ISDN B channel.

AVM´s market-proven proprietary protocol has been in practical use for more than four years. It is based on X.75SLP, which is standardized in ISDN. Since it offers more powerful features than PPP over ISDN such as data compression (according to V.42bis) and various line management features, it is the recommended protocol to be used for connections between AVM´s NetWare MultiProtocol Routers for ISDN and NetWare MultiProtocol Router for ISDN and AVM´s remote node product NetWAYS / ISDN. Both have been on the market since 1992 and support channel bundling and compression according to V.42bis.

PPP over ISDN has been an international standard since 1994 and is intended to provide interoperability between remote access products of different manufacturers over ISDN. Channel bundling (PPP MP), for example, has been defined in 1995.

Note

PPP over ISDN is not supported with the GSM protocol stack.

10. Specify the *Subaddress*.

The Subaddress is a supplement to the number that is dialed to reach the ISDN-Controller configured at the remote site, and specifies the concrete address of its logical interface. The Subaddress is not used for PPP connections.

Enter the address of the interface for this particular call destination.

The entry in this field must be identical with the Origination Subaddress configured for the respective interface of the ISDN-Controller at the opposite end of the link. Otherwise the call is rejected and one charge unit is wasted.

11. Check the *Inactivity Timeout*.

Since charges accrue for the duration of a call whether data is being transferred or not, this feature is essential for saving connection charges.

The Inactivity Timeout deactivates an existing ISDN connection physically if no data traffic is detected in either direction for the specified period of time. This process is transparent to all workstations linked over this ISDN connection, since the logical (protocol specific) connection between both sites is maintained, and the physical connection is automatically re-established within 1 or 2 seconds, if data traffic is detected for the remote site.

Default:	10 seconds
Options:	0 seconds to 59 min 59 sec (0=disabled); Time-Controlled

You can either specify a fixed value for the Inactivity Timeout or select Time-Controlled and configure different Inactivity Timeout values for different times in the Time Restrictions menu (see Step 29). The latter is useful when you cannot use the Self-Learning Timeout (for example Advice On Charge During Call not activated) and want to configure times at which the Inactivity Timeout is changed to adapt it to the different day and night tariffs of the ISDN network.

If you want to use a fixed Inactivity Timeout, set the value appropriate for the call destination; i.e. take the meter clock pulse valid for the current call destination and set the Inactivity Timeout a little lower. Thus, the Inactivity Timeout will disconnect the ISDN connection physically shortly before the next charge unit will be counted.

Note

For information on the charge intervals, please contact your local PTT.

Setting this timeout value to zero disables the Inactivity Timeout facility.

Important

If you disable the Inactivity Timeout, keep in mind that the ISDN line is maintained physically from the first set up to the final clear down, whether data is transferred or not. This means that charges accrue for this whole period!!! Therefore, never set the Inactivity Timeout to "0" if standard circuit-switched lines are used.

Note

Please keep the following in mind: if the physical ISDN connection is cleared by the Inactivity Timeout, the interface of the ISDN-Controller maintains the logical connection and thus rejects all incoming calls from any other remote sites (except when Remote Node Usage is set to On Demand Interface Reservation). This means that if a different site tries to establish an ISDN connection to that interface, the call will be switched through by the local exchange, but the ISDN-Controller will disconnect this incoming call and reject establishment of the logical connection to this interface, since it is already in use.

12. **Check the *Self-Learning Timeout*.**

The Self-Learning Timeout automatically adjusts the Inactivity Timeout for outgoing connections to different charge intervals over the day. To calculate the appropriate timeout value, the intervals between two charging pulses sent by the PTT are measured.

To use the Self-Learning Timeout, the following requirements must be met:

- Advice On Charge During Call (AOCD) must be activated at your ISDN access
- the connection charges must be counted during the ISDN connection and not only at the end of the connection.

Default: Disabled

Options: Enabled, Disabled

When the Self-Learning Timeout is enabled, the NetWare Multi-Protocol Router for ISDN sets the Inactivity Timeout to one charge interval minus two seconds. The new value is displayed on the system console as "`Calculated Self-Learning Timeout <x>`" when

- you set up a physical connection and the Self-Learning Timeout has been calculated for the first time.
- the meter clock pulse changes and a new Self-Learning Timeout is calculated.

For information on the influence of the Self-Learning Timeout and the Disconnect Timeout, refer to Chapter 14, section "Operation of the Self-Learning Inactivity Timeout" in this Guide.

13. Check the *Disconnect Timeout*.

When the Inactivity Timeout clears down an idle connection physically, a logical connection is maintained, which means that all line management parameters negotiated during the initial call set-up remain valid. The logical connection is controlled by the Disconnect Timeout. When the Disconnect Timeout expires, the logical network connection to the remote LAN is cleared as well. The interfaces of the ISDN-Controllers at both the local and the remote site are no longer reserved for this connection, and, if a routing protocol is used, the remote LAN "vanishes". This may be compared to pressing <Del> on an entry with the status "In-Connected" or "Out-Connected" in the CALLMGR to clear connections.

Default:	0 (=disabled)
Range:	0 seconds to 18 hours (0=disabled); Same as Inactivity Timeout

Set the Disconnect Timeout value appropriate for the ISDN Call Destination, if necessary.

The value for Disconnect Timeout must be higher than or equal to the value for Inactivity Timeout. The difference between the two is the period after which the connection is cleared logically as well.

Example: Inactivity Timeout = 10 seconds; Disconnect Timeout = 2 hours

-> The physical connection is cleared after 10 seconds whereas the interface is cleared logically after 2 hours of inactivity. If data traffic is detected within these 2 hours, the Inactivity Timeout and Disconnect Timeout begin to count anew.

If you want to clear interfaces for other connections after a certain period of inactivity, set the Disconnect Timeout to "Same as Inactivity Timeout".

Setting this timeout value to zero disables the Disconnect Timeout. For on-demand connections, the interface that has been handling the connection to the current call destination will be reserved for this call destination (except when Remote Node Usage is set to "On Demand Interface Reservation") until: the Inactivity Timeout expires, the connection is cleared manually (CALLMGR or CICCOFF), the Call Status of this destination expires (if Time Restrictions are configured), one of the interface threshold values or one of the call destination´s budget values is reached.

14. Check the *Outbound Call Processing*.

This parameter defines whether or not initial outgoing calls are allowed to this destination.

Default:	Enabled
Options:	Enabled, Disabled, Time Restricted

When Outbound Call Processing is enabled, outgoing calls to this destination are possible.

When this parameter is disabled, no initial outgoing calls are allowed to this destination. Only incoming calls from this destination are allowed. This makes sense whenever the protocol requires a local destination configuration (for examples for static routes), but you do not want to allow initial outgoing calls to this destination.

Note

Please note that this does not affect calls performed after an inactivity timeout. These calls are allowed if the initial call was set-up by the remote site and can be controlled via COSO or Interface Outbound Call Processing.

Time Restricted lets you enable and disable Outbound Call Processing at specified times. This can be used for security purposes, to allow connections only at certain times (for example to transfer e-mails only at the weekend) and to save connection charges.

For more information on configuring Time Restrictions, refer to Step 29.

15. **Check the setting for *COSO*.**

COSO (Charge One Site Only) lets you define which site of an ISDN connection is to assume the charges.

Default:	Disabled
Options:	Disabled, Local, Remote, No Dial-Out, Time Restricted

When COSO is disabled, the site that established the (underlying) physical connection assumes the charges.

When you set COSO to Local, your site assumes the total connection costs. In this case, your router identifies an incoming call from this site by the number delivered on the D channel (CLI number), rejects the call and calls back. This is why you must enter the CLI number of this remote site in the CLI List (see Step 30).

When you set COSO to Remote, the following happens: Each time your router has to transfer data to this remote site, it will issue a call set-up request over the D channel. It expects that the remote site rejects the call and calls back to assume the charges. If the remote site does not reject the call on the D channel, the connection is switched through on the B channel(s) and connection charges accrue for your site. In this case, COSO is automatically changed to "No Dial-Out" and the connection is cleared. No further charges accrue for your site.

When you set COSO to No Dial-Out, no call set-up request is issued over the D channel. All kinds of outgoing calls to this destination are barred.

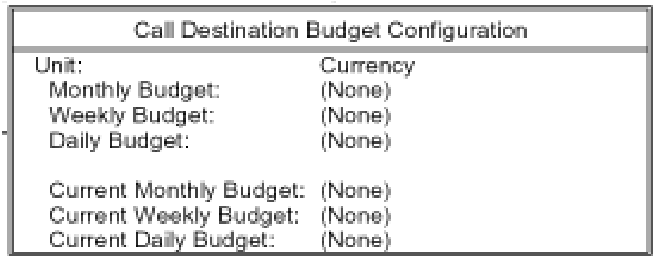
Time-Restricted lets you define times and days at which you want to change COSO automatically. For information on how to configure time restrictions, refer to Step 29.

For an example for the use of COSO, refer to the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*.

16. **Press** <Enter> **on *Budget*.**

The following menu is displayed:

Figure 7-2:
Call Destination Budget Configuration menu



```
              Call Destination Budget Configuration
Unit:                       Currency
  Monthly Budget:           (None)
  Weekly Budget:            (None)
  Daily Budget:             (None)

  Current Monthly Budget:   (None)
  Current Weekly Budget:    (None)
  Current Daily Budget:     (None)
```

Here you can specify the maximum amount of money or the maximum number of charge units you want to spend for a call destination per month, week and day.

The lower half of the menu shows the amounts that have been spent so far in the specified period.

When one of the maximum values is reached, the connection to the remote site is cleared and incoming and outgoing connections to this call destination are no longer allowed. To allow connections again, either set the expired budget value to (None) or configure a higher value. The current values are not reset when one of the maximum values is reached!

16a. Select the *Unit* in which you want to configure the budgets.

Default: Currency

Options: Currency, Charge Units

The currency display and the cost of one charge unit are configured in the *Global MPR for ISDN Configuration*. For more information, refer to Chapter 8, "Global Configuration".

16b. *Monthly Budget*.

Default: (None)

Enter the maximum amount of money or the maximum number of charge units you want to spend for this call destination per month.

16c. ***Weekly Budget*.**

Default: (None)

Enter the maximum amount of money or the maximum number of charge units you want to spend for this call destination per week.

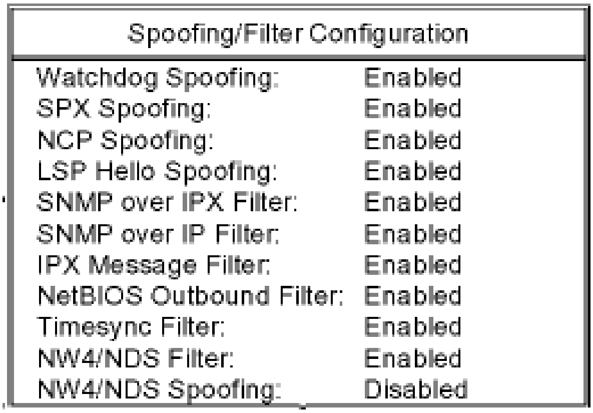
16d. ***Daily Budget*.**

Default: (None)

Enter the maximum amount of money or the maximum number of charge units you want to spend for this call destination per day.

17. To set spoofings and filters for this call destination, press <Enter> **on *Spoofings/Filters* to display the following menu:**

Figure 7-4:
Spoofing/Filters Configuration menu



Spoofing/Filter Configuration

Watchdog Spoofing:	Enabled
SPX Spoofing:	Enabled
NCP Spoofing:	Enabled
LSP Hello Spoofing:	Enabled
SNMP over IPX Filter:	Enabled
SNMP over IP Filter:	Enabled
IPX Message Filter:	Enabled
NetBIOS Outbound Filter:	Enabled
Timesync Filter:	Enabled
NW4/NDS Filter:	Enabled
NW4/NDS Spoofing:	Disabled

Warning

Please be very careful when changing the defaults for the parameters in this menu. All these filter and spoofing mechanisms are provided to hold the physical ISDN connection to remote LANs and remote node clients and the NetWare MultiProtocol Router for ISDN down as long as possible in order to avoid ISDN connection charges. Changing one of the defaults will, in most cases, result in frequent ISDN call set-ups to transmit the packets not filtered or spoofed. This will cause unneccessarily high ISDN connection charges. Therefore, you should never change one of the default values preconfigured for the above listed parameters, unless you are sure you have to change one of the defaults and are aware of the consequences.

Spoofing and filtering can be performed on both, the network protocol and the ISDN driver layer. On the network layer, filters and spoofings are configured via Bind Options or via FILTCFG. For more information, refer to the *NetWare MultiProtocol Router 3.1* documentations.

For connecting networks via ISDN, however, spoofing and filtering on the ISDN driver level is much more effective. The NetWare MultiProtocol Router for ISDN 3.1 provides filter and spoofing mechanisms for a large number of packets.

Spoofed and filtered packets can be made visible via a packet trace. Packet Trace can be enabled in the ISDN Console or via the MPR for ISDN Router Manager and Router Agent. Filtered packets will be displayed as "Dropped-Send", spoofed packets as either "Local-Send" or "Local-Receive".

18. Check the *Watchdog Spoofing*.

NetWare servers send out so called "Watchdog" packets at regular intervals (default: every 5 minutes) to poll the status of IPX clients; i.e. they check that clients that have logged into the server are still "alive".

Watchdog packets can be spoofed on the network protocol level by enabling the "On Demand Spoofing" parameter in the IPX binding options, as well as on the ISDN driver level with the parameter "Watchdog Spoofing".

Default:	Enabled
Options:	Enabled, Disabled

When Watchdog Spoofing is enabled, Watchdog packets are confirmed by the NetWare MultiProtocol Router for ISDN on the local site and will not be transmitted via ISDN to the remote site.

When this parameter is disabled, an ISDN connection will be set up each time watchdog packets are to be transferred.

19. Check the *SPX Spoofing*.

Many applications use SPX besides IPX. When SPX is used, so-called "SPX keep-alive packets" are exchanged frequently (average every 50 seconds) between the client and the application server (host) to check whether the same application is still running. These packets must be acknowledged on both sides in order to maintain the session.

On the server, two solutions are provided: one on the network protocol and on on the ISDN driver level.

On the network level, propagation of SPX Keep-Alive packets can be turned off by using SPXWDOG.NLM on the server and the corresponding mechanism on the client. See the *NetWare MultiProtocol Router 3.1 Release Notes*, p. 40, for information about using SPXWDOG.

The NetWare MultiProtocol Router for ISDN provides SPX Spoofing on the ISDN driver level to acknowledge SPX keep-alive packets issued by the application server locally, and not to transmit them over ISDN to the client site. If the ISDN connection to the client site is cleared, the NetWare MultiProtocol Router for ISDN will stop acknowledging keep-alive packets issued by the application server. In this way, the ressources reserved for the client will be released after 75 minutes at the latest if the user at the client site switches off the PC without logging out properly. This is indispensible for host sessions and database applications, since otherwise the reserved ressources would never be released.

Default: Enabled

Options: Enabled, Disabled

When SPX Spoofing is enabled, SPX keep-alive packets issued by the application server are never transmitted to the remote site, but are acknowledged locally by the NetWare MultiProtocol Router for ISDN.

If you select "Disabled", ISDN connections over this interface to remote sites would be set up when SPX keep-alive packets, generated by the server component, are to be transferred.

Warning

For the client application, it is absolutely necessary to transmit a keep-alive packet at least every hour to check whether the server is still there.
To minimize call set-ups initiated by the client, you must set the SPX-specific timers on the client to a value appropriate for use with ISDN. This is done in the network configuration of the client. A value of 65 000 for "spx verify timeout" and "spx abort timeout" will let the client issue appr. one SPX keep-alive packet per hour.

20. Check the *NCP Spoofing*.

Default: Disabled

Options: Enabled, Disabled

NCP Spoofing prevents the ISDN transmission of "get directory path" and "end of job" requests (NCP request type 2222, transported over IPX packet type 17) often issued in conjunction with a File Open box in any Windows, Windows for Workgroups or Windows 95 application such as Word for Windows. The number and frequency of such NCP requests depends on whether Micosoft´s or Novell´s NetWare Requester is used.

When NCP Spoofing is disabled, all NCP requests type 2222 are transmitted over ISDN to all remote servers this client has drive mappings on.

21. Check the *LSP Hello Spoofing*.

When NLSP is used over ISDN links, the protocol regularly sends out so-called LSP Hello Packets (default: every 20 seconds, maximum: every 600 seconds). The interval in which these packets are sent can be configured via the "NLSP Convergence Rate Configuration" menu (parameter "Non-Broadcast Hello Interval").

LSP Hello Spoofing is provided to confirm WAN LSP Hello packets locally on the NetWare MultiProtocol Router for ISDN for each interface. This avoids frequent call set-ups over ISDN and thus saves connection charges.

Default: Enabled

Options: Enabled, Disabled

When LSP Hello Spoofing is enabled, LSP Hello Packets are confirmed locally on the NetWare MultiProtocol Router for ISDN and are not transmitted over ISDN.

If it is disabled, ISDN connections to remote sites would be set up over this interface each time the router creates LSP Hello Packets.

22. Check *SNMP Over IPX Filter*.

Many network management systems/applications use SNMP to gather network information.

This parameter specifies whether SNMP over IPX packets (Socket 900F), SNMP Traps over IPX packets (Socket 9010) and IPX diagnostic packets (Socket 456) are filtered.

Default: Enabled

Options: Enabled, Disabled

When the SNMP over IPX Filter is enabled, SNMP information transported over IPX by the source or destination socket numbers 900F, 9010 and 456 are filtered and not transmitted over this interface to any remote site.

When this filter is disabled, ISDN connections to remote sites will be set up each time when those packets generated by the SNMP applications are to be transferred.

Example: For the NetExplorer of NMS / ManageWise, the IPX Diagnostic Packets send for the Workstation Discovery Process would be filtered.

23. Check the *SNMP Over IP Filter*.

In conjunction with SNMP, the protocol IP can also be used to transmit SNMP-related packets.

This parameter specifies whether SNMP over UDP packets (port 161) and SNMP Traps over UDP packets (port 162) are filtered.

Default: Enabled

Options: Enabled, Disabled

When the SNMP over IP Filter is enabled, SNMP information transported over IP by the source or destination ports 161 and 162 are filtered and not transmitted over this interface to any remote client.

When this filter is disabled, ISDN connections to remote sites will be set up each time when those packets, generated by the SNMP applications, are to be transferred.

Example: For the NetExplorer of NMS / ManageWise, the IP Diagnostic Packets send for the Workstation Discovery Process would be filtered.

24. Check the *IPX Message Filter*.

When a problem occurs on a NetWare server (e.g. "Server out of disk space") or when a client issues a message (e.g. "Send to all"), the corresponding warning or message is sent to all clients that are logged in to that server. Afterwards, so-called "IPX Broadcast Message Waiting" packets are sent to these clients in 2 second intervals, until this warning or message is confirmed by the clients. This does not cause any problems within a LAN, but when two LANs are connected over ISDN, the following situation may appear:

Clients log in to a server over ISDN and Watchdog Spoofing is enabled on the local router. Watchdog packets that poll the status of IPX clients are consequently confirmed on the router as long as the clients connected over ISDN are registered to be logged in to the server. If the user of such a client forgets to log out before switching the PC off and leaving the office (a quite common behaviour), the client is still registered to be logged in. Or, users of clients connected over ISDN leave their desks for hours. In both cases, IPX Broadcast Message Waiting packets cause the ISDN line to stay up all the time because they are not confirmed until the clients log in to the server the next day or the users return to their desks.

Another method, entering "castoff", has been reported not to work on Windows clients under certain conditions and has a major disadvantage: no messages are sent to those clients at all. Thus, the IPX Broadcast Message Waiting Filter enhances especially your LAN-LAN links in two ways:

Users at their clients will receive such messages / warnings. The IPX Broadcast Message Filter starts counting the subsequent "IPX Broadcast Message Waiting" packets issued over ISDN to clients as soon as no data packets are concurrently transferred over such an ISDN link and starts filtering after five of these packets have passed (after ten seconds, if the default polling interval of 2 seconds is used). As soon as the Inactivity Timeout expires, the ISDN link is cleared physically. If the ISDN line is set up again to transmit data, this filter is reset and begins to count anew as described above.

For Remote Node-LAN connections with NetWAYS / ISDN, the situations described are very unlikely to cause such ISDN links to stay up because of Disconnect Timeout and other mechanisms implemented for Remote Node-LAN links, however this filter naturally applies for both LAN-LAN and Remote Node-LAN links.

Default: Enabled

Options: Enabled, Disabled

The following example shows how the filter works:

When a NetWare server or a client issues a message or warning (e.g. an "NLM" on the server such as ARCserve, or a user using the "send" command on a client), this will be transported to the addressed clients, also to those connected via ISDN. The IPX Broadcast Message Filter starts counting the subsequent "IPX Broadcast Message Waiting" packets issued over ISDN to clients as soon as no data packets are concurrently transferred over such an ISDN link and starts filtering after five of these packets have passed (after ten seconds, if the default polling interval of 2 seconds is used) and disables the ISDN link as soon as the Inactivity Timeout expires. If the ISDN line is set up again to transmit data, this filter is reset and begins to count anew as described above.

25. Check the ***NetBIOS Outbound Filter***.

Windows-based systems frequently initiate NetBIOS broadcasts. For the transmission of NetBIOS packets within IPX, IPX Packet Type 20 is used.

On the network protocol layer, NetBIOS broadcasts can be filtered by enabling the "Advanced Packet Type 20 Flooding" parameter in the IPX expert configuration or via FILTCFG.NLM.

The NetBIOS Outbound Filter allows outbound filtering of IPX Type 20 packets on the ISDN driver level to prevent them from being transmitted to remote sites over ISDN.

Default: Enabled

Options: Enabled, Disabled

When the NetBIOS Outbound Filter is enabled, NetBIOS broadcasts transmitted over IPX Type 20 packets are filtered, and therefore not transmitted over ISDN to remote sites.

If this filter is disabled, ISDN connections to remote sites are set up by the NetWare MultiProtocol Router for ISDN each time such a broadcast packet is to be transferred.

26. **Check the *Timesync Filter*.**

In a NetWare 4 environment, NetWare Directory Services (NDS) is distributed across the network. When users or objects are added to the directory, they are added to the local copy of the database and then propagated throughout the network to other copies (replicas) of the database. If the same object is modified in two different replicas, the order of the modification must be preserved to correctly propagate the changes. One way to ensure the correct ordering of directory events is to time stamp them. Without a common time source, each of the NDS servers can have a different reference time. Time synchronization solves this problem by synchronizing the time among NDS servers in the network.

On the network protocol level, you can use the TIMESYNC.NLM to reduce the frequency in which Time synchronization packets are sent. For more information, refer to the *NetWare MultiProtocol Router 3.1 Release Notes,* pp. 48-50.

The Timesync Filter filters NCP requests type 114 that are used to synchronize time between NDS servers on the ISDN driver level. In this case, you have to use a different mechanism to synchronize NDS servers, for example by using external clock devices.

Default:	Enabled
Options:	Enabled, Disabled

When the Timesync Filter is enabled, NCP requests type 114 are not sent over ISDN to other NDS servers in the WAN.

When you disable the filter, an ISDN connection is set up each time if time synchronization packets are issued.

27. **Check the *NW4/NDS Filter*.**

In all versions of NetWare 4, the NDS synchronization logic checks with each server in its replica list regularly to determine whether any changes have occurred. There are different processes with different synchronization tasks. Examples are the Heartbeat, Backlink and Schema process. Each synchronization is initiated with a so-called Ping-for-NDS packet (NCP request type 104).

To reduce the NDS synchronization packets, two solutions are provided:

One possibility is to use two NLMs (DSFILTER.NLM and PINGFILT.NLM) delivered with the product. These filters must be installed and configured on each NetWare 4 server in the internetwork. For more information on how to configure and use these filters, refer to the *NetWare MultiProtocol Router 3.1 Release Notes*, pp. 51-55.

The second solution is to use the NW4/NDS Filter, which filters Ping-for-NDS packets on the ISDN driver level to prevent them from being sent over ISDN.

Default: Enabled

Options: Enabled, Disabled

When the NW4/NDS Filter is enabled, NCP requests type 104 packets are filtered and not sent over ISDN to each remote NetWare 4 server in the NDS tree.

When you disable the NW4/NDS Filter, an ISDN connection is set up to all remote LANs with NDS servers each time an NCP request type 104 is issued.

28. **Check the *NW4/NDS Spoofing*.**

The NW4/NDS Spoofing acknowledges Ping-for-NDS packets (NCP request type 104) locally and prevents them from being sent over ISDN to all remote NetWare 4 servers in the NDS tree. However, NDS synchronization is required in regular intervals. This is why NDS Pass Through Times must be configured on the NetWare MultiProtocol Router for ISDN 3.1 to allow initiation of synch processes by Ping-for-NDS packets.

Default: Disabled

Options: Disabled, Enabled, Time Restricted

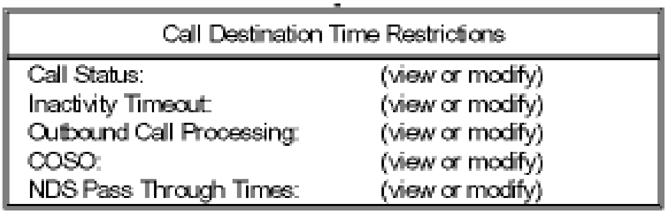
When NW4/NDS Spoofing is enabled, the NetWare MultiProtocol Router for ISDN acknowledges Ping-for-NDS packets locally and sends back error 663 (DS is locked).

To make sure that synchronization throughout the WAN is effected in regular intervals, select Time Restricted and configure NDS Pass Through Times and use the NDSSYNC.NLM. For more information, refer to Step 29e below and to the *Technical Note*.

When you disable NW4/NDS Spoofing, an ISDN connection is set up to all remote LANs with NDS servers each time a Ping-for-NDS packet is issued.

29. Check the *Time Restrictions*. Press <Enter> **on this parameter to display the following window:**

**Figure 7-3:
Time Restrictions menu**

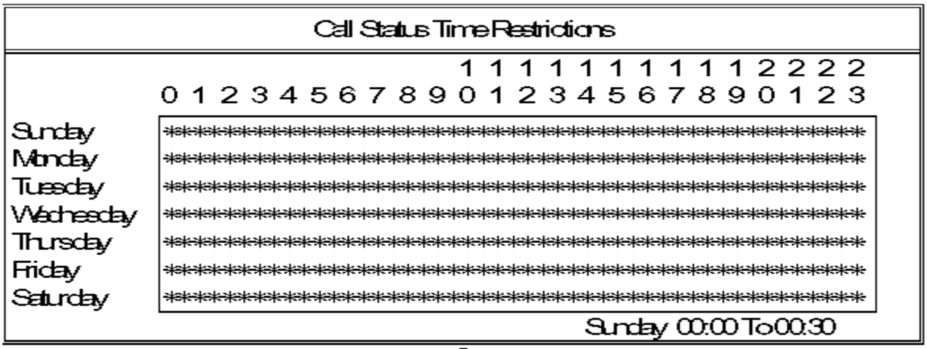


```
           Call Destination Time Restrictions
Call Status:                     (view or modify)
Inactivity Timeout:              (view or modify)
Outbound Call Processing:        (view or modify)
COSO:                            (view or modify)
NDS Pass Through Times:          (view or modify)
```

29a. *Call Status*.

When you press <Enter> on *Call Status*, the following window appears:

**Figure 7-4:
Call Status Time Restrictions Configuration menu**



```
                        Call Status Time Restrictions
                               1 1 1 1 1 1 1 1 1 1 2 2 2 2
           0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
Sunday     ************************************************
Monday     ************************************************
Tuesday    ************************************************
Wednesday  ************************************************
Thursday   ************************************************
Friday     ************************************************
Saturday   ************************************************
                                     Sunday 00:00 To 00:30
```

In this window you can determine the days and times during which the current call destination can be dialed and calls from it are accepted. Out of these times no outgoing or incoming connections to or from this call destination are possible.

When a connection to this call destination is active and the Call Status changes to "Disabled", the connection is automatically terminated. No outgoing calls to this destination are possible and incoming calls from it are rejected. A configured backup call destination would then be activated.

As you can see, all the input fields are already filled in with asterisks. This means the call destination can be used each day of the week and every hour of the day.

To deny use at certain times, delete the corresponding asterisks by pressing <Del> or the Space Bar. To restore the asterisks, press <Ins> or *.

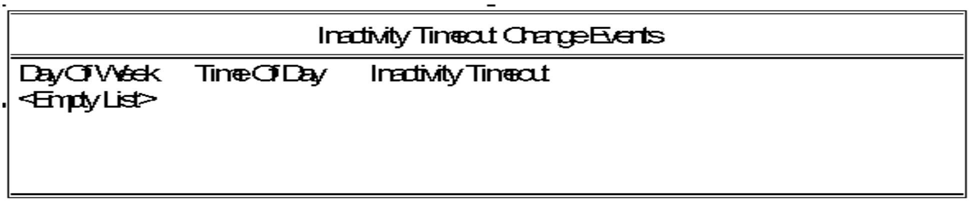
The key assignment is similar to that in the SYSCON utility (NetWare 3.12) and NETADMIN / NWADMIN utilities (NetWare 4.x).

To leave the menu and return to the *Call Destination Time Restrictions* menu, press <Esc>.

29b. ***Inactivity Timeout.***

Press <Enter> on *Inactivity Timeout* to display the following menu:

Figure 7-5:
Inactivity Timeout Change menu



```
Inactivity Timeout Change Events

Day Of Week    Time Of Day    Inactivity Timeout
<Empty List>
```

In this list you can determine days and times at which you want the Inactivity Timeout to be changed automatically. This is useful when you cannot use the Self-Learning Timeout (for example Advice On Charge During Call not activated) and want to configure times at which the Inactivity Timeout is changed to adapt it to the different day and night tariffs of the ISDN network.

Initially, the list is empty.

To enter a new time, press <Ins>. Enter the *Day of Week*, the *Time of Day* and the new *Inactivity Timeout* value in the menu and press <Esc>. The new time is now shown in the list.

29c. *Outbound Call Processing*.

When you press <Enter> on *Outbound Call Processing*, a window similar to that for *Call Status Time Restrictions* is displayed.

This menu lets you enable and disable Outbound Call Processing at specified times. This can be used for security purposes, to allow connections only at certain times (for example to transfer e-mails only at the weekend) and to save connection charges.

29d. *COSO*.

Press <Enter> on *COSO* to display a menu similar to that for Inactivity Timeout (see above).

In this list you can determine days and times at which you want COSO to be changed automatically. Initially, the list is empty.

To enter a new time, press <Ins>. Enter the *Day of Week*, the *Time of Day* and the new setting for *COSO* in the menu and press <Esc>. The new time is now shown in the list.

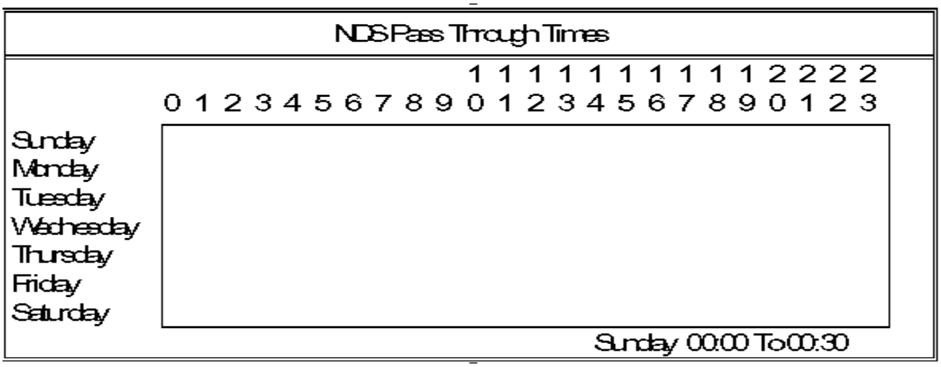
29e. *NDS Pass Through Times*.

NDS databases must be updated in regular intervals. Thus, if you NW4/NDS Spoofing to Time Restricted above, you have to define days and times at which so-called Ping for NDS packets are not spoofed in order to enable synchronization within the WAN.

To save money, you can use the NDS Pass Through Times to allow updates in times where connections charges are low, for example during the night.

When you press <Enter> on *NDS Pass Through Times*, the following menu is displayed:

Figure 7-6:
NDS Pass Through Times Configuration menu



```
                         NDS Pass Through Times
                                         1 1 1 1 1 1 1 1 1 1 2 2 2 2
             0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
                                             Sunday 00:00 To 00:30
```

As you can see, all the input fields are empty.

To allow transmission of Ping for NDS packets at certain times, press <Ins> or *.

Press <Esc> until you return to the *ISDN Call Destination Configuration* menu.

For more information on initiation of Ping-for-NDS packets, refer to the *Technical Note*.

30. Press <Enter> **on *CLI List*.**

The CLI List is a database containing all CLI numbers of this remote site for incoming calls. The CLI number is required

- to relate an incoming call to a configured call destination (see explanation at the beginning of this chapter).
- to perform a security check if Call Acceptance is set to "Only Registered Numbers: CLI" or "Only Registered Numbers: CLI and Caller-Specified".
- if you set COSO to "Local". In this case, the CLI number is used to determine whether your router is allowed to assume the charges for calls from this remote site.

30a. To enter the CLI number of a new remote site, press <Ins>**.**

30b. Enter the CLI number of the remote site.

Important

If the remote site calls you from a call number pool, you have to register all remote CLI numbers in that pool in your CLI List for the call destination.

30c. To return to the *ISDN Call Destination Configuration*, press <Esc> **and save your changes.**

31. Check the *Header Compression*.

Header Compression is a set of standard compression options intended to eliminate nonessential information from the network protocol header and maximize the bandwidth available from ISDN connections. IPX headers can maximally be compresses from 36 to 2 bytes, and TCP / IP headers from 40 to 3 bytes.

According to the network protocol used, CIPX Header Compression (RFC 1553) or Van Jacobsen TCP / IP Header Compression (RFC 1144) can be enabled.

Header compression can also be performed on the network protocol level for IPX. It is configured in the *Expert Binding Options*. However, header compression on the ISDN driver level is more effective since compression is performed on the ISDN-Controller and does not take memory from the server.

Note

Header Compression is negotiated during call set-up with a remote site. If the remote site is not able to apply it, it is not used.

Default:	Enabled
Options:	Enabled, Disabled

If Header Compression is performed on the ISDN driver level, header compression on the network protocol level is switched off.

After header compression, data compression according to V.42bis can be applied.

32. Check the *Data Compression*.

This parameter specifies whether the data shall be compressed during transmission to increase transmission rate. Data compression is more effective than header compression and achieves a compression rate of up to 8:1.

Default:	V.42bis
Options:	No Compression, V.42bis

When data compression is performed on the ISDN-Controller, the server memory is not burdened with this task. Per B channel, 128 bytes are downloaded on the ISDN-Controller.

33. Check *Channel On Demand*.

If a large amount of data packets is to be transferred, it may be favorable to use more than one data channel to accelerate transmission. By bundling the data channels the bandwidth can be increased considerably.

Channel On Demand allows flexible use of the available ISDN data channels on one ISDN-Controller by automatically activating the required data channels if a large number of data packets has to be transferred.

If you have *more than one* AVM ISDN-Controller installed and configured on your router, refer to Step 36 below, "Multi-Controller Bundling".

Note

When two or more channels are bundled on demand, the connection charges are of course multiplied by the number of data channels used. Please keep this in mind when configuring this parameter.

Important

If you want to use Channel On Demand, the required data channels must be available for this connection on the ISDN-Controller of both the local and the remote site. For more information on this, refer to Chapter 14, section "Static Bundling and Channel On Demand" in this Guide.

Default:	Disabled	
BRI:	Options:	Disabled, Enabled
PRI:	Options:	Disabled, 1 B Channel, 2 B Channels, 3 B Channels, ..., 15 B Channels

If Channel On Demand is disabled, only one data channel is used for an ISDN connection, irrespective of the number of data packets transferred. The other data channel(s) available on the ISDN-Controller may be used separately by other ISDN Call Destinations for the other interface(s).

If Channel On Demand is enabled on an AVM ISDN-Controller for BRI, the second data channel is switched through automatically if the load exceeds the configured Channel Allocate Threshold (see Step 34a).

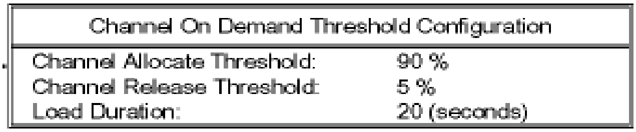
If you want to use Channel On Demand on an AVM ISDN-Controller for PRI, specify the number of additional data channels to be switched through automatically if the load exceeds the configured Channel Allocate Threshold (see Step 34a).

When the load falls below the configured Channel Release Threshold (see Step 34b), the additional data channels are again deactivated.

34. If you enabled *Channel On Demand* above, press <Enter> **on *Channel On Demand Threshold*.**

The following menu is displayed:

Figure 7-7:
Channel On Demand Threshold Configuration menu



```
          Channel On Demand Threshold Configuration
 Channel Allocate Threshold:          90 %
 Channel Release Threshold:           5 %
 Load Duration:                       20 (seconds)
```

34a. Enter the *Channel Allocate Threshold* in per cent.

This parameter defines the load per data channel in per cent at which the next channel is switched through for transmission.

Default: 90 %

Range: 0 - 100 % (0=disabled)

The basis for channel allocation is the net throughput rate displayed in the ISDN Console.

Example: If you enter 90 %, an additional channel will be switched through when the load reaches 90 % of the load one channel can handle (64 Kbps) over the Load Duration (see below).

34b.Enter the *Channel Release Threshold* in per cent.

Default: 5 %

Range: 0 - 100 % (0=disabled)

If you set a value for the Channel Release Threshold, the additional channel(s) is (are) disconnected when the load is below the threshold over the Load Duration (see below).

When the Channel Release Threshold is set to 0%, the additional channel(s) is (are) only deactivated when the Inactivity Timeout expires.

34c. Specify the *Load Duration*.

The Load Duration defines the time during which the load must match the Channel Allocate Threshold or the Channel Release Threshold before additional channels are switched through or disconnected.

35. Check *Static Bundling*.

Static Bundling specifies whether a specified number of data channels is automatically bundled on an ISDN-Controller each time a physical connection is set up to the current ISDN Call Destination, thus increasing the bandwidth to a multiple of 64 Kbps, irrespective of the actual data traffic.

If you have *more than one* AVM ISDN-Controller installed and configured on your router, refer to Step 36 below, "Multi-Controller Bundling".

Note

When two or more data channels are bundled, the connection charges are of course multiplied by the number of data channels used. Please keep this in mind when configuring this parameter.

Important

If you want to use Static Bundling, the required data channels must be available for this connection on the ISDN-Controller of both the local and the remote site. For more information on this, refer to Chapter 14, section "Static Bundling and Channel On Demand" in this Guide.

Default:	Disabled	
BRI:	Options:	Disabled, Enabled
PRI:	Options:	Disabled, 1 B Channel, 2 B Channels, 3 B Channels, ..., 15 B Channels

If Static Bundling is disabled, only one data channel is used to establish an ISDN connection. The other data channel(s) available on the ISDN-Controller may be used separately by other ISDN Call Destinations for the other interfaces.

If Static Bundling is enabled on an AVM ISDN-Controller for BRI, the second data channel is automatically used to establish the ISDN connection to the remote site, providing double bandwidth.

To use Static Bundling on an AVM ISDN-Controller for PRI, specify the number of additional data channels to be used to establish an ISDN connection to this remote site.

36. Check *Multi-Controller Bundling*.

Multi-Controller Bundling can be used to bundle data channels over different ISDN-Controllers.

Default:	Disabled
Options:	Disabled, Primary Call Destination, Static Secondary Call Destination, On Demand Secondary Call Destination

If you want to use Multi-Controller Bundling, you have to configure more than one call destination for the same remote site. The call destinations are identified by their identical Remote System ID. When a connection is established to a remote site, the router looks for Call Destinations with identical Remote System IDs and Multi-Controller Bundling set to "Static Secondary Call Destination" or "On Demand Secondary Call Destination". The connection to the Primary Call Destination is established, and if the remote site also supports multi-controller bundling,

- all additional channels are switched through for Static Secondary Call Destinations
- On-Demand Secondary Call Destinations are reserved for channel allocation in case the Channel Allocate Threshold is reached.

For detailed configuration information and for sample scenarios in which Multi-Controller Bundling makes sense, refer to the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*.

37. If you are using PPP over ISDN, check *PPP Multilink*.

The PPP Multilink protocol (PPP MP) was developed by the Internet Engineering Task Force (IETF) as an extension to PPP. PPP MP extends PPP so that it can split and combine packets over multiple parallel links in order to create a higher aggregate data rate. It can be used to combine several ISDN B channels to increase the effective wire speed of 64 Kbps.

Default: Disabled

Options: Disabled, Enabled

Disabled means that only one data channel is used to establish an ISDN connection. The other data channel(s) available on the ISDN-Controller may be used separately by another ISDN Call Destination for the other interface.

Enabled means that your router will try to negotiate PPP Multilink with the remote site during LCP negotiation. If the remote site supports PPP MP too, additional channels can be allocated through Channel On Demand or Static Bundling.

38. Decide whether you want to use a *Specific Dial-Back Number*.

If configured, the Dial-Back Number will be used by a remote NetWare MultiProtocol Router for ISDN to call your router back after an Inacitvity Timeout or if the parameter "Security Call-Back" is set to "Force Call-Back to Caller-Specified Number" (see "Expert Configuration of ISDN Interface <*Interface Name*>").

The number for underlying physical call set-ups / dial-backs is normally taken from the ISDN number field of a call destination. In some cases, it is preferable to configure a Specific Dial-Back Number: For example, if the Area Code differs for national and international calls, or where the number in the ISDN Number field is not the optimum number to dial, which might be the case in frontier areas.

When a Dial-Back Number is configured, this number is transmitted to the remote site during initial call set-up, and is then always used by the remote site for dialing back, i.e. for all subsequent underlying physical call set-ups.

For PPP over ISDN connections, the Dial-Back Number can be used during LCP negotiation to request a call-back (RFC 1570, callback option).

38a. Specify the *Dial-Back Number*.

Enter the Dial-Back Number to be used to call your router back.

39. If you have installed the separate AVM encryption module, check the *Encryption*.

AVM´s implementation is software-based and performed on the ISDN-Controller(s). It is a hybrid system and uses the recognized procedures IDEA and RSA.

Encryption is not included as standard with the NetWare Multi-Protocol Router for ISDN 3.1, but offered as a separate module. For more information, please contact AVM.

Default: Disabled

Options: Enabled, Disabled

For more information on Encryption, refer to the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*.

40. Check *Static Remote Node*.

Here, you can define whether the NetWare MultiProtocol Router for ISDN is allowed to initiate calls to a specific remote node in order to transfer data such as e-mails.

Default: Disabled

Options: Disabled, Enabled

Disabled means that data for the specific remote node is only transferred when the connection has been initiated by the remote node.

Enabled means that the router itself will initiate a connection to this remote node when data such as e-mails have to be transferred, irrespective of whether the remote node established an initial connection. Currently, this is only possible with special IPX applications or any IP-based application such as FTP demon. In this case, you must always configure the Node Address of the remote node for IPX or the IP address for TCP/IP (see below).

For PPP over ISDN, enabling this parameter defines that calls from this remote site are always accepted as Remote Node-LAN. In this case, the transmitted caller-specified number or the delivered system ID must match the configured ISDN Number or Remote System ID. It is not necessary to configure the Node Address or the IP Address. If Static Remote Node is disabled, calls are accepted as LAN-LAN.

40a. If you want to use IPX, enter the *Node Address* of the remote node.

40b. If you want to use TCP/IP, enter the *IP Address* of the remote node.

41. Specify the *Inbound Authentication*.

Inbound Authentication lets you specify the inbound authentication protocol to use for incoming and outgoing connections.

Default: None

Options: None, PAP, CHAP

None means that no inbound authentication is performed for incoming and outoing connections.

PAP means that inbound authentication is performed with PAP for incoming and outgoing calls to this destination. The call is identified by Local System ID, Remote System ID and Password. The Password is not coded for transmission.

CHAP means that inbound authentication is performed with PAP for incoming and outgoing calls to this destination. The call is identified by Local System ID, Remote System ID and Password. CHAP is more secure than PAP, since the Password is coded for transmission.

Warning

If you want to use Inbound Authentication, do not forget to enter a Password (see below).

42. Specify a *Password*.

The Password is used for Inbound Authentication and for Encryption.

Specify the Password for the current Call Destination.

43. Enter the *Local System ID*.

This field allows you to specify the name sent to the remote peer during authentication of an outbound call to identify this system when using this ISDN Call Destination.

The Local System ID can contain up to 47 alphanumeric characters.

44. Specify a *Remote System ID*.

The Remote System ID specifies the name of the remote peer associated with this ISDN Call Destination.

You must configure a Remote System ID

- for on-demand TCP / IP connections,
- to identify incoming calls from this remote site by its system ID,
- for inbound authentication,
- if you want to use Multi-Controller Bundling (see the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*).

To change the Remote System ID, press <Enter> on this field. Select from the pop-up list displayed, or press <Ins> to create a remote system ID.

45. Check the *Retry Mode*.

Retry Mode specifies the conditions under which a failed connection is retried automatically.

Default:	Never Retry
Options:	Never Retry, Retry Self-Correcting Failures, Retry All Failures

It is recommended not to change the default "Never Retry" when you are using standard circuit-switched lines. Otherwise, high connection charges may occur when the router permanently tries to set up a connection to a remote site is not active.

For connections with the Call Type set to *Permanent* (D64S, DS01 and DS02 connections, see Step 6 above), set the Retry Mode to *Retry All Failures*.

Note

Note that even if the Retry Mode is activated, a configured backup destination is switched through.

46. Check the *Retry Limit Handling*.

Retry Limit Handling specifies the action taken when the connection retry interval exceeds the configured limit. Permanent call retries can continue indefinitely at the configured interval limit, or retry attempts can be terminated and the connection failed.

Default: Stop At Limit

Options: Continuous At Limit, Stop At Limit

For connections with the Call Type set to *Permanent* (D64S, DS01 and DS02 connections, see Step 6 above), set this parameter to *Continuous At Limit*.

47. **Check the *Retry Interval Limit*.**

    Retry Interval Limit specifies the maximum delay interval (in HH:MM:SS) between attempts to establish a connection. The delay is set to about 8 seconds and increases exponentially.

48. **Press** <Esc> **to return to the *Internetworking Configuration* menu and save your changes when prompted.**

Changing ISDN Call Destination Parameters

To change any parameter associated with an ISDN Call Destination, complete the following steps:

1. **At the server prompt, type**

   ```
   LOAD INETCFG <Enter>
   ```

   The *Internetworking Configuration* menu is displayed.

2. **From the *Internetworking Configuration* menu, select *WAN Call Directory*, then press** <Enter>**.**

   A new window displays a list of the configured WAN Call Destinations.

3. **Highlight the desired *ISDN Call Destination* in the list, then press** <Enter>**.**

   A new window displays the ISDN Call Destination parameters for the selected interface.

4. **Make new selections for the parameters that need to change, then press** <Esc>**.**

   A new window prompts you to save the changes.

Important

If you change the Call Type or Network Interface of a WAN Call Destination that is used in a bind, the bind is no longer valid. If this occurs, edit the bind or delete it.

5. **Select *Yes* to save the changes, then press** <Enter>**.**

   The list of configured WAN Call Destinations is redisplayed.

6. **Press** <Esc> **to return to the *Internetworking Configuration* menu.**

Deleting an ISDN Call Destination

To delete an ISDN Call Destination, complete the following steps:

1. **At the server prompt, type**

   ```
   LOAD INETCFG <Enter>
   ```

   The *Internetworking Configuration* menu is displayed.

2. **From the *Internetworking Configuration* menu, select *WAN Call Directory*, then press** <Enter>**.**

   A new window displays a list of the configured WAN Call Destinations.

3. **Highlight an *ISDN Call Destination* in the list, then press** <Delete>**.**

   A message is displayed indicating that deleting this ISDN Call Destination also deletes all binds that refer to this ISDN Call Destination.

4. **Select *Yes* to delete the ISDN Call Destination and all binds that refer to it, then press** <Enter>**.**

5. **Press** <Esc> **to return to the *Internetworking Configuration* menu.**

chapter 8

Configuring Global Parameters

Global MPR for ISDN Configuration

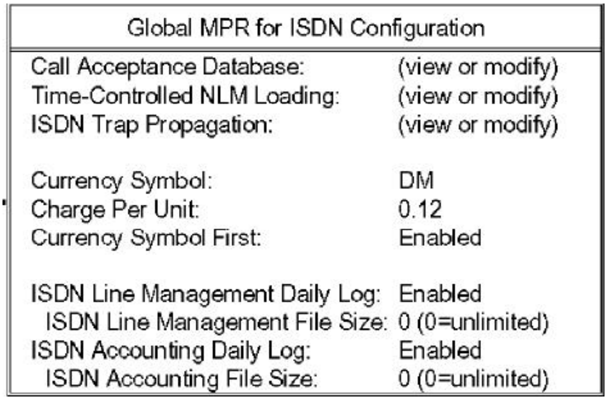
From the *Global MPR for ISDN Configuration* menu, you can

- view the Call Acceptance Database and insert new registered numbers,
- configure time-controlled loading of NLMs,
- configure propagation of SNMP Traps,
- define the currency symbol used in your country and the cost of one charge unit, and
- configure logging of ISDN line management messages and accounting information and define the log file size.

Parameter path: load INETCFG > *Network Interfaces* > *Global MPR for ISDN Configuration*.

The following menu appears:

Figure 8-1:
Global MPR for ISDN Configuration menu



```
              Global MPR for ISDN Configuration
Call Acceptance Database:           (view or modify)
Time-Controlled NLM Loading:        (view or modify)
ISDN Trap Propagation:              (view or modify)

Currency Symbol:                    DM
Charge Per Unit:                    0.12
Currency Symbol First:              Enabled

ISDN Line Management Daily Log:     Enabled
  ISDN Line Management File Size:   0 (0=unlimited)
ISDN Accounting Daily Log:          Enabled
  ISDN Accounting File Size:        0 (0=unlimited)
```

Completing the Call Acceptance Database

The Call Acceptance Database (SYS:ETC\ISDNCADB.CFG) contains all remote sites and their numbers you want to allow access to your router.

To perform this special ISDN security check, you have to set the parameter "Call Acceptance" in the "Expert Configuration of ISDN Interface <*Name*>" menu to "Only Registered Numbers" with the desired option (see Chapter 6, "Configuring ISDN Interfaces").

To find out the CLI number and the caller specified number, have the respective remote sites set up a connection to your router. The CLI number, transmitted over the D channel, and the caller specified number will be printed on the NetWare system console.

Perform the following steps to register authorized remote sites and their numbers in the Call Acceptance Database:

Procedure

1. **From the *Global MPR for ISDN Configuration* menu, select *Call Acceptance Database* and press** <Enter>**.**

   The *Call Acceptance Database* window appears. Initially, the database is empty.

2. **To add entries, press** <Ins> **to display an empty *Registered Number* mask.**

3. **In the *Registered Number* field, enter the number of the remote site you want to allow access.**

4. **Select the *Registered Number Type*.**

   Options are "Caller-Specified Number" and "CLI Number". Select the type of number you entered before.

5. **(Optional) Enter any comment (name or remark) that helps you to identify the entry and to relate the number to the corresponding remote site.**

6. **Quit the mask with** <Esc>**. You are asked if you want to make a second entry for the remote site.**

   When you set "Only Registered Numbers: CLI and Caller Specified" for Call Acceptance, you have to make two entries for this destination: one containing the CLI number and one containing the number transmitted over the ISDN B channel. In this case, select *Yes* and enter the second number.

If not, select *No*. The new remote site appears in the Call Acceptance Database menu. The entries are sorted automatically in descending order.

7. **Repeat Steps 2 through 6 for each site you want to allow access.**

8. **When you are finished, press** <Esc>**, select *Yes* and press** <Enter> **to return to the *Global MPR for ISDN Configuration*.**

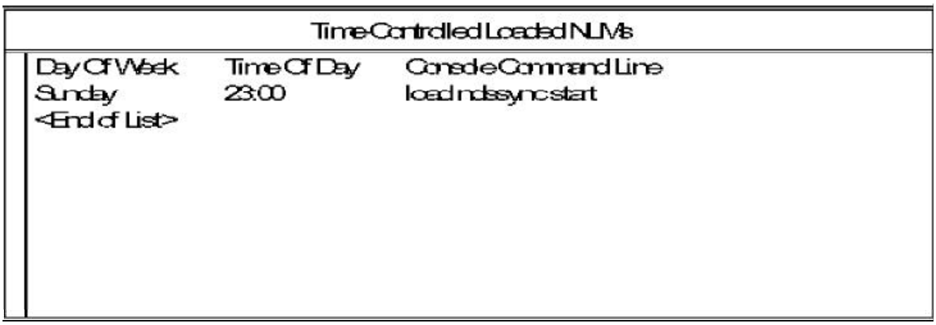
Automatically Loading NLMs at Specified Times

The option *Time-Controlled NLM Loading* of the *MPR for ISDN Global Configuration* menu allows you to automatically load NLMs at specified times.

For example, you can load CICCON.NLM and CICCOFF.NLM at specified times to automatically transfer data to a remote site, activate and deactivate ARCServer or start an NDS synchronization at predefined times.

Press <Enter> on *Time-Controlled NLM Loading* to display the following menu:

Figure 8-2:
Time-Controlled Loading of NLMs Configuration



```
                    Time-Controlled Loaded NLMs
Day Of Week    Time Of Day    Console Command Line
Sunday         23:00          load ndssync start
<End of List>
```

To enter an NLM in the list, press <Ins> to display an empty mask.

Enter the *Day of Week*, the *Time of Day* and the *Minute of Hour* you want to have the NLM loaded and specify the *Command Line* for the NLM.

When you are finished, press <Esc> and save your changes. The new entry is now included in the list.

To return to the *MPR for ISDN Global Configuration*, press <Esc>.

ISDN Trap Propagation

SNMP enables network management clients to exchange information about the configuration and status of nodes on an internetwork. The information available is defined by a set of managed objects referred to as the Management Information Base (MIB).

To enable SNMP management on the NetWare MultiProtocol Router for ISDN, you have to enable Trap propagation and configure SNMP information. ISDN Trap Propagation is configured in the Global MPR for ISDN Configuration. To configure SNMP information, refer to section "Configuring SNMP Information" later in this Chapter.

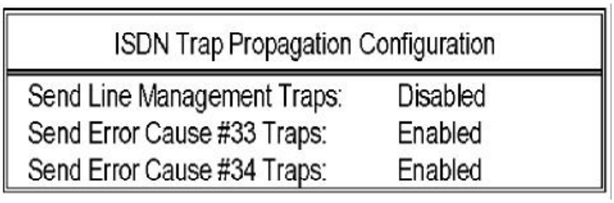
The *ISDN Trap Propagation* command in the *Global MPR for ISDN Configuration* lets you define whether ISDN Line Management Traps and Traps reporting ISDN error causes 0x33 and 0x34 are sent to any SNMP-based management console.

Note

If you enable one of the parameters described below and the management console is connected over ISDN, you have to disable the SNMP over IPX Filter or SNMP over IP Filter, depending on which network protocol you want to use for sending Traps. Otherwise, the Traps will be dropped at the ISDN driver level.

Press <Enter> on *ISDN Trap Propagation* in the *Global MPR for ISDN Configuration* to display the following menu:

Figure 8-3:
ISDN Trap Propagation Configuration



ISDN Trap Propagation Configuration

Send Line Management Traps:	Disabled
Send Error Cause #33 Traps:	Enabled
Send Error Cause #34 Traps:	Enabled

Procedure

1. **Check *Send Line Management Traps*.**

   This parameter defines whether ISDN Line Management Traps are sent to any SNMP-based management console or not.

   Default: Disabled

   Options: Disabled, Enabled

2. **Check *Send Error Cause #33 Traps*.**

   Here you specify whether you want Traps reporting ISDN error causes 0x33 to be sent to any management console.

   Default: Enabled

   Options: Enabled, Disabled

3. **Check *Send Error Cause #34 Traps*.**

   Define whether you want Traps reporting ISDN error messages 0x34 to be sent to any management console.

   Default: Enabled

   Options: Enabled, Disabled

Adjusting the Currency Display

The NetWare MultiProtocol Router for ISDN 3.1 provides a number of statistics in its ISDN Console, among them information on connection charges. Besides, it allows you to configure budget values for each call destination. In order that these values are displayed correctly, you have to adjust the currency display in the *Global MPR for ISDN Configuration*.

Procedure

1. **Check the *Currency Symbol*.**

   Default: DM

   Enter the symbol for the currency used in your country.

2. **Enter a value for *Charge Per Unit*.**

   Default: 0.12

   Enter the price of one charge unit in your country.

3. Decide whether you want to display the *Currency Symbol First*.

Default: Enabled

Options: Enabled, Disabled

Enabled means that any connection charges are displayed in the form *DM <Amount>*.

If this parameter is disabled, charges are displayed as *<Amount> DM*.

Writing Daily Log Files

Procedure

1. *ISDN Line Management Daily Log*.

The ISDN Line Management Daily Log keeps a record of all actions that are performed on the router on a single day. The file name is of the form isdn??.log, the question marks being replaced with the day of the month, e.g. isdn01.log for the first day of the month, isdn02.log for the second, etc. With the beginning of a new month, the files are subsequently written over. The log files are by default stored in the SYS:ETC directory. All ISDN line management messages are listed and described in Appendix A.

1a. Check the maximum file size for the ISDN Line Management Daily Log.

Specify the size of a single ISDN Line Management Daily Log. Logging is stopped when the maximum size of a single file is reached. A value of 0 means that the size is unlimited.

Note

You should not set the file size to unlimited. If you are using an AVM ISDN-Controller for PRI, the file can become very big in a short time.

2. *ISDN Accounting Daily Log*.

The ISDN Accounting Log stores ISDN connection oriented information provided via ISDN Console. The file name is of the form isdn??.acc, the question marks being replaced with the day of the month, e.g. isdn01.acc for the first day of the month, isdn02.acc for the second, etc. It allows you to monitor all important details on all ISDN connection on a router from the first logical set up to the final logical clear down. Each time an ISDN connection is cleared logically (Disconnect Timeout expires or by pressing Delete in the Call Connection Manager for example), the ISDN connection information is written to the ASCII-format log files in a single line.

2a. Check the maximum file size for the ISDN Accounting Daily Log.

Specify the size of a single ISDN Accounting Log File. Logging is stopped when the maximum size of a single file is reached. A value of 0 means that the size is unlimited.

Note

You should not set the file size to unlimited. If you are using an AVM ISDN-Controller for PRI, the file can become very big in a short time.

Configuring SNMP Information

Configuring SNMP Parameters

SNMP enables network management clients to exchange information about the configuration and status of nodes on an internetwork. The information available is defined by a set of managed objects referred to as the Management Information Base (MIB).

To configure SNMP parameters for a specific node, complete the following steps:

Procedure

1. At the server prompt, type

```
LOAD INETCFG <Enter>
```

The *Internetworking Configuration* menu is displayed.

2. From the *Internetworking Configuration* menu, select *Manage Configuration*, then press <Enter>**.**

The *Manage Configuration* menu is displayed.

3. From the *Manage Configuration* menu, select *Configure SNMP Parameters*, then press <Enter>**.**

The *SNMP Parameters* window is displayed.

4. **From the *SNMP Parameters* window, select *Monitor State*, then press** <Enter>**.**

   The following options allow you to indicate how the SNMP agent handles SNMP read operations coming from outside this node.

Table 15-1: Monitor State Parameters

Option	Description
Any Community May Read	Allows all read operations no matter what community name is provided in the incoming read request.
Leave as Default Setting	Avoids changing the Monitor Community name from its default (which is usually public). The default Monitor Community can still be changed manu lly through SNMP command-line options.
No Community May Read	Disables all read operations no matter what community name is provided in the incoming read request.
Specified Community May Read	Allows only read operations that contain the name specified in the Monitor Community field.

5. **Select one of the options described above, then press** <Enter>**.**

6. **If you selected *Specified Community May Read*, enter a name in the *Monitor Community* field, then press** <Enter>**.**

   Enter the name of the community that is allowed to read management information. SNMP management stations that belong to this community can read the network management database.

7. **Select *Control State*, then press** <Enter>**.**

   The following options allow you to indicate how the SNMP agent handles SNMP write operations coming from outside this node.

Table 15-2: Control State Options

Option	Description
Any Community May Write	Allows all set operations no matter what community name is provided in the incoming read request.

Leave as Default Setting	Avoids changing the Control Community from its default, which is usually not to allow any write requests. The default can be changed manually through SNMP command-line options.
No Community May Write	Disables all set operations no matter what community name is provided in the incoming read request.
Specified Community May Write	Allows only set operations that contain the name specified in the Control Community field.

8. **Select one of the options described above, then press** <Enter>**.**

9. **If you selected *Specified Community May Write*, enter a name in the *Control Community* field, then press** <Enter>**.**

   Enter the name of the community that is allowed to read and write management information. SNMP management stations that belong to this community can read or modify any value in the network management database.

10. **Select *Trap State*, then press** <Enter>**.**

    The following options allow you to indicate how the SNMP agent handles SNMP trap operations coming from outside this node.

Table 15-3: Trap State Options

Option	Description
Do Not Send Traps	Disables all SNMP traps no matter what community name is provided in the incoming trap request.
Leave as Default Setting	Avoids changing the Trap Community from its default (which is usually public). The default can still be changed manually through SNMP command-line options.
Send Traps With Specified Community	Enter the community name to include in trap messages in the Trap Community field.

Important

Configuration of the list of SNMP Managers is described in the next section, "Configuring SNMP Manager Tables."

11. **Select one of the options described above, then press** <Enter>**.**

12. **If you selected *Send Traps With Specified Community* , enter a name in the *Trap Community* field, then press** <Enter>**.**

    Enter the community name to be included in trap messages.

13. **Select *Other SNMP Parameters*, then press** <Enter>**.**

    Enter other SNMP command-line parameters in the window that is displayed, then press <Enter>.

    The parameters should be entered in the same format they would appear when entered on the LOAD SNMP command line.

14. **When you are finished, press** <Esc>**; if prompted, select *Yes* to save the changes to the SNMP parameters, then press** <Enter>**.**

    The *Manage Configuration* menu is displayed.

15. **Select *Configure SNMP Information*, then press** <Enter>**.**

    The *General SNMP Information For This Node* window is displayed.

16. **Select *Node Name for SNMP*, then press** <Enter>**.**

    Enter the name SNMP reports to the management client for this node, then press <Esc>.

    By convention, this is the IP hostname for the node. If the node does not have an IP hostname, it is recommended that you use the NetWare® file server name for this node.

17. **Select *Hardware Description*, then press** <Enter>**.**

    Enter the hardware description for this node, then press <Esc>.

    The hardware description can include the CPU type, bus speed, size of memory, size and type of disks, printers, tape drives, and so on. This description, combined with the information about the software taken from the system, makes up the SNMP system description.

18. **Select *Physical Location*, then press** <Enter>**.**

    Enter the location description for this node, then press <Esc>.

19. **Select *Human Contact*, then press** <Enter>**.**

    Enter the contact information for the persons responsible for this node, then press <Esc>. The contact information should include phone numbers and mailing addresses.

20. **When you are finished, press** <Esc>**; if prompted, select *Yes* to save the changes to the SNMP information, then press** <Enter>**.**

    The *Manage Configuration* menu is displayed.

21. **Press** <Esc> **to return to the *Internetworking Configuration* menu.**

Configuring SNMP Manager Tables

The list of SNMP Managers can be configured as follows:

For the IPX protocol, SNMP Managers cannot be configured from any NetWare MultiProtocol Router for ISDN 3.1 menu. Therefore, use EDIT.NLM to edit the traptarg.cfg directly:

```
load edit sys:etc\traptarg.cfg
```

Add or delete SNMP Managers from the file and save your changes.

For TCP/IP, SNMP Managers can be configured directly from the Internetworking Configuration menu:

Parameter path: Load INETCFG > Select *Protocols* > Select *TCP/IP* > Select *SNMP Manager Table*.

chapter 9 Configuring IPX

On-Demand IPX Calls with Static Routes and Services

An on-demand call is a point-to-point connection between two IPX routers that becomes active only when one router must send user data to the router at the other end.

No routing or service information crosses an on-demand call. Instead, remote routes and services are configured on the local router as static routes and services. In this way, the connection can remain inactive until user data needs to cross it. Workstations needing to reach remote destinations send packets to their local IPX router advertising the routes, assuming the packets can reach their destination. The local router stores the packets and tries to establish a connection to the remote router. After the local router completes the call and negotiates on-demand service, it forwards the stored packets to the remote router, which then forwards them to their destination.

Because each router is configured with the routes and services that are available at the opposite end of the connection, there is no need to send routing or services updates or periodic routing / service information across the connection. Each router simply advertises the routes and services locally as if they had just arrived over the connection. NetWare workstations and servers on the local LAN remain unaware that no active permanent connection exists. The locally configured static routes contain all information necessary for a local system to access any remote service.

Note

To avoid activating potentially expensive connections, type 20 (NetBIOS) packets are not forwarded over on-demand calls as NetWare serialization packets.

For design considerations for ISDN-WANs, refer to Chapter 4, "Basic Design of ISDN-WANs and Configuration Overview" in this Guide.

What You Need

Before configuring an on-demand IPX call, you need to have at least the following:

- the name and the IPX internal network number of the remote router,
- ISDN Number and Subaddress of the remote router
- SNMP write access to the remote router

Procedure

You configure on-demand calls and set up static routes and services with the following utilities:

- INETCFG - The Internetworking Configuration utility. Use INETCFG to set up WAN Call Destinations at each end of the connection (see instructions below).
- STATICON - The static route and service configuration utility. STATICON uses the Simple Network Management Protocol (SNMP) to discover which routes and services are available through a remote router and add them to the static routing table on a local router.

Before you use STATICON, you must do the following tasks from INETCFG:

Procedure

1. Configure an ISDN Call Destination entry.

Parameter path: Select *WAN Call Directory* > Press <Ins> > Specify a name for the call destination > Select a *Wide Area Medium*.

Detailed information on configuring ISDN Call Destinations is given in Chapter 7.

1a. Set the parameter *Call Type* to *On Demand.*

1b. Press <Enter> **on *Spoofings/Filters* and make sure that the *SNMP Over IPX Filter* is disabled.**

1c. Specify a *Local System ID*.

1d. Specify the *Remote System ID*.

With the help of the Remote System ID, the IPX protocol stack relates an incoming call to a specific call destination.

2. Configure IPX.

Parameter path: Select *Protocols* > Select *IPX*.

2a. Set *Packet Forwarding* to *Enabled*.

3. Bind IPX to an ISDN interface.

Parameter path: Select *Bindings* > Press <Ins> > Select *IPX* > Select a configured ISDN interface or interface group.

3a. Press <Enter> **on *WAN Call Destinations*, then press** <Ins>**.**

3b. Select a configured on-demand call destination from the list.

3c. Set the *Call Type* to *Static On Demand*.

3d. Select *Static Services*.

A new screen displays any configured static services.

3e. Press <Ins>**, then enter the following information:**

Service Name - Name of the service to be accessed through the on-demand call. This name, which is typically the server name, is added to the local service and routing tables.

Service Address Network - Enter the internal network number of the remote router.

3f. Press <Esc> **to return to the *Internetworking Configuration* menu; save your changes when prompted.**

4. Configure SNMP write access to the remote router.

For STATICON to configure a remote router's routing and service tables, it must support IPX SNMP and the IPX MIB variables and have write access to the router.

Protocol path: Load INETCFG on the remote router > Select *Manage Configuration* > Select *Configure SNMP Parameters*.

4a. The *Control State* field should read *Any Community May Write* or *Specified Community May Write*.

If it reads *Specified Community May Write*, note the name in the *Control Community* field.

5. **Activate the configuration on the local and the remote site with the *Reinitialize System* command.**

6. **You then load STATICON and configure all static routes and services on the routers at each end of the connection.**

   For information on configuring static routes and services with STATICON, refer to the *NetWare MultiProtocol Router 3.1 Configuration guide*, pp. 118 to 128.

   STATICON configures all routes and services automatically on each router and allows you to try the configuration before saving it to disk. The STATICON configuration becomes active immediately; you do not need to reinitialize or restart the router.

Manual IPX Connections via CALLMGR

The Call Connection Manager (CALLMGR.NLM) enables you to initiate and terminate IPX connections over ISDN manually and to monitor the status of an IPX connection.

Load CALLMGR by typing the following command at the server prompt:

```
load callmgr <Enter>
```

What You Need

Before configuring call destinations to use with CALLMGR, decide whether you want to use NLSP or RIP / SAP as a routing protocol. AVM recommends that you use RIP / SAP for connections over ISDN.

Note

For RIP/SAP connections over ISDN, the Periodic Update Interval for IPX RIP and SAP is automatically set to 10000 when you reinitialize your system!

Procedure

You configure manual IPX connections as follows:

Procedure

1. Configure an ISDN Call Destination entry.

Parameter path: Select *WAN Call Directory* > Press <Ins> > Specify a name for the call destination > Select a *Wide Area Medium*.

Detailed information on configuring ISDN Call Destinations is given in Chapter 7.

1a. Set the *Call Type* to *On Demand.*

2. Configure IPX.

Parameter path: Select *Protocols* > Select *IPX*.

2a. Set *Packet Forwarding* to *Enabled*.

3. Bind IPX to an ISDN interface.

Parameter path: Select *Bindings* > Press <Ins> > Select *IPX* > Select a configured ISDN interface or interface group > Select *Expert Bind Options*.

3a. If you chose *NLSP with RIP/SAP Compatibility* as *Routing Protocol*, select *NLSP Bind Options* and set the *NLSP State* to *Off*.

4. Activate the configuration by using the *Reinitialize System* command.

5. Load the Call Connection Manager utility and control your IPX connections manually.

Manual IPX Connections via Client Initiated Call Control (CICC)

CICC is available for the following platforms:

♦ CICC for NetWare in the form of two NetWare Loadable Modules™ (NLMs™) is installed per default in the SYS:SYSTEM directory.

- CICC for DOS, Windows and OS/2 are contained in the directory CICC on the software CD-ROM.

The CICC software allows control of IPX connections over ISDN directly from an IPX client. It may be used as an alternative to Call Manager under certain circumstances to manage the logical set-up and clear-down of IPX connections. CICC can be integrated into existing communication processes or applications by means of batch routines. CICC may be used mainly in situations where a large number of remote LANs have to be connected to the existing WAN and where the connection does not have to be permanent, but is only required for specific communication situations. Thus, CICC may be integrated for example into an existing electronic mail application by means of batch routines, so that electronic mail is automatically sent over a single data channel to all remote sites that are not permanently connected to the central WAN.

CICC may also be used "on demand" on any IPX client by the respective user to set up or clear down IPX connections or question the status of an IPX connection.

Please note that this is not the main purpose of CICC and the CICC software should not be offered to all users; it adds unnecessary complexity for users and a network manager should carefully consider whom to allow the use of CICC.

CICC for NetWare

CICC for NetWare is realized in the form of two NetWare Loadable Modules™ (NLMs™), **CICCON.NLM** and **CICCOFF.NLM**. They are automatically copied to the SYS:SYSTEM directory during installation of the NetWare MultiProtocol Router for ISDN 3.1.

To establish a connection to a remote site with CICCON.NLM, enter the following command at the system console:

```
load CICCON -dDestination_Name
```

where *Destination_Name* is the Call Destination Name of the remote site.

To set up a connection from a remote NetWare Protocol Router for ISDN to a remote site, enter the following command at the system console:

```
load CICCON -sServer_Name -dDestination_Name
```

where *Server_Name* is the name of the NetWare MultiProtocol Router for ISDN, and *Destination_Name* the Call Destination Name of the remote site.

To clear an ISDN connection manually, enter

```
load CICCOFF -dDestination_Name
```

at the system console.

To clear an ISDN connection from a remote NetWare Protocol Router for ISDN to a remote site manually, enter

```
load CICCOFF -sServer_Name -dDestination_Name
```

at the system console.

To automatically load CICCON and CICCOFF at specified times, use the *Time-Controlled NLM Loading* command in the *Global MPR for ISDN Configuration* menu. For more information, refer to Chapter 8, "Configuring Global Parameters."

CICC for DOS

CICC for DOS consists of three components in the form of .EXE files.:

CICCON.EXE and **CICCOFF.EXE -** serve to set up and clear down IPX connections. Thus they offer the same functions as "Insert" and "Delete" provided within Call Connection Manager to set up or clear down an IPX connection logically. There are two differences when using CICCON / CICCOFF instead of Call Connection Manager. First, batch routines for logical set up and clear down of IPX connections can be written to automatically set up a logical IPX connection to a remote site, perform a task (send electronic mail or update files), clear down this connection and set up the next IPX connection to another remote site to perform the same task at this site, etc. Second, RCONSOLE does not have to be loaded to get access to the Call Connection Manager in order to establish or delete a logical IPX connection.

CICCSTAT.EXE - allows display of the status of logical IPX connections, thus reflecting the status information also provided by the Call Connection Manager.

These components are started with additional arguments and allow connection set-up and clear-down of all the "ISDN Call Destination Configurations" that have been configured for IPX on the local router.

Call Set-Up - CICCON

To establish an IPX connection over ISDN, enter the following command:

```
CICCON -d<RemoteServer> [-s<LocalServer>] [-v]
```

Example: CICCON -dAVMBERLIN -sFS4 establishes an ISDN connection to the ISDN Call Destination with the name "AVMBERLIN" over the local server / router with the name "FS4".

Table 9-1:
Parameters for CICCON, CICCOFF and CICCSTAT

Parameter	Description
RemoteServer	"Call Destination Name" of the remote server/router that the ISDN connection is to be established to. The name should have been assigned in the ISDN Call Destination Configuration (see Chapter 2). This connection should not be logically active.
LocalServer	Name of the local server/router that will establish the connection. The argument needs to be added only if the server/ router is not the default server of the IPX client using CICC.
-v	For the use of CICC within batch routines: suppresses output of information printed on the client screen each time when starting CICCON or CICCOFF.

Call Clear-Down - CICCOFF

To clear down an existing connection, enter the following command:

```
CICCOFF -d<RemoteServer> [-s<LocalServer>] [-v]
```

Example: `CICCOFF -dAVMBERLIN -sFS4` clears an ISDN connection to the ISDN Call Destination with the name "AVMBERLIN" over the local server / router with the name "FS4".

Display Status Information - CICCSTAT

To display status information, enter the following command:

```
CICCSTAT [-s<LocalServer]
```

A list of all IPX connections currently logically active over ISDN is returned.

Example: `CICCSTAT -sFS4` lists all IPX connections that are currently established logically from or to the local server / router with the name "FS4".

Returncodes via Errorlevel for Batch Routines

The CICC module has been developed mainly for the use in batch routines. Information on the status of an action may be obtained by the corresponding errorlevel. A returncode other than "0" (zero) means that an error must have occurred.

Table 9-2: CICC Returncodes

Returncode	Description
0	Action successful ./.
1	Error during set up / incorrect parameter. Local system error.
2	IPX not found. Local system error
3	SPX not found. Local system error
4	No communication socket available. Local system error
5	No server found. Local system error.
6	Server/router does not respond / not found. Local system error
7	Local server not found (Read PropertyValue) Local system error.
10	No memory (client). System error.
20	Destination not known / found. Communication error.
21	Connection set-up to server/router not successful. Communication error.
22	Connection set-up to the remote server/router not successful. Communication error
23	No response from server/router (Invalid Target, Timeout). Communication error

CICC for Windows

The files **CICCDLL.DLL** and **CICCWIN.EXE** are needed to operate CICC under Windows. Thus, copy them into your local MS Windows directory. The files **SAMPLE.C**, **CICCDLL.LIB** and **CICCDLL.H** provide support for programming applications for CICC under Windows.

The program **CICCWIN.EXE** can be started with several command line options. This is useful for integrating it into batch routines. The following options can be used:

Table 9-3:
Command line options for CICCWIN.EXE

Option	Description
/S<server>	specifies the source server
/T<target>	specifies the target
/C	connects to the specified target
/D	disconnects from the target
/M	displays a diagnostic message (only in conjunction with /C or /D)

Example: CICCWIN.EXE /SFINANCE /TMUNICH /C

establishes a WAN connection from the FINANCE server/router to the MUNICH router.

If you do not specify any parameter, the interactive mode is started.

When CICCWIN.EXE is used in batch mode, the icon appears on the desktop to indicate that CICCWIN is active. The program terminates with an exit code which indicates the status of the operation. The values of the exit code are exactly the same as the returncodes of the functions of the CICCDLL.DLL. See the file CICCDLL.H for a description.

CICC for OS/2

The files **CICCDLL.DLL** and **CICCOS2.EXE** are needed to operate CICC under OS/2. Thus, create a new directory on your PC, e.g. C:\CICCOS2 and copy these files into this directory. The files

CICCDLL.LIB and **CICCDLL.H** provide support for programming applications for CICC under OS/2.

CICCOS2.EXE can be operated in batch mode and interactive mode.

To start CICC in *interactive mode*, enter CICCOS2 without any parameters.

In a dialog, you are prompted to enter the source server/router and the target. A list box shows the current call status of the source server.

The following functions are provided:

- The STATUS button updates the call status shown in the list box.
- The CONNECT button tries to connect to the specified target.
- The DISCONNECT button disconnects from the specified target.
- The ABORT button aborts the current function.

The application writes the last server name used and all used target names in a file named CICCOS2.INI.

To select one of the previously used target names, just pop up the combo box. The targets used and the server name are shown.

You cannot delete any entry of the .INI file, but you can delete the CICCOS2.INI file without loosing important configuration information.

The exit code of the program has no meaning in interactive mode.

In *batch mode*, CICCOS2.EXE performs one CICC operation and then terminates.

The following command line options can be used:

Table 9-4:
Command line options for CICCOS2.EXE

Option	Description
/S<server>	specifies the source server
/T<target>	specifies the target
/C	connects to the specified target
/D	disconnects from the target
/M	displays a diagnostic message (only in conjunction with /C or /D)

/F<filename>	Writes the strings “OK” or “ERROR” to a file, depending on the success of the operation. This is useful for quick and easy error detection in batch environments.

Table 9-5:
Exit codes (ERRORLEVEL) for CICCOS2.EXE

Code	Description
-1	Fatal error during program initialization
0	No error
1	IPX/SPX fatal error
2	Server/router not found
3	No free local SPX socket
4	Call Manager on the router not found
5	Aborted by user (should never occur)
6	Call Manager operation timed out (failed)
7	Requested target not found
8	The CICCDLL is busy (should never occur)

What You Need

Before configuring call destinations to use with CICC, decide whether you want to use NLSP or RIP / SAP as a routing protocol. AVM recommends that you use RIP / SAP for connections over ISDN.

Note

For RIP/SAP connections over ISDN, the Periodic Update Interval for IPX RIP and SAP is automatically set to 10000 when you reinitialize your system!

Procedure

You configure manual IPX connections as follows:

Procedure

1. **Configure an ISDN Call Destination entry.**

   Parameter path: Select *WAN Call Directory* > Press <Ins> > Specify a name for the call destination > Select a *Wide Area Medium*.

Detailed information on configuring ISDN Call Destinations is given in Chapter 7.

1a. Set the parameter *Call Type* to *On Demand.*

2. Configure IPX.

Parameter path: Select *Protocols* > Select *IPX*.

2a. Set *Packet Forwarding* to *Enabled*.

3. Bind IPX to an ISDN interface.

Parameter path: Select *Bindings* > Press <Ins> > Select *IPX* > Select a configured ISDN interface or interface group > Select *Expert Bind Options*.

3a. If you chose *NLSP with RIP/SAP Compatibility* as *Routing Protocol*, select *NLSP Bind Options* and set the *NLSP State* to *Off*.

4. Activate the configuration with the *Reinitialize System* command.

5. Then use *Client Initiated Call Control* as described above to set up and clear IPX connections manually from the NetWare server console, or from any DOS, Windows or OS/2 client.

Automatic/Permanent IPX Connections

Permanent connections are used to connect LANs in a static way; i.e. the interface of the ISDN-Controller is exclusively used for the permanent connection to the configured call destination. A permanent connection to a remote LAN is always established, when

- the router is started or reinitialized
- the logical connection has been disconnected for whatever reason.

The underlying physical call set-up is controlled by the Inactivity Timeout, i.e. the physical connection is cleared when no data traffic has been detected for the specified period, whereas the logical connection is (theoretically) maintained forever. This is why the Disconnect Timeout has no meaning for permanent connections.

What You Need

Before configuring permanent IPX connections decide whether you want to use NLSP or RIP / SAP as a routing protocol. AVM recommends that you use RIP / SAP for connections over ISDN.

Note

For RIP/SAP connections over ISDN, the Periodic Update Interval for IPX RIP and SAP is automatically set to 10000 when you reinitialize your system!

Procedure

Procedure

1. **Configure an ISDN Call Destination entry.**

   Parameter path: Select *WAN Call Directory* > Press <Ins> > Specify a name for the call destination > Select a *Wide Area Medium*.

   Detailed information on configuring ISDN Call Destinations is given in Chapter 7.

   1a. Set the parameter *Call Type* to *Permanent.*

   1b. Set the *Retry Mode* to *Retry All Failures*.

   1c. Set the *Retry Limit Handling* to *Continuous At Limit*.

   1d. Set the *Retry Interval Limit* to *8* seconds.

2. **Configure IPX.**

   Parameter path: Select *Protocols* > Select *IPX*.

   2a. Set *Packet Forwarding* to *Enabled*.

3. **Bind IPX to an ISDN interface.**

   Parameter path: Select *Bindings* > Press <Ins> > Select *IPX* > Select a configured ISDN interface or interface group.

   3a. Press <Enter> **on *WAN Call Destinations*, then press** <Ins>**.**

   3b. Select a configured permanent call destination from the list.

   3c. Set the *WAN Call Type* to *Automatic*.

3d. Set the *WAN Call Status* to *Enabled*.

3e. Leave the defaults in the *Expert Options*.

3f. Press <Esc> **to return to the *Binding IPX to a WAN Interface* menu.**

3g. Select *Expert Bind Options*.

3h. If you chose *NLSP with RIP/SAP Compatibility* as *Routing Protocol*, select *NLSP Bind Options* and set the *NLSP State* to *Off*.

4. Press <Esc> **until you return to the *Internetworking Configuration* menu and save your changes when prompted.**

5. Select the *Reinitialize System* command to bring configuration changes into effect and establish the permanent IPX connection.

Configuring Routed On-Demand Calls

Unlike the "standard" on-demand call, which relies on statically configured routes and services at each end of a point-to-point connection, a routed on-demand call runs a routing protocol while the link is active. When the link goes down, the routers and services made known by the routing protocol become unavailable. NetWare Multi-Protocol Router for ISDN 3.1 enables you to configure routed on-demand calls for each WAN call destination.

If no data crossed the link after some period of time, a Data-Link layer timer triggers the termination of the on-demand call. However, the routing protocol running over a routed on-demand call resets this timer each time it transmits a packet. This keeps the link continuously active. To solve this problem, NetWare MultiProtocol Router for ISDN 3.1 uses a similar timer that operates at the Network layer. This timer is reset only when data packets - not protocol packets - cross the link. In this way, the routing updates do not keep the link active when no data is being transmitted.

What You Need

Before you begin, you must have at least one on-demand WAN call destination configured. Further, decide whether you want to use NLSP or RIP / SAP as a routing protocol. AVM recommends that you use RIP / SAP for connections over ISDN.

Note

For RIP/SAP connections over ISDN, the Periodic Update Interval for IPX RIP and SAP is automatically set to 10000 when you reinitialize your system!

Procedure

To configure a routed on-demand call, complete the following steps:

Procedure

1. Configure an ISDN Call Destination entry.

Parameter path: Select *WAN Call Directory* > Press <Ins> > Specify a name for the call destination > Select a *Wide Area Medium*.

Detailed information on configuring ISDN Call Destinations is given in Chapter 7.

1a. Set the parameter *Call Type* to *On Demand.*

2. Configure IPX.

Parameter path: Select *Protocols* > Select *IPX*.

2a. Set *Packet Forwarding* to *Enabled*.

3. Bind IPX to an ISDN interface.

Parameter path: Select *Bindings* > Press <Ins> > Select *IPX* > Select a configured ISDN interface or interface group.

3a. Press <Enter> **on *WAN Call Destinations*, then press** <Ins>**.**

3b. Select a configured on-demand call destination from the list.

3c. Set the *WAN Call Type* to *Routed On Demand*.

3d. Set the *WAN Call Status* to *Enabled*.

3e. Leave the defaults in *Expert Options*.

3f. Select *Expert Bind Options*.

3g. If you chose *NLSP with RIP/SAP Compatibility* as *Routing Protocol*, select *NLSP Bind Options* and set the *NLSP State* to *Off*.

4. **Press** <Esc> **until you return to the *Internetworking Configuration* menu and save your changes when prompted.**

5. **Select the *Reinitialize System* command to bring configuration changes into effect.**

Reinitialize System and IPX Configuration Changes

If you change configurations that involve IPXRTR.NLM, i.e. any IPX routing protocol configurations such as from RIP / SAP to NLSP for example, select the *Reinitialize System* command from the *Internetworking Configuration* menu.

Reinitialize System automatically loads ISDNCHK.NLM to

- execute the `set force rip sap updates=on` command, and
- adjust the Update Interval for IPX RIP and IPX SAP to 10000.

chapter 10 Configuring TCP/IP

On-Demand IP Connections with Static Routes

An on-demand call is a WAN connection between two routers that becomes active only when one router must send data to the other.

Warning

On-demand calls are activated by routing protocol packets. Disable the routing protocol on the WAN interface to avoid keeping the connection up unnecessarily.

What You Need

You need the following information to configure on demand IP connections with static routes: the IP network addresses you want to route.

Procedure

To configure IP connections with static routes, perform the following steps:

Procedure

1. **Configure an ISDN Call Destination entry.**

   Parameter path: Select *WAN Call Directory* > Press <Ins> > Specify a name for the call destination > Select a *Wide Area Medium*.

   Detailed information on configuring ISDN Call Destinations is given in Chapter 7.

   1a. Set the parameter *Call Type* to *On Demand.*

   1b. Specify a *Local System ID.*

   1c. Specify the *Remote System ID*.

   With the help of the Remote System ID, the TCP / IP protocol stack relates an incoming call to a specific call destination.

2. Configure TCP/IP.

Protocol path: Select *Protocols* > Select *TCP/IP*.

2a. Set *IP Packet Forwarding* to *Enabled ("Router")*.

3. Bind IP to a WAN board.

Parameter path: Select *Bindings* > Press <Ins> > Select *TCP/IP* > Select a configured WAN interface.

3a. For *WAN Network Mode* select *Unnumbered Point-to-Point*.

The WAN Network Mode governs how IP operates over the connection.

3b. Select *WAN Call Destinations*, then press <Ins>**.**

The parameters in this menu apply only to this WAN call.

3c. Press <Enter> **on *WAN Call Destination* and select a call destination name from the list.**

3d. Set the *Type* to *Static On Demand*.

3e. Press <Enter> **on *Static Routing Table*, then press** <Ins>**.**

3f. Configure the following static route parameters:

Route to Network or Host - Enter the destination at the other end of the static route, which can be a single IP host or an IP network (that is, a group of hosts).

IP Address of Network/Host - Enter the address of the destination network or host. To select from a list of symbolic network names and addresses, press <Ins>.

Subnetwork Mask - Enter the IP address of the subnet mask. If the destination is an IP network, this is the subnet mask of that network.

Metric for this route - Enter the number of hops to the destination. This metric is directly proportional to the cost of the route. Given two routes to the same destination, the router chooses the lower-cost route.

Type of route - Specify whether the static route is *Active* or *Passive*. If the static route is active and the router discovers a lower-cost dynamic route to the same destination, it uses the lower-cost route instead of the active static route. If the lower-cost route becomes unavailable, the router returns to using the active static route. A passive static route is always used, regardless of whether the router discovers a lower-cost route to the same destination. If you want to use the static route as a backup route, select *Active*.

3g. **Press** <Esc> **to return to the *Binding TCP/IP to a WAN Interface* menu.**

3h. **Press** <Enter> **on *RIP Bind Options* and set the *Status* to *Disabled*.**

3i. **Press** <Enter> **on *OSFP Bind Options* and set the *Status* to *Disabled*.**

4. **Activate the configuration by selecting the *Reinitialize System* command from the *Internetworking Configuration* menu.**

chapter 11 *Configuring AppleTalk*

On-Demand AppleTalk Connections

You configure connections using AppleTalk as follows:

Procedure

1. **Configure an ISDN Call Destination entry.**

   Parameter path: Select *WAN Call Directory* > Press <Ins> > Specify a name for the call destination > Select a *Wide Area Medium*.

   Detailed information on configuring ISDN Call Destinations is given in Chapter 7.

   1a. Set the parameter *Call Type* to *On Demand.*

   1b. Enter your *Local System ID*.

   1c. Enter the *Remote System ID*.

   With the help of the Remote System ID, the AppleTalk protocol stack relates an incoming call to a specific call destination.

2. **Configure AppleTalk.**

   Parameter path: Select *Protocols* > Select *AppleTalk.*.

   2a. Set *Internal Network* to *Enabled*.

   An internal network is a virtual network contained within the AppleTalk module. It has no physical components and it appears to the router as if it were one of a number of networks to which the router is connected. The internal network supports two nodes, the AppleTalk stack (node 1 on the internal network) and the AppleTalk router (node 2 on the internal network).

   Packets must be routed from an external network interface to the internal network. Because the internal network requires an address, it takes up a network number. If you configure AppleTalk without configuring an internal network, to allow application support you must configure one of the bound LAN interfaces.

2b. Select *Network Number*.

Assign a unique network number between 1 and 65279 to your internal network.

2c. Select *Network Zones List*.

Enter the number of desired network zones. You can enter up to 255 zone names. If your router uses transitional routing, it is allowed to use only one zone name. Each zone name can be up to 32 characters.

2d. Set *Static Routes for On-Demand Calls* to *Enabled*.

3. Bind AppleTalk to a WAN interface.

Parameter path: Select *Bindings* > Press <Ins> > Select *AppleTalk*> Select a configured ISDN interface.

3a. For *WAN Network Mode*, select *Unnumbered Point to Point*.

The WAN network mode governs how AppleTalk operates over a WAN connection.

3b. Select *WAN Call Destinations*, then press <Ins>**.**

The parameters in this menu apply only to this WAN call.

3c. Select a call destination from the list and press <Enter>**.**

3d. Set the *WAN Call Type* to *On Demand*.

3e. Select *Static Routes*, then press <Enter>**.**

3f. Press <Ins> **to enter a static route.**

The *Static Routes for On-Demand Calls* screen is displayed. Configure the following static route parameters:

AppleTalk Network Type - Press <Enter>, select Extended or NonExtended depending on the network type of the destination network that you are configuring, then press <Enter> again.

Network Range/Number - Press <Enter>, specify the network range for extended networks or a single network number for nonextended networks, then press <Enter> again.

Hops to Network - Press <Enter>, specify the number of hops between this router and the destination network, then press <Enter> again.

Each router the packet goes through is one hop.

Network Zone(s) List - Press <Enter>, then press <Ins>, add a zone, then press <Enter> again. Repeat this procedure until you have entered all the zones on the destination network.

4. **Activate the configuration by selecting the *Reinitialize System* command from the *Internetworking Configuration* menu.**

chapter 12 Configuring Source Route Bridge

The NetWare® MultiProtocol Router™ for ISDN 3.1 product includes source route bridging software that enables you to link token ring networks over ISDN and create an extended network. This functionality is compatible with the source route bridging mechanism used by IBM to handle the flow of data between token ring networks. Source route bridging allows end stations to discover routes dynamically and determine which one to use when sending data to any particular destination.

Warning

You should use source route bridging only with leased lines such as D64S, DS01 and DS02. With standard circuit-switched lines, a high number of connection charges would accrue.

What You Need

You need the following to configure Source Route Bridge:

- the ISDN Number and Subaddress of the remote router,
- the local ring number and the remote ring number.

Procedure

To connect a bridge to another NetWare MultiProtocol Router for ISDN bridge, each side of the WAN link must be configured to operate as a half-bridge.

Complete the following steps:

Procedure

1. **Configure an ISDN Call Destination entry.**

   Parameter path: Select *WAN Call Directory* > Press <Ins> > Specify a name for the call destination > Select a *Wide Area Medium*.

Detailed information on configuring ISDN Call Destinations is given in Chapter 7.

1a. Set the parameter *Call Type* to *Permanent.*

1b. Set the *Retry Mode* to *Retry All Failures*.

1c. Set the *Retry Limit Handling* to *Continuous At Limit*.

1d. Set the *Retry Interval Limit* to *8* seconds.

2. Configure Source Route Bridge.

Parameter path: Select *Protocols* > Select *Source Route Bridge*.

2a. Set the *Bridge Status* to *Enabled*.

2b. Set the *Bridge Number*.

Both half-bridges must have the same bridge number.

3. Bind the Source Route Protocol to a WAN interface.

Parameter path: Select *Bindings*.

3a. Press <Ins>**, then select *Source Route Bridge* from the list of configured protocols.**

3b. Select the interface to which you are binding the protocol.

3c. Enter the *Ring Number* of the remote bridge.

3d. Set *Virtual WAN Ring* to *On*.

3e. Select the WAN call destination that connects the bridge to the other bridge.

4. Press <Esc> **to return to the *Internetworking Configuration* screen; save your changes when prompted.**

5. Select the *Reinitialize System* command to bring configuration changes into effect.

chapter 13 Advanced Configuration

This chapter contains information on special configuration scenarios such as semipermanent connections, backup calls and mobile-to-mobile links.

This chapter contains the following sections:

- "Special Connection Types" on page 193
- "Configuring Backup Calls for LAN-LAN Connections" on page 197

Special Connection Types

Configuring 56-Kbps Connections

In some countries (e.g. in the USA), ISDN bandwidth is restricted to 56 Kbps (instead of 64 Kbps). To achieve connectivity, the 56 Kbps option is included in the following NetWare MultiProtocol Router for ISDN D channel drivers: DSS1, VN3, CT1, NI1, 5ESS and AUSTEL.

To establish a connection to a router in a country with ISDN bandwidth restricted to 56 Kbps, add a small `r` to the ISDN Number in the ISDN Call Destination Configuration configuring this particular call destination:

```
ISDN Number: 1234567r
```

Using En-Bloc Dialing

For certain international connections, a special character is needed to indicate the end of the phone number. This will accelerate call set-up considerably from within about 12 to 15 seconds to 1 to 2 seconds.

Thus, the *Expert Configuration of ISDN Interface <Name>* contains the parameter "Dialing Suffix". The suffix you configure here is then added to the ISDN Number for international connections to mark the end of the number to be dialed.

Ask your ISDN provider whether there is a dialing suffix for the country you want to connect to.

For connections from Belgium to Germany, for example, the character to enter is #.

DS01, DS02 and D64S Leased Line Connections

Configuration of the NetWare MultiProtocol Router for ISDN 3.1 for leased lines is as follows:

Procedure

1. **Select the appropriate *D Channel Protocol* when configuring your ISDN-Controller(s) on each site.**

   This is either DS01, DS02 or D64S.

2. **Configure only one interface of your ISDN-Controller.**

   2a. Enter an *ISDN Number* at both sites.

   Configuration of an ISDN Number is required because of protocol dependencies on the network protocol layer.

   Example:

   Router A: ISDN Number: 10

   Router B: ISDN Number: 20

   2b. Leave the defaults in the *Expert Configuration of ISDN Interface <Name>*.

   2c. In the *Default Call Destination Configuration of ISDN Interface <Name>*, set the *Encapsulation Protocol* to either *AVM Proprietary* or *PPP*.

3. **Configure an ISDN Call Destination at each site.**

   3a. Set the *Call Type* to *Permanent*.

   3b. Select an *Encapsulation Protocol*.

   3c. Specify the *ISDN Number* of the respective remote site.

   In our example, this would be:

Call Destination of Router A: ISDN Number: 20

Call Destination of Router B: ISDN Number: 10

3d. Set the *Retry Mode* to *Retry All Failures*.

3e. Set the *Retry Limit Handling* to *Continuous At Limit*.

3f. Set the *Retry Interval Limit* to *8* seconds.

Using Hunt Groups

If you applied for Hunt Group Numbers, you receive a single number for different physical Basic Rate Accesses. Use of Hunt Groups is possible with all supported D channel protocols except for D64S, DS01, DS02 and GSM.

- To use Hunt Group numbering, configure an Interface Group and set the Origination Subaddress on all interfaces to the same value or leave the Origination Subaddress field empty. As a result, the system selects any available interface associated with the group for in- and outbound connection attempts.

  When you set the Origination Subaddress on all interfaces of an ISDN-Controller to the same value, incoming calls directed to this subaddress will be forwarded to any interface. When you leave this field empty, incoming calls directed to any subaddress will be accepted at this interface. For incoming calls, remote sites can be given one ISDN Number and one Subaddress to call your router.

- For LAN-LAN connections, set the Disconnect Timeout to "Same As Inactivity Timeout" to avoid situations like the following:

  If Hunt Group numbering is used for LAN-LAN calls and the Disconnect Timeout value is higher than the Inactivity Timeout, i.e. the logical connection is not terminated as soon as the physical connection goes down, the following happens: When the remote site tries to set up the physical connection after an Inactivity Timeout and all interfaces on ISDN-Controller 1, which handled the initial connection, are busy at that moment, the call is rejected by ISDN-Controller 2, the interfaces of which belong to the same Interface Group. This is because all parameters negotiated during initial call set-up and all pieces of information on the remote site are stored in ISDN-Controller A´s memory in order to take the load of the server memory. Therefore, ISDN-Controller 2 does not have this information and rejects the underlying call from the remote site.

Configuring Semipermanent Connections

Semipermanent connections are possible with the D channel protocols 1TR6, 1TR6T1 and AUSTEL.

To use semipermanent connections with the D channel protocols **1TR6** or **1TR6T1**, special .T4 files are required. For more information, refer to the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*. Configuration of semipermanent connections is as follows:

Add a small `s` to the ISDN Number. This will tell the ISDN-Controller, that this is not a circuit-switched connection and therefore treated in a different way:

```
ISDN Number: 1234567s
```

Warning

If you do not add the “s” to the ISDN Number, this connection is treated as a normal circuit-switched ISDN connection by the local exchange. This means that you would be billed the normal connection charges for circuit-switched lines in addition to the monthly fee for the “Vorbestellte Dauerwählverbindung”.

For configuring Semi Permanent Connections in Australia (D channel protocol **AUSTEL**), note the following:

In Australia, configuration of “Semi Permanent Connections” within the D channel protocol AUSTEL is done by using MSNs, not by adding an “s” at the end of the call number. The service provider assigns a specific MSN to your ISDN access if you apply for a “Semi Permanent Connection” at your ISDN access. This MSN is defined within the service provider´s own switches to be switched through as “Semi Permanent Connections”. You can mix standard circuit switched connections and “Semi Permanent Connections” by using different MSNs.

Configuring Backup Calls for LAN-LAN Connections

This section describes how to use the Internetworking Configuration utility (INETCFG) to configure a backup call for a WAN connection.

A backup call enhances the reliability of your WAN. It ensures that new connections are made successfully and that permanent connections are maintained even if your primary WAN call destination goes down. As a result, you avoid unnecessary delays and maintain high reliability over your WAN connection.

When you configure a backup call, you specify a backup WAN call destination to be used in the event that the primary WAN call destination becomes unavailable. NetWare MultiProtocol Router for ISDN switches automatically to the backup WAN call destination if the primary WAN call destination goes down. When the primary connection is restored, NetWare MultiProtocol Router for ISDN switches to the primary and terminates the backup.

You specify a backup WAN call destination by configuring two existing WAN call destinations to have an association by which NetWare MultiProtocol Router for ISDN recognizes one as the primary destination and the other as its backup.

Example:

You can use a secondary circuit-switched connection as a backup for a leased line connection. As soon as the leased line connection is interrupted, the circuit-switched connection would be used.

Configuring a Backup Call Association

Before you begin, complete the following steps:

Configure two ISDN call destinations to the same destination so that you can associate one as the backup for the other:

- For both call destinations, set the *Call Type* to *Permanent*.
- For the primary call destination, do not forget to change the Retr*y Mode* to *Retry All Failures* and adjust the *Retry Limit Handling* and the *Retry Interval*.

To configure a backup call association, complete the following steps:

Procedure

1. **Load INETCFG, then select *Backup Call Associations*.**

   The *Backup Call Associations* screen is displayed. It lists all currently configured backup call associations with the following information:

   Primary Call Destination - A WAN call destination name that has been configured to be a primary call destination.

   Backup Call Destination - A WAN call destination name that has been configured to be a backup call destination to the primary call destination.

   Status - Current status of the backup call associations.

   This screen is empty if no backup call associations are configured.

2. **Press** <Ins> **to create a new backup call association.**

   The *Backup Association Configuration* screen is displayed. The *Primary Call Destination* field is highlighted.

3. **Press** <Enter> **to display a list of configured WAN call destinations that are available to be primary call destinations.**

   A list of WAN call destinations is displayed. These are the configured WAN call destinations that are available to define as primary call destinations. Destinations that have already been configured to be primary or backup call destinations are not listed here.

4. **Select a primary call destination.**

   The *Backup Association Configuration* screen is displayed again. The *Primary Call Destination* field is filled in, and the *Backup Call Destination* field is highlighted.

5. **Press** <Enter> **to display a list of configured WAN call destinations that are available to be backup call destinations.**

   The list of WAN call destinations is displayed again. The destination you selected as a primary call destination is no longer contained in this list.

6. **Select a backup call destination.**

   The *Backup Association Configuration* screen is displayed with the *Backup Call Destination* field filled in.

7. **Ensure that *Association Status* is set to *Enabled*.**

   To change the displayed status, select *Status,* select the desired status from the pop-up display, then press <Enter>.

8. **Optionally, do the following to modify the connect and disconnect timer values:**

   8a. **Enter a new value, in seconds, in the *Connect Delay Timer* field, then press** <Enter>**.**

   When the primary call destination failed, this value is the number of seconds to delay before attempting to connect to the backup call destination.

   8b. **Enter a new value, in seconds, in the *Disconnect Delay Timer* field, then press** <Enter>**.**

   When the backup call destination is up, and the primary call destination reconnects, this value is the number of seconds to delay before disconnecting the backup call association.

9. **Press** <Esc> **to return to the *Internetworking Configuration* screen; save your changes when prompted.**

   The backup call association you configured is listed in the *Configured Backup Call Associations* screen.

10. **To configure another interface, repeat Step 2 through Step 9.**

11. **If you want these changes to take effect immediately, select *Reinitialize System*.**

    If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

chapter 14 Configuration Interdependencies

Some parameters of the NetWare MultiProtocol Router for ISDN interfere with other parameters and can, in rare cases, lead to critical situations. To help you avoid such situations, the following lists dependencies between parameters and describes their consequences.

Important

You should read through the following very carefully to avoid configuration errors and high connection charges due to parameter inconsistencies!

Interdependencies with Call Processing

When Outbound Call Processing is disabled or COSO is set to "No Dial-Out" for an ISDN interface, no outgoing calls, whether initial or for underlying call set-ups after an inactivity timeout, are possible. This has the following consequences:

- The logical connection is terminated when the local router attempts to perform an underlying call set-up.
- The Self-Learning Timeout makes no sense, since no outgoing calls are allowed.
- A Recall Request by a remote NetWAYS / ISDN client is denied.
- Channel On Demand cannot be used on the respective ISDN-Controller in the local router, since the interface cannot activate a second data channel when needed.

Outbound Call Processing and Timeout Mechanisms

The following example shows what happens when Outbound Call Processing is disabled on an interface of Router A and Inactivity Timeout and Disconnect Timeout on Router B are not set to the same value, i.e. the physical and logical connection are not terminated at the same time:

Situation

Router A:

Interface 1: Outbound Call Processing: Disabled

Router B:

Call destination
for Router A: Inactivity Timeout ≠ Disconnect Timeout

- Router B calls Router A.

Consequence

Router A is not able to perform outgoing calls, because Outbound Call Processing is disabled on the interface-level. When the connection is idle for the period specified for Inactivity Timeout, it is disconnected physically, but not logically. The logical connection is only cleared when the Disconnect Timeout expires. If, in the meantime, Router A has data packets to be transferred to Router B, it is unable to set up the physical connection to Router B.

Important

When Outbound Call Processing is disabled on an interface, Inactivity Timeout and Disconnect Timeout should be set to the same value to prevent the router from trying to set up the physical connection after an inactivity timeout.

Inbound Call Processing and Timeout Mechanisms

The following example shows what happens when Inbound Call Processing is disabled on Router A, and Router B tries to set up the physical connection after an Inactivity Timeout:

Situation

Router A:

Interface 1: Inbound Call Processing: Disabled

Call destination
for Router B: Inactivity Timeout ≠ Disconnect Timeout

- Router A calls Router B.

Consequence

When the Inactivity Timeout expires, the ISDN connection can be set up again from either site. If Router B tries to set up the ISDN connection, Router A rejects the call since Inbound Call Processing is set to Disabled.

When Inbound Call Processing is enabled, Inactivity Timeout and Disconnect Timeout should be set to the same value to prevent the remote site from trying to set up the physical connection after an inactivity timeout.

Interdependencies with Timeout Mechanisms

Security Call-Back and Timeout Mechanisms

If Router B has to transfer data to Router A in regular intervals throughout the day and the connection is terminated physically and logically after a certain period of inactivity, it does not make sense to configure Security Call-Back, since this would lead to additional costs.

Situation

Router A:

Interface 1:	Security Call-Back:	Force Call-Back to Caller-Specified Number *or* Force Call-Back to CLI Number

Router B:

Call destination for Router A:	Inactivity Timeout = Disconnect Timeout

- Router B calls Router A.

Consequence

When the connection has been idle for a specified period, it is disconnected physically and logically. When Router B again sets up the physical and logical connection, Router A hangs up and calls back. In this way, one charge unit is wasted each time by Router B. If the connection would only be terminated physically after a certain time of inactivity, Router B would be able to set up the underlying physical connection without wasting a charge unit.

Inactivity Timeout and Disconnect Timeout Set to Different Values

The following example shows what happens when the physical ISDN connection is disconnected by the Inactivity Timeout, and the logical network connection is terminated later by the Disconnect Timeout:

Situation

Router A:

Call destination for Router B:	Inactivity Timeout = 19
	Disconnect Timeout =30

Consequence

The physical connection is cleared after 19 seconds of inactivity on the link. All B channels are disestablished. When the Disconnect Timeout expires 11 seconds later, one B channel is again switched through, i.e. the physical connection is established for a short time to notify the remote site that the logical connection is now cleared. Thus, one charge unit is wasted.

Timeout Mechanisms and Spoofing/Filtering

Spoofing and filter mechanisms work only when there is a logical network connection between two sites. For dynamic interface usage, consider the following critical situation:

Situation

Router A:

Call destination for Router B:	Inactivity Timeout = Disconnect Timeout

Router A and Router B:

Spoofing and filter mechanisms: Enabled

Consequence

Filter and spoofing mechanisms in NetWare MultiProtocol Router for ISDN work only when a logical connection between two sites exists. When Inactivity Timeout and Disconnect Timeout are set to the same value, both, the physical and the logical connection are cleared when the link has been idle for the specified period. Thus, spoofing and filtering is only active during this period. After that, spoofing and filtering is terminated, i.e. Watchdog packets, SPX keep-alive-packets etc. are anew transmitted to the remote site(s) and are not spoofed on the NetWare MultiProtocol Router for ISDN. For dynamic interface usage, where the physical connection is always set up when data packets are to be transferred, this can lead to a high number of call set-ups and, consequently, charge units.

Unique MSN, EAZ or DDI Required for Each Interface

To ensure that certain NetWare MultiProtocol Router for ISDN 3.0 features work properly in an internetwork, unique MSNs, EAZs (BRI) or DDIs (BRI, PRI) are required for each interface of an AVM ISDN-Controller. Consider the following explanations:

Interface Status Time Restrictions

The Interface Status Time Restrictions should always be configured equally on each interface of an ISDN-Controller if no MSNs, EAZs or DDIs are used or if the interfaces listen to the same MSN, EAZ or DDI. Otherwise, the following occurs:

Situation

Router A:

Interface 1:	Interface Status disabled due to Time Restrictions
Interface 2:	Interface Status enabled

Interface 1 and Interface 2 have no unique MSN, EAZ or DDI or listen to the same MSN, EAZ or DDI.

- Router B calls Router A.

Consequence

Since no unique MSNs, EAZs or DDIs are configured for each of the interfaces, the ISDN-Controller cannot decide to which interface the incoming call is addressed and tries to pass it on to any interface. If the call is addressed to interface 1, it will be rejected, because the Interface Status of interface 1 is disabled. One charge is therefore wasted by Router B. The main purpose of the Interface Status Time Restrictions, i.e. barring the router completely for incoming calls during certain periods, cannot be fulfilled.

Inbound Call Processing Set Unequally On One ISDN-Controller

Inbound Call Processing should always be configured equally on each interface of an ISDN-Controller if no unique MSNs, EAZs or DDIs are used of if the interfaces listen to the same MSN, EAZ or DDI. Otherwise, the following occurs:

Situation

Router A:

Interface 1:	Inbound Call Processing:	Disabled
Interface 2:	Inbound Call Processing:	Enabled

Interface 1 and Interface 2 have no MSN, EAZ or DDI or listen to the same MSN, EAZ or DDI.

Consequence

Since no unique MSNs, EAZs or DDIs are configured for each of the interfaces, the ISDN-Controller cannot decide to which interface the incoming call is addressed and tries to pass it on to any interface. If the call is addressed to interface 1, it will be rejected, because incoming calls are not processed on interface 1. One charge unit is wasted by Router B.

ISDN Connection Monitor Thresholds Set Unequally On One ISDN-Controller

ISDN Connection Monitor Thresholds should always be configured equally on each interface of an ISDN-Controller if no unique MSNs, EAZs or DDIs are used of if the interfaces listen to the same MSN, EAZ or DDI. Otherwise, the following occurs:

Situation

Router A:

Interface 1:	Thresholds configured
Interface 2:	No Thresholds configured.

Interface 1 and Interface 2 have no unique MSNs, EAZs or DDIs or listen to the same MSN, EAZ or DDI.

- Router B calls Router A when interface 1 is barred by the ISDN Connection Monitor.

Consequence

Since no unique MSNs, EAZs or DDIs are configured for each of the interfaces, the ISDN-Controller cannot decide to which interface the incoming call is addressed and tries to pass it on to any interface. If the call is addressed to interface 1, it will be rejected, because interface 1 is barred by the ISDN Connection Monitor. One charge unit is wasted by Router B. The main purpose of the ISDN Connection Monitor, i.e. barring the router completely for incoming calls when one threshold is reached, cannot be fulfilled. A solution for this is the configuration of an Interface Group. When a threshold is reached on one of the interfaces belonging to an Interface Group, all interfaces of this group are barred for incoming and outgoing calls.

Using CLI Number Check

If you want to use CLI number check, make sure that a CLI number check (Only Registered Numbers: CLI or Only Registered Numbers: CLI and Caller-Specified) is performed on each interface of an ISDN-

Controller, if no unique MSNs, EAZs or DDIs are used. Otherwise, the following occurs:

Situation

Router A:

Interface 1:	Call Acceptance:	All Numbers
Interface 2:	Call Acceptance:	Only Registered Numbers: CLI *or* Only Registered Numbers: CLI and Caller-Specified

- Router B calls Router A.

Consequence

When Router B calls Router A, its call will always be accepted even if its CLI Number is not configured in the Call Acceptance Database.

If the situation is the other way round, i.e. interface 1 is configured to perform a CLI number check and interface to accept all numbers, a call from router B will never be accepted when its CLI Number is not configured in the Call Acceptance Database.

The Remote Site Is Not Available

Static Bundling and Channel On Demand

If you want to use Static Bundling or Channel On Demand for a connection, the requested number of B channels must be available on the remote site.

Situation

Router A:

Uses an AVM ISDN-Controller T1.

Call destination for Router B:	Static Bundling enabled with more than 1 B channel.

Router B:

Uses an AVM ISDN-Controller B1.

- Router A calls Router B.

Consequence

Router A tries to establish the connection with more than 2 B channels. Router B can maximally offer 2 B channels. The connection is established using the number of B channels router B can provide. However, the ISDN-Controller T1 is constantly trying to set up the rest of the B channels. In countries, where the attempt to set up a connection already costs a charge unit (as for example in Switzerland), this can lead to high ISDN costs! Thus, be sure that the remote site is able to provide the number of B channels you want to use at the time of the connection.

Operation of the Self-Learning Inactivity Timeout

The Self-Learning Timeout automatically adjusts the Inactivity Timeout for outgoing connections to different charge intervals over the day. To calculate the appropriate timeout value, the intervals between two charging pulses sent by the PTT are measured.

To use the Self-Learning Timeout and adapt the Inactivity Timeout, the following requirements must be met:

- the Inactivity Timeout must not be disabled.
- Advice On Charge During Call (AOCD) must be activated at your ISDN access
- the connection charges must be counted during the ISDN connection and not only at the end of the connection.

If there are changes within your Private Branch Exchange or the Local Exchange, the charging pulse can be ´lost´. If this is the case, set the Inactivity Timeout to "Time-Controlled". For more information, refer to Chapter 7, "Configuring ISDN Call Destinations".

When the Self-Learning Timeout is enabled, the NetWare MultiProtocol Router for ISDN sets the Inactivity Timeout to one charge interval minus two seconds. The calculated value is displayed on the system console as follows:

```
Calculated self-learning timeout <x>
```

The Disconnect Timeout is only adjusted, when

- Disconnect Timeout = Same As Inactivity Timeout
- Inactivity Timeout is set to ´0´ (=disabled) and Disconnect Timeout is set to any other value

In any other case, the Disconnect Timeout is not adjusted.

Spoofing and Filtering on the ISDN Driver and Network Protocol Level

NetWare MultiProtocol Router for ISDN 3.1 provides a number of filter and spoofing mechanisms on the network protocol and ISDN-Controller level.

Filters and spoofings operating on the network protocol level are configured via INETCFG.NLM and FILTCFG.NLM. For detailed information on usage and configuration of these filters, refer to the *NetWare MultiProtocol Router 3.1 Configuration* guide.

Filters and spoofings operating on the ISDN driver level are exclusively configured via "WAN Call Directory" in the INETCFG.NLM. Configuration and usage are described in detail in Chapter 7, "Configuring ISDN Call Destinations".

The main difference between mechanisms on the ISDN driver and the network protocol level is that the latter is always active even if there is no active logical connection between two sites. Filters and spoofing mechanisms on the ISDN driver level are terminated when the logical connection is cleared.

A number of filter and spoofing mechanisms can be configured on the network protocol and the ISDN driver level. Thus, if you want to disable a special mechanism, make sure that it is disabled on both levels.

chapter 15 Configuring Remote Node Access

The NetWare® MultiProtocol Router™ for ISDN allows standalone PCs, laptops, notebooks or palmtops to dial into the LAN over terrestrial ISDN or GSM-based cellular networks in order to become remote nodes on the LAN. Remote nodes can use any servers, services and resources of the LAN - the same way locally connected PCs use them. On the standalones, a remote node software and an ISDN adapter is required.

In addition to providing the server component for remote node access, NetWare MultiProtocol Router for ISDN 3.1 now also includes a single-user license of AVM´s remote node product NetWAYS/ISDN® in the latest version 3.0 for Windows 95 and Windows NT. NetWAYS/ISDN, together with any of AVM´s ISDN-Controllers for Basic Rate Interface or AVM´s Mobile ISDN-Controller M1 provides full-featured remote node access to the LAN. It uses the protocols IPX/SPX, Novell NetBIOS and/or TCP/IP. You can use NetWAYS/ISDN v2.0, 2.1 as well as the latest version 3.0, which is included with the NetWare MultiProtocol Router for ISDN 3.1, of NetWAYS/ISDN to dial in to the LAN via NetWare MultiProtocol Router for ISDN 3.1.

But besides NetWAYS/ISDN, you can use any remote node product supporting IPX, TCP/IP or AppleTalk and the PPP over ISDN protocol for dial-up.

This chapter describes what has to be done on the NetWare MultiProtocol Router for ISDN 3.1 in order to provide access for remote nodes with NetWAYS/ISDN and any PPP over ISDN-compatible remote node product. For information on the remote node site, refer to the AVM NetWAYS/ISDN manual or the manual included in your remote node product.

This chapter contains the following sections:

- "Enabling ISDNWAYS" on page 212
- "Configuring an Interface for Remote Node Access" on page 213
- "Configuring Protocols" on page 214

- "Binding IPX to ISDNWAYS" on page 215
- "Binding IP to ISDNWAYS" on page 216
- "Configuring Global Remote Node Parameters" on page 217
- "Access From Mobile NetWAYS / ISDN Clients" on page 222

The configuration for remote node access on the NetWare MultiProtocol Router for ISDN consists of the following steps:

- Enable ISDNWAYS

Important

To allow remote access from remote nodes, you only have to load ISDNWAYS once, irrespective of the number of ISDN-Controllers you want to configure.

- Configure an interface to be used for remote node access
- Configure protocols
- Bind IPX and / or TCP / IP to ISDNWAYS
- Configure Global Remote Node Parameters

Enabling ISDNWAYS

ISDNWAYS is the driver for remote node access to the NetWare MultiProtocol Router for ISDN 3.1.

Perform the following steps to enable the ISDNWAYS driver on the NetWare MultiProtocol Router for ISDN:

Procedure

1. **Load INETCFG and select *Boards*.**
2. **Press** <Ins> **to add a new board.**
3. **Select *ISDNWAYS* from the list of available drivers.**
4. **Specify a *Board Name* for ISDNWAYS.**
5. **Press** <Esc> **twice and answer *Yes* to the prompt to save your changes.**

The NetWAYS / ISDN driver is now loaded each time the router is started or reinitialized.

Configuring an Interface for Remote Node Access

Procedure

1. **From the *Internetworking Configuration* menu, select *Network Interfaces* and press** <Enter>**.**

2. **Select the interface on which you want to allow remote node access from the list of network interfaces.**

   The *ISDN Network Interface Configuration* menu is displayed.

3. **Specify *ISDN Network Interface Configuration* parameters.**

   For more information and parameter descriptions, refer to Chapter 6, section "ISDN Network Interface Configuration".

4. **Press** <Enter> **on *Expert Configuration*.**

   For more information and parameter descriptions, refer to Chapter 6, section "Expert Configuration of ISDN Interface <*Name*>".

   4a. Set the *Interface Usage* to either *Remote Node-LAN* or *Both LAN-LAN and Remote Node-LAN*.

   "Remote Node-LAN" means that this interface can only be used for connections to remote NetWAYS/ISDN and PPP-compatible clients.

   "Both LAN-LAN and Remote Node-LAN" allows both types of connections over this interface.

   4b. Set the *Remote Node Usage* to either *Exclusive Interface Reservation* or *On-Demand Interface Reservation*.

   "Exclusive Interface Reservation" means that an interface and the underlying ISDN data channel will be reserved for a connection from the first dial-in until the connection is cleared logically. The logical connection between the remote client and the interface will be maintained in case of an Inactivity Timeout (physical connection down), and any incoming call to the interface will be rejected during this period. This guarantees that an ISDN data channel will be physically available whenever data are to be transmitted from or to the remote client, and is the recommended type of remote node usage.

"On Demand Interface Acquirement" means that an interface and the underlying ISDN data channel will not be reserved for one connection, but will be released and become available for any other dial-in or dial-out operation as soon as the underlying physical ISDN data channel between the remote client and the interface is deactivated due to an Inactivity Timeout. This type is more flexible, since it allows more than one remote clients to share a single ISDN data channel. It cannot be guaranteed, however, that an ISDN data channel is available whenever data are to be transferred from or to the remote client, since the physical ISDN data channel might be in use for another remote client communicating with the LAN.

4c. Specify the other parameters as described in Chapter 6.

5. Press <Esc> **to return to the *ISDN Network Interface Configuration* menu.**

6. Select *Default Interface Call Destination*.

For more information, refer to Chapter 6, section "Default Call Destination Configuration".

6a. For PPP remote nodes, set the *PPP Destination Type* to *Remote-Node*.

The PPP Destination Type defines how PPP calls from "unknown" sites are accepted.

Remote-Node means that parameters will be negotiated as defined in RFC 1552 (IPXCP) or RFC 1332 (IPCP), depending on the network protocol. In addition, the call is visible in the ISDN Console (Remote Nodes).

7. Press <Esc> **until you are at the *Internetworking Configuration* main menu and save your changes when prompted.**

Configuring Protocols

Configure IPX and / or TCP / IP protocol parameters. For more information, refer to Chapters 9 and 10 of this Guide.

For IPX, check the setting for "Get Nearest Server Requests" and "Override Nearest Server".

Binding IPX to ISDNWAYS

Procedure

1. **From the *Internetworking Configuration* menu, select *Bindings*.**

2. **Press** <Ins> **and select *IPX* from the list of configured protocols.**

3. **Select your ISDNWAYS ´board´ from the list of configured network interfaces.**

   The *Binding IPX to a LAN* Interface menu is displayed.

4. **Enter a valid *IPX Network Number*, then press** <Enter>**.**

   The IPX Network Number is the 4-byte network number assigned to the network to which the ISDNWAYS ´board´ is attached. The range is 00000001 through FFFFFFFE.

5. **Leave the default for *Frame Type*.**

6. **Press** <Enter> **on *Expert Bind Options*.**

7. **Select *RIP Bind Options*.**

   7a. **Set the *RIP State* to *Off*.**

   Press <Esc> to return to the *Binding IPX to a LAN Interface* menu.

8. **Select *SAP Bind Options*.**

   8a. **Set the *SAP State* to *Off*.**

   8b. **Set *Get Nearest Server Requests Override* to *Accept* to allow access from remote nodes.**

   Press <Esc> to return to the *Binding IPX to a LAN Interface* menu.

9. **Select *NLSP Bind Options*.**

9a. **Set the *NLSP State* to *Off*.**

Press <Esc> to return to the *Binding IPX to a LAN Interface* menu.

10. **Press** <Esc> **until you are again at the *Internetworking Configuration* main menu and save your changes when prompted.**

Binding IP to ISDNWAYS

Procedure

1. **From the *Internetworking Configuration* menu, select *Bindings*.**

2. **Press** <Ins> **and select *TCP/IP* from the list of configured protocols.**

3. **Select your ISDNWAYS ´board´ from the list of configured network interfaces.**

   The *Binding TCP/IP to a LAN Interface* menu is displayed.

4. **Enter the IP address assigned to this interface, then press** <Enter>**.**

   This is the node´s local IP address on the network connected to this interface. The address must be entered as four decimal or hexadecimal numbers separated by dots. Each IP address on an IP internetwork must be unique and is usually assigned by the network administrator.

5. **Enter the subnetwork mask of the network attached to this interface in the *Subnetwork Mask of Connected Network* field, then press** <Enter>**.**

   This setting must match the mask used by the other nodes on the network. You can enter the subnetwork mask in decimal or hexadecimal form.

   If you do not specify the mask, the standard IP network mask is used. You can use the default subnetwork mask if your network is not subnetted. In the standard mask, each bit of the address network number is set to one and each bit of the address host number is set to zero (FF.0.0.0).

6. **Select *RIP Bind Options*.**

   6a. **Set the *Status* to *Disabled*.**

   6b. **Leave the defaults for the other parameters.**

   Press <Esc> to return to the *Binding TCP/IP to a LAN Interface* menu.

7. **Select *OSPF Bind Options*.**

   7a. **Set the *Status* to *Disabled*.**

   7b. **Leave the defaults for the other parameters.**

8. **Press** <Esc> **until you are again at the *Internetworking Configuration* main menu and save your changes when prompted.**

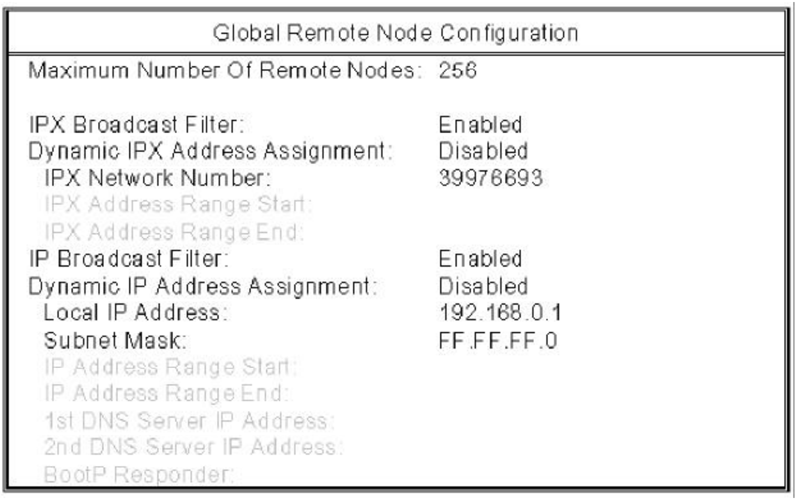
Configuring Global Remote Node Parameters

Global parameters for remote nodes include the Maximum Number of Remote Nodes and general parameters for IPX and TCP / IP. They apply for all remote nodes dialing into the NetWare MultiProtocol Router for ISDN.

The parameter path is as follows: load INETCFG > select *Network Interfaces* > select *Global Remote Node Configuration*.

The following menu is displayed:

Figure 15-1:
Global Remote Node Configuration Menu



```
                    Global Remote Node Configuration
Maximum Number Of Remote Nodes:  256

IPX Broadcast Filter:            Enabled
Dynamic IPX Address Assignment:  Disabled
  IPX Network Number:            39976693
  IPX Address Range Start:
  IPX Address Range End:
IP Broadcast Filter:             Enabled
Dynamic IP Address Assignment:   Disabled
  Local IP Address:              192.168.0.1
  Subnet Mask:                   FF.FF.FF.0
  IP Address Range Start:
  IP Address Range End:
  1st DNS Server IP Address:
  2nd DNS Server IP Address:
  BootP Responder:
```

Procedure

1. **Enter the *Maximum Number of Remote Nodes*.**

   This parameter defines the maximum number of remote nodes that can be handled on the NetWare MultiProtocol Router for ISDN.

   Default: 256

   Options: 0 - 2048

   Specify the maximum number of remote nodes you want to allow access to the NetWare MultiProtocol Router for ISDN.

Note

Each active remote node requires 6 KB of RAM on the router PC.

2. **Check the *IPX Broadcast Filter*.**

   This parameter specifies whether all IPX broadcasts not directed to a specific remote client are filtered.

   Default: Enabled

   Options: Enabled, Disabled

   When the IPX Broadcast Filter is enabled, all IPX broadcasts that are not directed to a specific remote client, i.e. broadcasts with the destination type FF.FF.FF.FF, are filtered.

When it is disabled, such IPX broadcasts are duplicated for each active remote client and sent over ISDN.

3. **Decide whether you want to use *Dynamic IPX Address Assignment*.**

Dynamic IPX Address Assignment defines whether or not a remote node is assigned an available node address on call set-up.

Dynamic IPX Address Assignment can only be used if this feature is supported by the remote node access software used on the remote site. With AVM NetWAYS/ISDN 2.1 and the 16-bit IPXODI protocol stack, this is possible. With NetWAYS/ISDN 3.0 and Windows 95, this cannot be used.

Default:	Disabled
Options:	Disabled, Enabled

If this parameter is disabled, the remote node will use the node address configured in the remote node access software.

Enabled means that each time a logical connection between a remote node and the router is established, the remote node is assigned an available node address from the configured IPX address range.

3a. **Check the *IPX Network Number*.**

This field is read-only. It shows the network number ISDNWAYS is bound to (see above).

3b. **Enter the *Address Range Start*.**

Enter the starting address of the range for remote IPX clients.

3c. **Enter the *Address Range End*.**

Enter the ending address of the range for remote IPX clients.

4. **Check the *IP Broadcast Filter*.**

This parameter specifies whether all IP broadcasts not directed to a specific remote client are filtered.

Default:	Enabled
Options:	Enabled, Disabled

When the IP Broadcast Filter is enabled, all IP broadcasts that are not directed to a specific remote client, i.e. broadcasts with the destination type 255.255.255.255, are filtered.

When it is disabled, such IP broadcasts are duplicated for each active remote client and sent over ISDN.

5. **Decide whether you want to use *Dynamic IP Address Assignment*.**

   Dynamic IP Address Assignment defines whether or not a remote node is assigned an available node address on call set-up.

   Dynamic IP Address Assignment can only be used if this feature is supported by the remote node access software used on the remote site. With AVM NetWAYS/ISDN 2.1 and the 16-bit IPXODI protocol stack, this is done with the help of BootP and the BootP Responder. With NetWAYS/ISDN 3.0 and Windows 95, this is done using a DHCP server.

Default:	Disabled
Options:	Disabled, Enabled

   If this parameter is disabled, the remote node will use the IP address configured in the remote node access software.

   Enabled means that each time a logical connection between a remote node and the router is established, the remote node is assigned an available node address from the configured IP address range. This is also possible with PPP remote nodes (IPCP).

   5a. Check the *Local IP Address*.

   This field is read-only. It shows the IP address ISDNWAYS is bound to (see above).

   5b. Check the local *Subnet Mask*.

   This field is read-only. It shows the Subnet Mask ISDNWAYS is bound to (see above).

   5c. Enter the *Address Range Start.*

   Enter the starting address of the range for remote IP clients. The client address range must be on the same network or subnetwork as the server address specified in the *Local IP Address* field (see above).

5d. Enter the *Address Range End*.

Enter the ending address of the range for remote IP clients. The client address range must be on the same network or subnetwork as the server address specified in the *Local IP Address* field (see above).

5e. *1st DNS Server IP Address*

Enter the IP Address of the first DNS server that is accessed during BootP or IPCP negotiation (RFC 1877).

5f. *2nd DNS Server IP Address*

Enter the IP Address of the second DNS server that is accessed during BootP or IPCP negotiation (RFC 1877).

5g. BootP Responder.

This parameter lets you define whether or not the NetWare MultiProtocol Router for ISDN should answer BootP requests from remote nodes.

Default: Disabled

Options: Disabled, Enabled

When this parameter is disabled, the NetWare MultiProtocol Router for ISDN does not answer BootP requests from remote nodes.

When BootP Responder is enabled, the ISDN driver responds to BootP requests from remote nodes.

Important

Do not use BootP Responder when DHCP server is loaded on the NetWare MultiProtocol Router for ISDN.

To bring the configuration changes into effect, use the *Reinitialize System* command from the *Internetworking Configuration* menu.

Access From Mobile NetWAYS/ISDN Clients

NetWare MultiProtocol Router for ISDN 3.1 supports both, access from NetWAYS / ISDN clients through cellular digital networks and NetWAYS / ISDN clients through terrestrial ISDN lines, concurrently on the same ISDN-Controller.

In order to set up calls, underlying call-backs as well as security call-backs, to remote NetWAYS / ISDN clients using Mobile ISDN-Controller M1 and cellular networks, NetWare MultiProtocol Router for ISDN is able to interpret the dialing suffix “m” if delivered by the NetWAYS / ISDN client.

chapter 16 Utilities

This Chapter lists and describes the ISDN-specific utilities included in the NetWare MultiProtocol Router for ISDN 3.1. For information on other utilities, refer to the *NetWare MultiProtocol Router 3.1 Configuration* guide.

ISDN Budget Manager

The ISDN Budget Manager is integrated in ISDNCCA.NLM and allows configuration of the maximum amount of money or the maximum number of charge units you want to spend for a call destination per month, week and day.

When one of the maximum values is reached, the connection to the remote site is cleared and incoming and outgoing connections to this call destination are no longer allowed.

ISDN Console (ISDNCON.NLM)

ISDN Console is a menu-assisted utility providing detailed information for the monitoring and controlling of ISDN connections as well as of ISDN-Controllers and their interfaces.

ISDN Console is described in detail in Chapter 18, "Monitoring ISDN Connections."

ISDN Connection Monitor

The ISDN Connection Monitor is integrated in ISDNCCA.NLM and allows you to configure special interface-related thresholds on a 24 h basis, such as the maximum physical up-time per interface, the maximum outgoing calls per interface and the maximum charge units per interface. Those values are configured via INETCFG.

The ISDN Connection Monitor watches the interfaces of an ISDN-Controller. As soon as the threshold value for an interface is reached, an alert is generated 3 times in 1-minute intervals and printed on the system console. After that, the respective interface is automatically barred; i.e., all connections set up over this interface are cleared, no outgoing calls can be established over it and incoming calls on the ISDN-Controller are rejected if addressed to this interface until the administrator removes this bar.

The ISDN Connection Monitor is described in detail in Chapter 18, "Monitoring ISDN Connections."

ISDNU.NCF

The ISDNU.NCF file contains commands for unloading the ISDN drivers of the NetWare MultiProtocol Router for ISDN 3.1.

ISDNSNMP.NLM

ISDNSNMP.NLM is the SNMP Agent to be used by AVM´s MPR for ISDN Router Manager product or by any SNMP-based application. ISDNSNMP.NLM initiates and responds to requests for management information as described in the MPR4ISDN.MIB.

The load command for ISDNSNMP.NLM is included in the autoexec.ncf file of the server, thus ensuring that it is automatically loaded each time the server is started.

ISDN.CFG

ISDN.CFG is the configuration file for various NLMs and drivers provided with the NetWare MultiProtocol Router for ISDN 3.1. It contains sections for configuring the following:

Statistic Update Interval, ISDNCON.NLM, ISDNLOG.NLM, ISDNSNMP.NLM, ISDNCMON.NLM, ISDN*.LAN, etc.

ISDNCONV.NLM

ISDNCONV.NLM is a utility that converts existing NetWare Multi-Protocol Router for ISDN 2.x and 3.0 databases to 3.1 databases.

ISDNCONV.NLM does the following:

- Converts the ISDNCMON.CFG to the ISDN.CFG.
- Generates load commands in the autoexec.ncf file to load SPX and Packet Burst patches.
- Removes old NetWare MultiProtocol Router for ISDN files from the SYS:SYSTEM directory, such as ISDN.LAN, VN3.T4, CT1.T4, PPPDEBUG.NLM, etc.
- Logs all changes in the SYS:ETC\ISDNCONV.LOG file.

Note

There are some items which are not automatically chaged with the ISDNCONV.NLM. For more information, refer to the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*.

ISDNCHK.NLM

The ISDNCHK.NLM is a tool to verify your configuration. It detects inconsistencies in your router configuration and displays them on the system console, together with the necessary tasks to perform.

ISDNCHK is loaded automatically each time you select the *Reinitialize System* command from the *Internetworking Configuration* menu and performs the `set force rip sap updates=on` command and adjusts the Periodic Update Interval for IPX RIP and IPX SAP to 10000.

ISDNINFO.NLM

ISDNINFO.NLM is a support tool to gather relevant information in a quick and convenient way. The gathered information is stored in the ISDNINFO.DAT file which is automatically written to the SYS:ETC directory.

Before calling AVM Technical Support, you should therefore run ISDNINFO.NLM.

Enter the following command at the system console of each router in the WAN:

```
load isdninfo <Enter>
```

The ISDNINFO.DAT file gathers the following information:

- The configuration of all interfaces loaded
- All ISDN call destination configurations
- The contents of the following files:

STARTUP.NCF	
AUTOEXEC.NCF	
ETC\INITSYS.NCF	
ETC\NETINFO.CFG	-> all INETCFG commands
ETC\SNMP.CFG	-> SNMP information for this node
ETC\TRAPTARG.CFG	-> SNMP Manager Table (IPX, TCP/IP)
ETC\REMOTE.ID	-> contains all Remote System IDs
ETC\NLSP.CFG	-> IPX configuration information
ETC\IPWAN.CFG	->TCP/IP configuration information
ETC\TCPIP.CFG	-> "
ETC\ATTYPES.CFG	-> AppleTalk configuration information
ETC\ATWAN.CFG	-> "
ETC\ATZONES.CFG	-> "
ETC\AURP.CFG	-> "
ETC\BUILTINS.CFG	-> FILTCFG.NLM configuration
ETC\FILTERS.CFG	-> "
ETC\ISDN.CFG	-> ISDN configuration file
ETC\ISDNCRON.CFG	-> Time Restrictions configuration file
ETC\ISDNCADB.CFG	-> ISDN Call Acceptance Database
SYSTEM\INSTALL.LOG	-> Installation log file
ETC\CONSOLE.LOG	
ETC\ISDNCONV.LOG	-> ISDNCONV.NLM log file
ETC\NWPARAMS.LOG	
SYSTEM\SETANDS.CP	->NetWare 4.1
SYSTEM\TIMESYNC.CFG	-> "
SYSTEM\DSFILTER.DAT	-> "

To gather configuration information, you can also use the TECHWALK.NLM. For more information, refer to the NetWare *MultiProtocol Router 3.1 Configuration* guide.

NDS over ISDN Console (NDSCON.NLM)

The NDS over ISDN Console is realized in the form of a NetWare Loadable Module™ (NLM™) and monitors NDS traffic on ISDN lines.

For more information on using the NDS over ISDN Console, refer to Chapter 18, "Monitoring ISDN Connections."

chapter 17 Testing and Troubleshooting

This chapter describes possibilities to test your ISDN access and the configuration of your router and discusses solutions for common problems.

This chapter contains the following sections:

- "Testing Possibilities" on page 229
- "Troubleshooting Tips" on page 235

Testing Possibilities

The following sections provide a set of procedures for verifying the correct operation of NetWare MultiProtocol Router for ISDN. Once you have correctly and completely installed and configured NetWare MultiProtocol Router for ISDN, testing the router is relatively easy.

You can do the following to test your router:

- ♦ Establish an IPX connection to the NetWare MultiProtocol Router for ISDN in the AVM Data Call Center to check your ISDN access and your router configuration.
- ♦ Perform a TCP/IP loopback test to check your ISDN access and your router configuration.
- ♦ Use ISDNCHK.NLM to verify correct configuration of the Periodic Update Interval.

  For more information on ISDNCHK.NLM, refer to Chapter 16 of this Guide, "Utilities".
- ♦ Use IPXPING to test reachability of an IPX target node on your internetwork.
- ♦ Use TPING/PING to test reachability of an IP target node on your internetwork.

Calling the AVM Data Call Center

The MPR for ISDN Server in the AVM Data Call Center (ADC) in Berlin can be used as a test destination, for example if you configure your first router and do not have an own remote site to connect to. You may further dial-up the AVM Data Call Center from time to time to check for any *news and downloads*, such as Release Notes on new products or enhancements to existing products.

To access the NetWare MultiProtocol Router for ISDN in the AVM Data Call Center, you will need the following connection parameters:

- Calling information:

ISDN Number: 03039984350 (when calling from somewhere in Germany)

Subaddress: 1

For calls from outside Germany, complete the Destination Address by first entering your international dialing prefix and the country code "49" for Germany, and then continue with "3039984350".

- Protocol specifics

Currently, only IPX/SPX is enabled on this router. The internal network numbers of the intranet are 39984xxx. Do not configure this number on your router too if you want to connect to AVM's ISDN Service Router, since this number must be unique within a WAN. Further, make sure that it is not filtered.

Note

TCP/IP will be enabled in the future. Access information will then be given in the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*.

- Login information

Server: adc

User name: guest.avm

Password: no password required

Performing a TCP/IP Loopback Test

After configuring the router software, you can first run a loopback test to check your ISDN access as well as the configuration of your router. To perform such a loopback test you will configure your local router to call itself. For this test, an outgoing call can be initiated over one interface of an ISDN-Controller to another interface of the same ISDN-Controller.

In the following, configuration of a loopback test on an AVM ISDN-Controller B1 is described. The outgoing call is initiated over interface 1 of the Controller and is received on interface 2. The interfaces are called AVM-B1-1_1 (interface 1) and AVM-B1-1_2 (interface 2):

Procedure

1. Configure an ISDN Call Destination.

Parameter path: Select *WAN Call Directory* > Press <Ins> > Specify LOOP as a name for the call destination > Select a *Wide Area Medium*.

Detailed information on configuring ISDN Call Destinations is given in Chapter 7.

1a. As a *Wide Area Medium*, select *ISDN-BRI*.

1b. For *Interface Name*, select the first interface of your ISDN-Controller.

In this example, it is AVM-B1-1_1.

1c. In the *ISDN Number* field, specify the number of the ISDN access, the ISDN-Controller is connected to.

1d. Enter *2* in the *Subaddress* field.

1e. Enter *LOOP* for *Local System ID and Remote System ID*.

1f. Leave the default values in the other fields.

2. Configure TCP/IP.

Parameter path: Select *Protocols* > Select *TCP/IP*.

2a. Leave the default values in the *TCP/IP Protocol Configuration*.

3. Bind TCP/IP to the two ISDN interfaces.

Parameter path: Select *Bindings* > Press <Ins> > Select *TCP/IP* > Select a configured ISDN interface.

3a. For each of the two interfaces, select *Unnumbered Point-to-Point* as the *WAN Network Mode*.

4. **Press** <Esc> **until you return to the *Internetworking Configuration* menu and save your changes.**

5. **Select the *Reinitialize System* command from the *Internetworking Configuration* to bring the configuration changes into effect.**

6. **Load CALLMGR.NLM.**

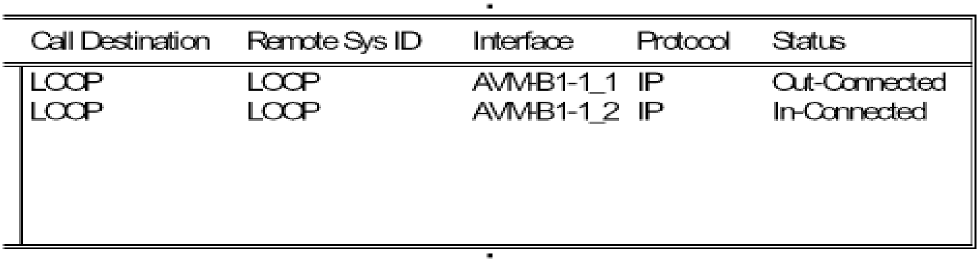
7. **Establish the loopback connection.**

   7a. **Press** <Ins> **and select the *LOOP* entry from the list. Press** <Enter> **to establish the connection.**

   The connection is displayed as follows:

For an AVM ISDN-Controller T1, loopback configuration is similar. You have to select ISDN-PRI instead of ISDN-BRI as a wide area medium, of course.

Figure 17-1: Loopback Test



```
Call Destination   Remote Sys ID   Interface      Protocol   Status
LOOP               LOOP            AVM-B1-1_1     IP         Out-Connected
LOOP               LOOP            AVM-B1-1_2     IP         In-Connected
```

The IPXPING utility enables you to check connectivity to an IPX server on your internetwork.

Using the IPXPING Utility

IPXPING determines the reachability of the IPX server or workstation - the target node - to which it sends the request packet. After the node receives the packet, it sends an IPXPING reply packet to the system that sent the request packet.

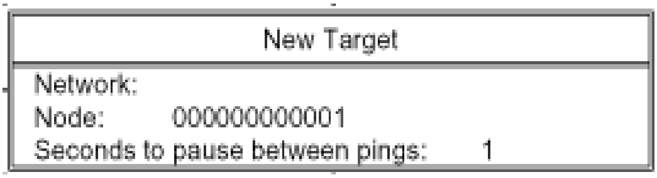
This section describes the interface for IPXPING. IPXPING determines the reachability of an IPX "target" node on your internetwork, to which it sends a request packet. If the target node receives the request packet, it sends back a reply packet.

To use IPXPING, type the following command at the server prompt:

```
LOAD IPXPING <Enter>
```

The system displays the *New Target* window:

Figure 17-2:
IPXPING New Target window



New Target

Network:
Node: 000000000001
Seconds to pause between pings: 1

The IPXPING New Target window allows you to configure and perform the PING function.

Table 17-1:
Fields in the IPXPING New Target window

Field	Description
Network	Lets you select a target IPX server by entering its IPX address.
Node	Lets you select a target IPX server by entering its node number. You must enter both the IPX address and node number to select the server.
Seconds to pause between pings	Lets you specify the number of seconds between each packet transmission.

To start sending request packets, press <Esc>. The sending node continues to send request packets and collect response time statistics until you press <Esc> again and exit IPXPING.

Request and reply packets use the same format; each packet contains the standard IPX header.

To select additional IPX servers, press <Insert>. Enter the IPX address of the server in the Address field. Press <Esc> to start sending packets.

Using the TPING Utility

The TPING utility enables you to send an ICMP echo request packet to an IP node on your internetwork.

TPING determines the reachability of an IP target node on your internetwork, to which it sends a request packet. If the target node receives the request packet, it sends back a reply packet.

To use TPING, type the following command at the server prompt and press <Enter>:

```
LOAD TPING host [packet size [retry count]]
```

where,

Host is the symbolic hostname or IP address of a TCP/IP system on the network.

Packet size is the size, in bytes, of the ICMP packet.

Retry count is the number of times you want to send an ICMP packet to the host system until a reply is received.

TPING sends a maximum of five ICMP echo request packets to the target node by default. If it receives a response, TPING stops sending requests and displays a message indicating that the target node is reachable. If it does not receive a response, TPING displays a message indicating that the target node did not respond.

Using the PING Utility

The PING utility enables you to send an ICMP echo request packet to an IP node on your internetwork.

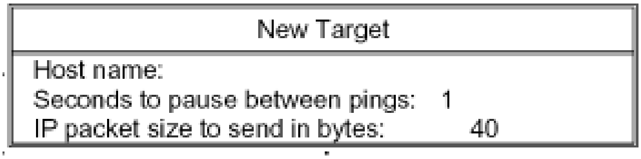
This section describes the interface for PING. PING determines the reachability of an IP target node on your internetwork, to which it sends a request packet. If the target node receives the request packet, it sends back a reply packet.

To start PING, type the following command at the server prompt:

```
LOAD PING <Enter>
```

The system displays the New Target window:

Figure 17-3:
PING New Target window



New Target

Host name:
Seconds to pause between pings: 1
IP packet size to send in bytes: 40

The PING New Target window allows you to configure and perform the PING function.

Table 17-2:
Fields in the PING New Target window

Field	Description
Host name	Lets you select a target IP node by entering its hostname or Internet address.
Seconds to pause between pings	Lets you specify the number of seconds between each packet transmission.
IP packet size to send in bytes	Lets you specify the size of the PING packet in bytes.

To start sending packets, press <Esc>. The sending node continues to send request packets and collect response time statistics until you press <Esc> again and exit PING.

To select additional IP nodes, press <Insert>. Enter the IP address of the node in the Host Name field. Press <Esc> to start sending packets.

Troubleshooting Tips

This section is intended to give you hints and tips for solving common problems on your own. However, if you are not able to solve your problem, refer to section “Before Calling Technical Support” at the end of this Chapter for details on which pieces of information you have to provide to technical support.

Please note that in this *NetWare MultiProtocol Router for ISDN 3.1 Installation and ISDN Configuration* guide, only the ISDN-related troubleshooting information is given. Further ISDN-related troubleshooting tips might be found in the *Technical Note on NetWare*

MultiProtocol Router for ISDN 3.1. If this does not help to solve your problem, please refer to the *NetWare MultiProtocol Router 3.1 Management and Troubleshooting* guide for further troubleshooting information.

Important

To solve your problems arousing during operation of the NetWare MultiProtocol Router for ISDN, also have a look at the ISDN line management messages. They contain information that might help you to sort out the problem quickly.

One frequent support issue is that customers so not configure ISDN at all during their very first NetWare MultiProtocol Router for ISDN installation, and contact support personnel for help.
Please make sure you read through all the set-up and configuration information provided in this Guide including configuration information for ISDN-Controllers, Interfaces and Call Destinations before you consider to contact your support personnel.

Problems with Call-Setup over ISDN (ISDN Error Messages 34xx and 33xx)

ISDN Errors 33xx and 34xx

To locate the problem, check whether you can set up a connection to the AVM Data Call Center with the routers at either side (see above for access information).

If you installed your NetWare MultiProtocol Router for ISDN and the ISDN-Controllers within a Private Branch Exchange (PBX), make sure you entered your "PBX Outside Line Access" in the "ISDN Network Interface Configuration" and as the first digit(s) of the "ISDN Number" of a remote site you want to call in the "ISDN Call Destination Configuration".

Use the CONNECT file transfer program coming with your AVM ISDN-Controller(s) for BRI between both routers to verify that your ISDN accesses are working properly for incoming and outgoing connections. For information on how to use CONNECT, refer to your controller manual.

You can also try to establish a connection between the CONNECT program and a NetWare MultiProtocol Router for ISDN. You will not be able to transfer files, of course, but if the ISDN network returns the message "Incompatible file transfer protocol", an ISDN connection could be set up and your ISDN accesses are working properly. If you do not get this message, use the CONNECT program on both sites and try again.

If you do not see an incoming call on the system console, perform a packet trace on the D channel to analyze the problem. For more information on packet trace, refer to Chapter 18, "Monitoring ISDN Connections."

If none of the tests is successful, contact your local PTT and have them check your ISDN accesses.

If this does not help either, refer to section "Before Calling Technical Support" at the end of this Chapter.

Network Protocol Errors

Inconsistencies in the configuration of the protocol-specific parameters (Protocol Parameters and / or Protocol Bindings) may cause problems in the logical, protocol-specific connection handling.

These causes do not exclude each other. For example, an IPX connection to a remote router could not be established because a) the call has been initiated to a Destination Subaddress that is not configured at the remote router, which causes a problem in the ISDN-specific connection handling and b) there are no IPX static routes and services configured on the local router, which causes a problem in the logical, IPX-specific connection handling.

For more information, see "Problems with IPX" below.

Problems with IPX

1. **A connection to a remote router using IPX cannot be established or a server on a remote LAN B is at first reported in LAN A, but "disappears" after a certain time.**

The most likely cause for this problem is that an IPX network number exists twice in the WAN. The assigned network numbers for IPX (file servers, LAN adapters) must be unique in the entire WAN. When interconnecting separate LANs (as well as when locally adding new segments to a LAN) for the first time, IPX network address conflicts, resulting from inconsistencies in the IPX number assignment, frequently occur.

Conflicts caused by inconsistencies in the IPX number assignments will result in one of the following situations:

- An IPX-connection over ISDN cannot be established between two networks although the ISDN-specific connection handling works properly.
- A server on a remote LAN B is at first reported in LAN A (e.g. by SLIST), but “disappears” after a certain time.
- A copy operation is successful from LAN A to LAN B, but not from LAN B to LAN A. (This situation might also be caused by incorrect packet size settings, see 3. below)

Solution:

Check IPX Network Numbers and , if you are dialing a NetWare MultiProtocol Router for ISDN 3.1, whether “set force rip / sap updates” is set to “on”.

The network numbers and internal network numbers assigned for IPX must be unique throughout the WAN; i.e. you must not assign the same address twice. This restriction often leads to one or more address conflicts when individual LANs are first connected, or when new segments are added to a LAN.

2. **A copy operation is successful from LAN A to LAN B, but not from LAN B to LAN A.**

A collision problem might exist between the configured IPX network numbers.

Solution:

Check the assignment of IPX network numbers configured for inconsistencies, all numbers must be unique in the whole WAN.

Suggestion

Novell has developed a special “Network Registry Program” to perform the task of assigning IPX numbers. If you are interested in this program, contact Novell at +1 408 321-1506 (phone) or +1 408 956-0463 (fax).

Problems with TCP/IP

If you are running FTP, you might see the following warning messages on the system console:

```
CANNOT START SYS:ETC\NET\NETWARE\SERVICES

NETDIR_GET BY NAME:N2A:SERVICE NAME NOT FOUND

CANNOT MAP TO TCP
```

```
UDP:REMOTE TRANSPORT
```

```
-OR-
```

```
MODULE NISBIND.NLM IS BEING REFERENCED. YOU
MUST UNLOAD HOSTG.NLM BEFORE UNLOADING
NISBIND.NLM
```

```
ERROR UNLOADING. KILLED LOADED MODULE.
```

You might also see the following message on the product kernel message screen:

```
COULD NOT START UDP SERVICE.
```

Miscellaneous Problems

Ignore these messages. FTP will function normally.

An ISDN connection is physically established although there are no active workstation sessions with the remote servers/routers.

The causes for this may be very diverse. It may happen that routing information is exchanged unnecessarily often or that an anti-virus program automatically scans all servers in very short intervals.

Solution:

a. Check, if you set all filter and spoofing mechanisms and all timers to appropriate values.

b. If you set appropriate values for the items mentioned above and you still have a number of ISDN connections built up, use the Packet Trace function of the ISDN Console or use SNMP to find out which packets cause these frequent ISDN call set-ups.

Getting Information on Product Enhancements and Fixes

c. Perform a packet trace. For more information on packet trace, refer to Chapter 18, "Monitoring ISDN Connections."

To stay informed about product enhancements and fixes, AVM recommends to regularly dial up the AVM Data Call Center.

There, you will find information on new releases and patches for the NetWare MultiProtocol Router for ISDN and other networking

Before Calling Technical Support

products by AVM. Maybe a solution to your problem already exists!

See section "Calling the AVM Data Call Center" above for numbers and access information.

To solve your problem, the following information is required:

1. A detailed description of the problem and a sketch of your WAN including the IPX and IP addresses of all components.
2. Your ISDN numbers and the D channel protocol used.
3. The error message displayed.
4. If you are not able to set up an ISDN connection, the results of the tests with the CONNECT file transfer program.
5. The latest ISDNINFO.DAT file (SYS:ETC\).

   To create ISDNINFO.DAT, enter

   ```
   load isdninfo.nlm
   ```

   at the server console.
6. If it is not included in the ISDNINFO.DAT, a copy of the STARTUP.NCF file.
7. The ISDN line management daily log file that documents your problem.
8. A hard copy of your SYS:SYSTEM directory.

This information is important and will help to solve your problem more quickly.

chapter 18 *Monitoring ISDN Connections*

You should read through this chapter very carefully, since it provides important information on monitoring and controlling ISDN connections.

Monitoring ISDN connections is extremely important. It gives you an impression of the number of ISDN connections established each day and of the resulting connection charges. To keep connection charges as low as possible, monitoring is indispensable for cost-effective use of the NetWare®MultiProtocol Router™ for ISDN 3.1.

The NetWare MultiProtocol Router for ISDN 3.1 provides the following monitoring features:

- ISDN Console to display detailed online information on ISDN connections and on ISDN-Controllers and their interfaces. In addition, all ISDN line management messages and connection information can be stored in log files and different trace options can be defined and enabled.
- ISDN Budget Manager to define the maximum amount of charges allowed for an individual call destination per month, per week and per day. When one of the maximum values is reached, the Call Status of this call destination is disabled, i.e. no outgoing or incoming connections are allowed to or from this destination.
- ISDN Connection Monitor to limit the maximum physical up-time, the maximum outgoing calls and the maximum charge units per interface by defining individual thresholds for these values. When a threshold is exceeded, the interface is barred for outgoing and incoming calls.
- NDS over ISDN Console to monitor NetWare 4.1 synchronization traffic over ISDN.

This chapter contains the following sections:

- "Online Information via ISDN Console (ISDNCON.NLM)" on page 242

- "Limiting ISDN Connections" on page 259
- "NDS over ISDN Console - Monitoring NDS Traffic" on page 261

Online Information via ISDN Console (ISDNCON.NLM)

ISDN Console is a menu-assisted utility providing detailed information for the monitoring and controlling of ISDN connections as well as of ISDN-Controllers and their interfaces.

ISDN Console offers:

- Online information on all established ISDN connections at a glance (daily, weekly and monthly statistics).
- Detailed status information and statistics on all ISDN connections, remote nodes, ISDN-Controllers and their interfaces, as well as on all protocols.
- "Packet Trace" options to extract packet specific information (source, destination, etc.) during transmission:
  - Network Protocol Trace option (IPX, TCP / IP,...)
  - D Channel Protocol Trace option
  - PPP Protocol Trace option

It is strongly recommended that you use ISDN Console to monitor all ISDN activities at regular, daily intervals and especially after having installed new applications, such as antivirus programs, electronic mail applications or management software, or after having reorganized the communication structure. Besides, use the log file option of ISDN Console to automatically log and store all ISDN line management messages.

Loading ISDN Console

Load the ISDN Console by typing the following command at the system console:

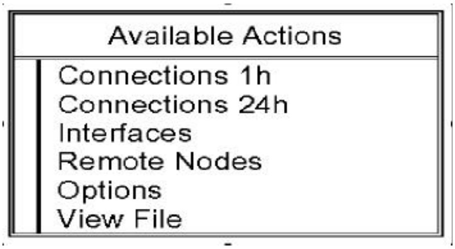
```
load ISDNCON <Return>
```

To have the ISDN Console loaded each time the server / router is reset, use the *User-specified proto* option in `INETCFG -> Protocols`:

Press <Ins> to display an empty "Protocol Command Configuration" mask and enter ISDNCON in the first line. Press <Enter>, then <Esc> and save your changes. ISDNCON will be loaded each time the server / router is reset.

The ISDN Console main menu appears on the screen:

Figure 18-1:
ISDN Console, Available Actions



Note Logging is always activated, even if ISDN Console is not loaded.

The function key assignment within ISDN Console is listed in Table 18-1:

Table 18-1:
ISDNCON function keys

Key	Description
Arrow keys	Move the highlight through menu items.
PgUp/PgDn, Arrow keys	Scroll through table entries.
Enter	Select the currently highlighted entry.
Del	Connections 1h and Connections 24h: Clear protocol connections from or to one interface manually. You should mind, however, that, if the connections are established automatically, the connection will always be set up again.
Del	Interface statistics: Reset Thresholds.
Del	Remote Nodes: Clear connection to the remote node manually.
Del	View File: Delete highlighted file.
F3	View File: Delete all files.
Tab	Connections 1h and Connections 24h: toggle between display of the call destination name and the number of the remote site.

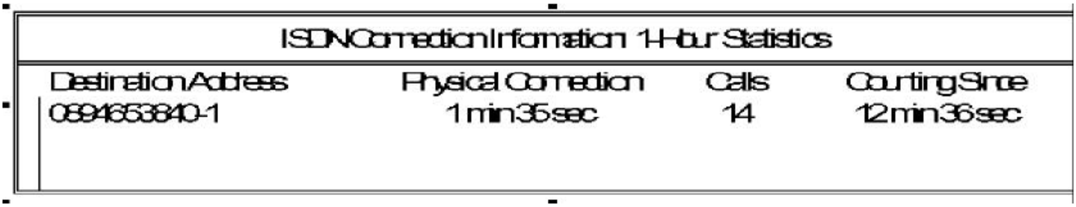
Tab	Interface statistics: Activate Trace and display the Trace window.
Esc	Return to the previous menu level (from the start-up screen also quit ISDN Console).

Statistics in ISDN Console

"Connections 1h" and "Connections 24h": Connection-Oriented Information

The submenus "Connections 1h" and "Connections 24h" display status information on all ISDN connections logically established at a given time. When you select "Connections 1h", the following menu appears on your screen:

Figure 18-2:
Connections 1h



```
              ISDN Connection Information 1-Hour Statistics
 Destination Address     Physical Connection    Calls    Counting Since
 0894653840-1                1 min 35 sec         14      12 min 36 sec
```

Table 18-2:
Information provided in "1-Hour Statistics" and "24-Hour Statistics"

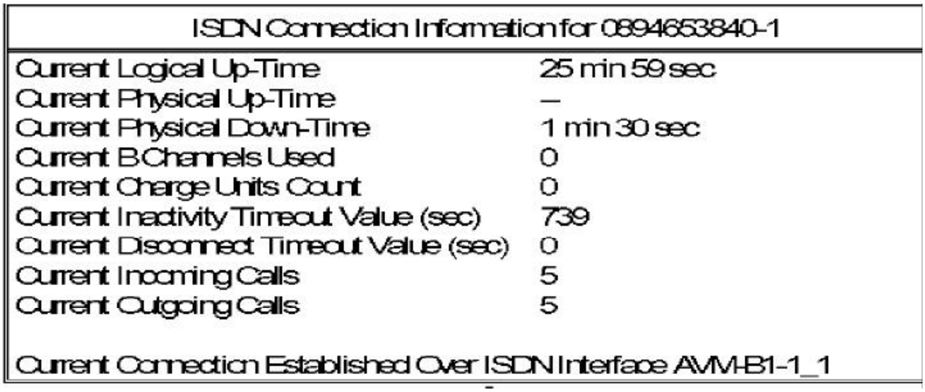
Information	Description
Destination Address	Complete ISDN number to reach the remote LAN, consisting of the Destination Address and Destination Subaddress configured in the ISDN Call Destination Configuration.
Physical Connection	Total physical connection time, as compared with the time indicated in "Counting Since".
Calls	Total number of sent and received calls, as compared with the time indicated in "Counting Since".
Counting Since	Current counting time, as compared with the time interval (1 hour or 24 hours).

Note

"Counting Since" always shows the time that has passed between the last reset (after each hour or each day, starting at 00.00 h PC time) and the current time, and does not depend on whether ISDN Console has already been loaded or is loaded for the first time.

To view more details on a single ISDN connection, select it from this menu by moving the Up and Down arrow keys and press RETURN. The following menu will be displayed on the screen:

Figure 18-3:
ISDN Connection Information for ...



```
              ISDN Connection Information for 0894653840-1
Current Logical Up-Time                  25 min 59 sec
Current Physical Up-Time                 –
Current Physical Down-Time               1 min 30 sec
Current B Channels Used                  0
Current Charge Units Count               0
Current Inactivity Timeout Value (sec)   739
Current Disconnect Timeout Value (sec)   0
Current Incoming Calls                   5
Current Outgoing Calls                   5

Current Connection Established Over ISDN Interface AVM-B1-1_1
```

Table 18-3:
Information provided in "ISDN Connection Information for ..."

Information	Description
Current Logical Up-Time	indicates the time during which the current logical connection has been logically active since it has been set up for the first time.
Current Physical Up-Time	indicates the time during which the current ISDN connection has been physically active during the specified period (1h or 24h).
Current Physical Down-Time	indicates the time during which the current ISDN connection has been physically inactive during the specified period (1h or 24h).
Current B Channels Used	is the total number of B channels currently used for the current connection (0=no B channel active, either because no connection is active over this interface or the Inactivity Timeout expired).
Current Charge Units Count	is the approximate number of charge units for the current connection which have accrued during the specified period (1h or 24h). If no values are shown here, refer to the note on p. 225.

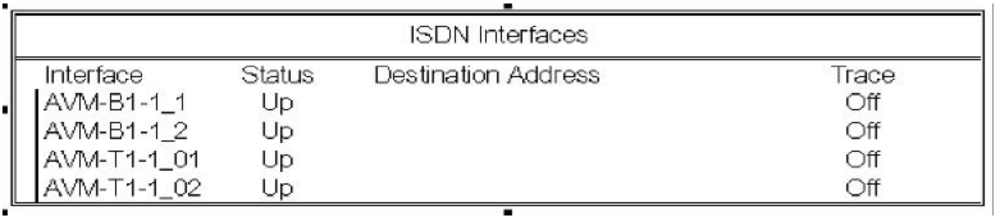
Current Inactivity Timeout Value (sec)	shows the Inactivity Timeout value (in seconds) configured in the ISDN Call Destination Configuration for the current connection. If Self-Learning Timeout is enabled, the adjusted Timeout value is displayed here.
Current Disconnect Timeout Value (sec)	is the Disconnect Timeout value (in seconds) that has been configured in the ISDN Call Destination Configuration for the current connection. If Self-Learning Timeout is enabled, the adjusted Timeout value is displayed here.
Current Incoming Calls	indicates the number of incoming calls during the specified period (1h or 24h).
Current Outgoing Calls	indicates the number of outgoing calls during the specified period (1h or 24h).

The detailed status and statistical information within the menu "Interfaces" is ISDN-Controller- and interface-oriented. Most information is also accessible via SNMP and is defined in the MPR4ISDN.MIB.

"Interfaces": ISDN-Controller and Interface-Oriented Information

When you select "Interfaces", the following menu appears on your screen:

Figure 18-4:
ISDN Interfaces



ISDN Interfaces

Interface	Status	Destination Address	Trace
AVM-B1-1_1	Up		Off
AVM-B1-1_2	Up		Off
AVM-T1-1_01	Up		Off
AVM-T1-1_02	Up		Off

Table 18-4:
Information in ISDN Interfaces

Information	Description
Interface	The name of the interface in the form of BoardName_n, where n is the interface number.

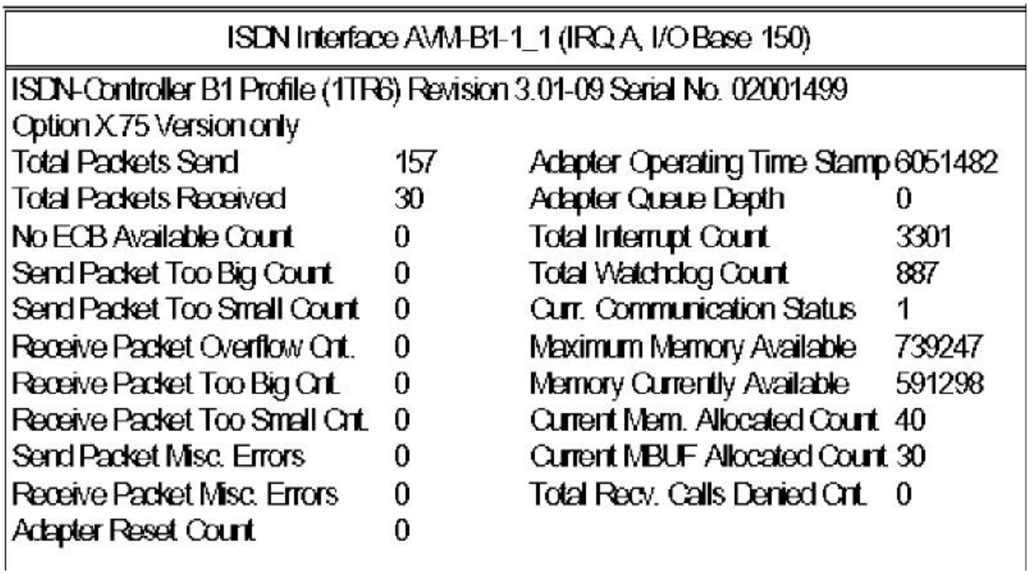
Status Status of the network interface. (Down=interface disabled; Up=interface enabled; Up 1 B Channel=physically active connection using 1 B channel; Up 2 B Channels=physically active connection using 2 B channels; Up Connected=physical connection down after Inactivity Timeout).

Destination Address If a connection to a remote site exists, its ISDN Number is displayed here.

Trace Status of the trace option (Off=Trace enabled. On=Trace disabled.) Press <Tab> to enable Trace, <Esc> or <Tab> again to disable Trace. Trace options can be defined in the "Options" menu (see p. 258).

Select the interface you want to have more information on from this list of available ISDN interfaces by pressing the Up and Down arrow keys, then press <Enter>. The following menu appears on the screen:

Figure 18-5:
Interface Information:...



```
                 ISDN Interface AVM-B1-1_1 (IRQ A, I/O Base 150)

ISDN-Controller B1 Profile (1TR6) Revision 3.01-09 Serial No. 02001499
Option X.75 Version only
Total Packets Send              157     Adapter Operating Time Stamp 6051482
Total Packets Received          30      Adapter Queue Depth          0
No ECB Available Count          0       Total Interrupt Count        3301
Send Packet Too Big Count       0       Total Watchdog Count         887
Send Packet Too Small Count     0       Curr. Communication Status   1
Receive Packet Overflow Cnt.    0       Maximum Memory Available     739247
Receive Packet Too Big Cnt.     0       Memory Currently Available   591298
Receive Packet Too Small Cnt.   0       Current Mem. Allocated Count 40
Send Packet Misc. Errors        0       Current MBUF Allocated Count 30
Receive Packet Misc. Errors     0       Total Recv. Calls Denied Cnt. 0
Adapter Reset Count             0
```

Press <PgDn> to view the next screens containing further details on the ISDN connection.

The ISDN statistics and status information provided by the NetWare MultiProtocol Router for ISDN via the ISDN Console menu "Interfaces" are divided into information related to the ISDN-Controllers, connection statistics and packets / bytes statistics, and will be described in the following table.

Table 18-5: Information in ISDN Interface Information...

Information	Description
Total Packets Sent	is the total number of frames sent on this interface since it has been loaded. This count includes LCP, NCP, network protocol data frames and call set-up frames for each active network protocol.
Total Packets Received	is the total number of frames received on this interface since it has been loaded. This count includes LCP, NCP, network protocol data frames, and call setup frames for each active network protocol.
No ECB Available Count	is the total number of times a receive ECB allocation failed for this interface since it has been loaded. Each occurrence of this error results in a receive frame being dropped. When this value increases rapidly, it is recommended to set the "maximum packet receive buffers" in the AUTOEXEC.NCF file to a higher value.
Send Packet Too Big Count	is the total number of times a transmit frame request failed on this interface since it has been loaded because the data size exceeded the Maximum Transfer Unit (MTU) size previously negotiated by the Protocol LCP. The default MTU value for the ISDN driver is 4530 bytes.
Send Packet Too Small Count	is the total number of times a transmit frame was too small and was padded for transmission.
Receive Packet Overflow Cnt.	is the total number of packets dropped because a receive ECB allocation failed for this interface since it has been loaded. When this value increases rapidly, it is recommended to set the "maximum packet receive buffers" in the AUTOEXEC.NCF file to a higher value.
Receive Packet Too Big Cnt.	is the total number of times a receive frame was discarded on this interface since it has been loaded because it exceeded the Maximum Transfer Unit (MTU) size previously negotiated.
Receive Packet Too Small Cnt.	is the total number of times a receive frame was discarded on this interface since it has been loaded because the frame was not large enough to contain a minimum ISDN frame format.
Send Packet Misc. Errors	is the total number of times the Queue Limit was exceeded or packets were sent for a destination that is no longer active. Set the Queue Limit to a higher value (see "ISDN-Controller Expert Interface Configuration").

Receive Packet Misc. Errors is the total number of all receive frame errors on this interface since it has been loaded. Note that this count can exceed the number of receive frames discarded because multiple errors can occur within a single receive frame.

Adapter Reset Count is the total number of times the ISDN-Controller was reset due to internal failure since this interface was loaded.

Adapter Operating Time Stamp is the time stamp indicating the last time the operational status of the ISDN-Controller changed (e.g. the interface was loaded or the ISDN-Controller was reset).

Adapter Queue Depth is the number of Transmit Packets that are queued at a given time for all interfaces of this ISDN-Controller.

Total Interrupt Count is the total number of interrupts generated by the ISDN-Controller since this ISDN interface was loaded.

Total Watchdog Count is the total number of watchdog packets generated by the ISDN-Controller since this ISDN interface was loaded. A watchdog packet is generated every 10 seconds.

Curr. Communication Status is a bit-mask that displays the communication status. When value 1000 is shown, a packet is being transmitted to the ISDN-Controller. When value 1 is shown, the ISDN-Controller is waiting for a packet. When value 1001 is displayed a packet is being transmitted to the ISDN-Controller and the driver is waiting for a packet.

Maximum Memory Available is the total number of memory in bytes implemented on the ISDN-Controller.

Memory Currently Available is the current number of bytes that are currently not in use on the ISDN-Controller.

Current Mem. Allocated Count is the number of Memory Blocks allocated on the ISDN-Controller.

Current MBUF Allocated Count is the number of Receive/Transmit Control Blocks allocated on the ISDN-Controller.

Total Recv. Calls Denied Cnt. is the total number of incoming calls on this ISDN-Controller denied access to the router.

Interface Status shows the current status of the interface. Up means that the interface is currently activated. Down means that the interface is disabled either because the ISDN Connection Monitor barred it, Time Restrictions do not allow usage at this time or it was barred via any SNMP based application.

Outbound Call Processing shows the current setting for Outbound Call Processing on this ISDN interface.

Inbound Call Processing shows the current setting for Inbound Call Processing on this ISDN interface.

Origination Address shows the complete address of this ISDN interface. The Origination Address is made up of the ISDN Number, the PBX Extension and the Subaddress.

Call Acceptance indicates the Call Acceptance status configured in the "Expert Configuration" for this interface.

Interface Usage the usage of the interface as configured in the "Expert Configuration". "LAN-LAN" means that no connections to remote NetWAYS/ISDN and PPP-compatible nodes are allowed over this interface. "Remote Node-LAN" means that this interface can only be used for connections to remote NetWAYS/ISDN and PPP-compatible nodes. "Both" allows both types of connections over this interface.

Total Queue Limit Count shows the value of the "Queue Limit" parameter that has been configured for this interface in the ISDN Expert Port Configuration since this ISDN interface was loaded (the default for this Queue Limit is 100).

Queue Depth Count is the number of Transmit Packets that are queued on the ISDN-Controller at a given time for this interface.

Total Send Packets Dropped Count is the total number of packets to be sent that were dropped because the maximum Queue Limit was exceeded since this ISDN interface was loaded.

Total Receive Packets Dropped Count is the total number of packets to be received that were dropped because of ECB allocation errors since this ISDN interface was loaded.

Total Send Calls Failed Count is the total number of calls and call retries (see parameter "Number of Retries" configured for each interface in the "ISDN-Controller Expert Interface Configuration") without subsequent successful establishment of a connection since this ISDN interface was loaded. Note that this number is a subset of Total Outgoing Calls.

Total Physical Connection Time Count is the total amount of time in seconds during which the interface has been physically in use since the ISDN interface was loaded. Note that at any given time either the Total Physical Connection Time Count or the Total Inactivity Time Count increases, depending on whether this ISDN line is physically in use or not.

Total Inactivity Time Count is the total amount of time the interface has been physically disconnected since the ISDN interface was loaded. Note that at any given time either the Total Physical Connection Time Count or the Total Inactivity Time Count increases, depending on whether this ISDN line is physically in use or not.

Physical Up-Time Threshold shows the Maximum Physical Connection Time threshold as configured in the ISDN-Controller Expert Interface Configuration. As soon as this threshold is reached, the interface of the ISDN-Controller is barred.

Actual Physical Up-Time shows the actual physical connection time of the interface.

Outgoing Calls Threshold shows the Maximum Outgoing Calls threshold as configured in the ISDN-Controller Expert Interface Configuration.

Actual Outgoing Calls shows the actual outgoing calls over the interface.

Charging Threshold shows the Maximum Charging threshold as configured in the ISDN-Controller Expert Interface Configuration.

Actual Charging shows the actual charge units accrued for connections over the interface.

Current Active is the name of the remote LAN that is connected to this interface.

ISDN Number is the ISDN Number of the remote site that is connected to this interface.

Remote Client Node Address is the MAC Address used by the remote node.

Remote Client IP Address is the IP Node Address used by the remote node.

Current Charge Units Count is the approximate number of charge units for a specific ISDN link over this interface (see "Current Active Call Destination"). If no values are shown here, refer to the note following this table.

Current Inactivity Timeout Value (sec) shows the Inactivity Timeout value (in seconds) configured in the ISDN Call Destination Configuration assigned for this connection. When Self-Learning Timeout is enabled, the adjusted Inactivity Timeout value is displayed in this place.

Current Disconnect Timeout Value (sec) is the Disconnect Timeout value (in seconds) that has been configured in the ISDN Call Destination Configuration for this connection. When Self-Learning Timeout is enabled, the adjusted Timeout value is displayed in this place.

Current Running Idle Timer (sec) indicates the time the current connection has been inactive so far.

Current B-Channels Used is the total number of B channels currently used for the connection indicated in the field "Current Active Connection" (0=no B channel active, either because no connection is active over this interface or the Inactivity Timeout expired).

Curent Packets Queued is the number of packets currently queued for this interface.

Current Logical Connection Time Count indicates, how long (in seconds) the current connection already exists logically since it has been set up for the first time.

Current Physical Connection Time Count indicates the time (in seconds) a connection is physically active between two periods of physical inactivity for the current logical connection.

Current Inactivity Time Count indicates the time (in seconds) a connection is physically inactive between two periods of physical activity for the current logical connection.

Current Filtered Packets is the total number of packets filtered on that interface.

Current Spoofed Packets is the total number of packets spoofed on that interface.

Current Dropped Packets is the total number of packets dropped on that interface because the Queue Limit was exceeded.

Compression shows the compression type negotiated with the remote site during initial call set-up.

Spoofing shows the spoofing mechanisms negotiated with the remote site during initial call set-up.

Bundling shows whether or not channel bundling was negotiated with the remote site during initial call set-up. Disabled:no channel bundling negotiated; Enabled: channel bundling negotiated.

Internal Diagnostic 1-4 These statistics represent ISDN internal statistics counts per ISDN-Controller. They are intended for use by technical support, and should be included when reporting problems.

PPP Send MRU, MRRU
PPP Receive MRU, MRRU is the negotiated Maximum Receive Unit (MRU) and Maximum Receive Reconstruct Unit (MRRU) for incoming/outgoing calls. The MRRU is a sign that PPP Multilink is used.

PPP Send Options
PPP Receive Options

shows the negotiated option for incoming/outgoing calls:
ACFC- address and control field compression enabled.
PFC - protocol and control field compression enabled.
MAGIC - magic number transmitted for the loopback detector.
PAP - password authentication protocol used.
CHAP - challenge handshake authentication protocol used.
CIPX - CIPX header compression enabled.
CIP - TCP/IP header compression enabled.
IPA - the remote site was assigned an IP address from the IP Address Range.
EPD - End-of-point descriptor used.
SSN - Short sequence number used.
AUT - authentication was performed.

Compression Send Reset Count

specifies how often the compression encoder has been reset. High values indicate that the data to be transmitted could not be compressed very well.

Compression Receive Reset Count

specifies how often the compression decoder has been reset. High values indicate that the data transmitted could not be compressed very well.

Compression Receive Error Count 1-2

specifies how often bad frames have been received.

Accounting Statistics:

Duration

is the total period during which the ISDN interface has been loaded so far for the period stated (1 day, 7 days, 4 weeks).

Physical Up-Time

shows the physical up-time of the interface during the period stated (1 day, 7 days, 4 weeks). Note that here, all B channel up-times are added and therefore the total physical up-time per day may exceed 24 h!

Incoming Calls

shows the incoming calls at the interface during the period stated (1 day, 7 days, 4 weeks).

Outgoing Calls

shows the outgoing calls at the interface during the period stated (1 day, 7 days, 4 weeks).

Chargings

shows the charge units accrued at the interface during the period stated (1 day, 7 days, 4 weeks).

Throughput rates for transmitted and received data:

Actual Data Rate (Bits/sec)

is the actual data throughput rate per second over this interface.

Net Data Rate (Bits/sec) is the net usage of the ISDN channel related to this interface.

Packet Rate (Packets/sec) is the number of packets transferred per second over this interface.

Compression Factor is the percentage to which the data could be compressed. A value of 30 indicates that the data packets could be compressed to 30 % of their original size.

Packets/Bytes Statistics:

Packets Sent is the total number of packets sent on this interface per protocol.

Packets Received is the total number of packets received on this interface per protocol.

Bytes Sent is the total number of bytes sent on this interface per protocol.

Bytes Received is the total number of bytes received on this interface per protocol.

Active Protocols lists the protocols that are currently active on this ISDN interface.

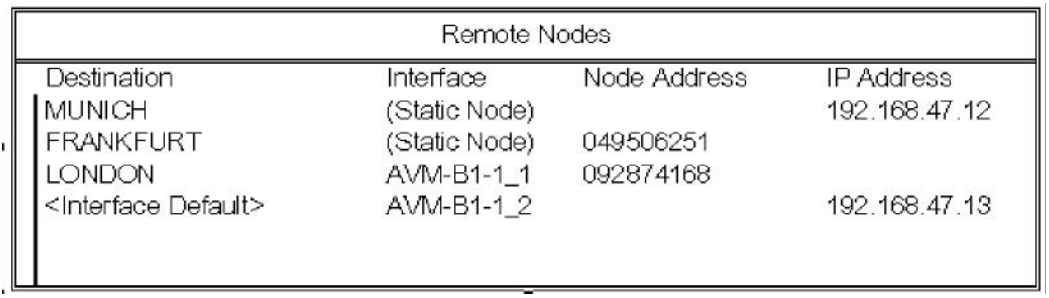
Note

If no values are shown for "Total Charge Units Count" and "Current Charge Units Count", please note that values in these parameters directly depend on the type of information delivered by the ISDN network and on how this is done; i.e. what kind of information services the PTTs provide.
Within the ETSI standards for Euro-ISDN, the NetWare MultiProtocol Router for ISDN and the corresponding ISDN-Controllers support the "Advice On Charge During Call" (AOCD) of the "Functional Interface" specification. If this service is provided by a national PTT for an Euro-ISDN interface, charging information will be provided within the ISDN statistics of the NetWare MultiProtocol Router for ISDN in the form of Charge Units. In Germany, this service is provided. If no values are shown for the two parameters, ask your local telecommunications agency whether this option is available and enabled for your ISDN access.

"Remote Nodes": Remote Node-Oriented Information

The "Remote Node" menu displays status information on all ISDN connections logically established to remote nodes at a given time. When you select "Remote Node", the following menu appears on your screen:

Figure 18-6:
Remote Nodes



Remote Nodes

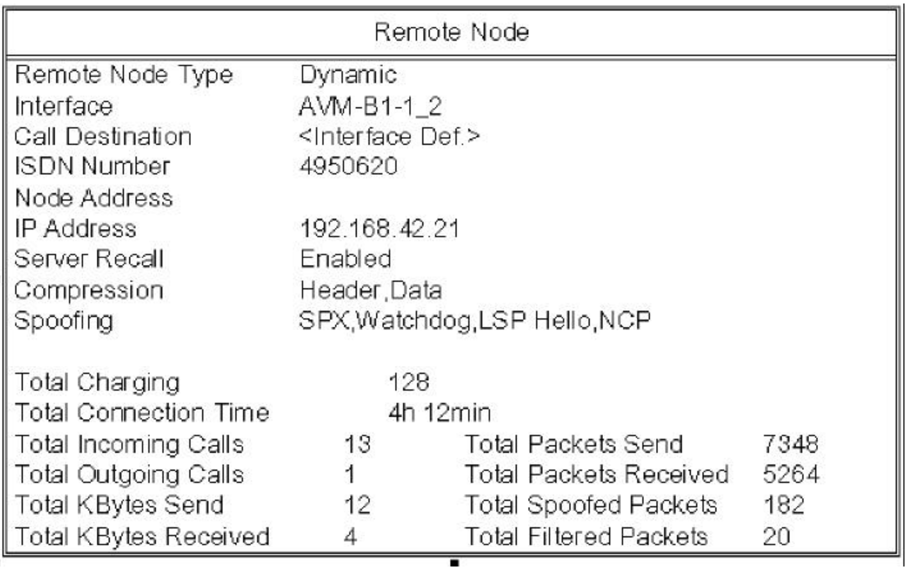
Destination	Interface	Node Address	IP Address
MUNICH	(Static Node)		192.168.47.12
FRANKFURT	(Static Node)	049506251	
LONDON	AVM-B1-1_1	092874168	
<Interface Default>	AVM-B1-1_2		192.168.47.13

Table 18-6:
Information in Remote Nodes

Information	Description
Destination	The call destination name of the remote node.
Interface	(Static Node) means that the remote node was configured to be a static remote node. If a connection exists to a remote node, the interface that handles the connection is displayed.
Node Address	The Node Address of the remote node.
IP Address	The IP Address of the remote node.

Select the remote node you want to have more information on from this list by pressing the Up and Down arrow keys, then press <Enter>. The "Remote Node" menu appears on the screen:

Figure 18-7:
Information in Remote Node



```
                              Remote Node
Remote Node Type        Dynamic
Interface               AVM-B1-1_2
Call Destination        <Interface Def.>
ISDN Number             4950620
Node Address
IP Address              192.168.42.21
Server Recall           Enabled
Compression             Header,Data
Spoofing                SPX,Watchdog,LSP Hello,NCP

Total Charging                128
Total Connection Time         4h 12min
Total Incoming Calls      13        Total Packets Send        7348
Total Outgoing Calls      1         Total Packets Received    5264
Total KBytes Send         12        Total Spoofed Packets     182
Total KBytes Received     4         Total Filtered Packets    20
```

Table 18-7:
Information in Remote Node

Information	Description
Remote Node Type	The type of remote node. Static means that the remote node was configured to be a static remote node. Dynamic means that this is no static remote node.
Interface	The name of the interface in the form of Board Name_n, where n is the interface number.
Call Destination	The call destination name of the remote node.
ISDN Number	The ISDN Number of the remote node.
Node Address	is the MAC Address used by the remote node.
IP Address	is the IP Node Address used by the remote node.
Server Recall	Displays whether Server Recall was negotiated. Enabled: Server Recall negotiated; Disabled: no Server Recall negotiated.

Compression shows the compression type negotiated with the remote site during initial call set-up.

Spoofing shows the spoofing mechanisms negotiated with the remote site during initial call set-up.

Total Charging is the approximate number of charge units that have accrued on the router for the current remote node.

Total Connection Time is the total time during which connections to this remote node have been physically up.

Total Incoming Calls indicates the total number of incoming calls from this remote node.

Total Outgoing Calls indicates the total number of outgoing calls to this remote node.

Total Kbytes Sent is the total number of bytes sent to this remote node.

Total Kbytes Received is the total number of bytes received from this remote node.

Total Packets Sent is the total number of frames sent to this remote node. This ‘count includes LCP, NCP, network protocol data frames and call set-up frames for each active network protocol.

Total Packets Received is the total number of frames received from this remote node. This ‘count includes LCP, NCP, network protocol data frames and call set-up frames for each active network protocol.

Total Spoofed Packets is the total number of packets spoofed.

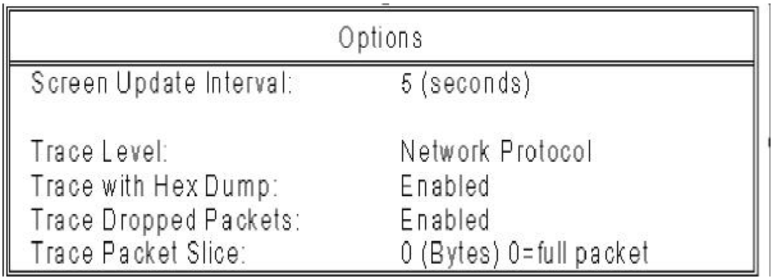
Total Filtered Packets is the total number of packets filtered.

"Options": Enabling Traces

The "Options" menu provides parameters to configure the screen update interval, to enable ISDN line management logging and to specify trace options.

Press <Enter> on "Options" to display the following menu:

Figure 18-8:
ISDN Console, Options menu



```
                         Options
Screen Update Interval:         5 (seconds)

Trace Level:                    Network Protocol
Trace with Hex Dump:            Enabled
Trace Dropped Packets:          Enabled
Trace Packet Slice:             0 (Bytes) 0=full packet
```

Table 18-8:
Configurable Parameters in the "Options" Menu

Parameter	Description
Screen Update Interval	specifies how often ISDN Console screens are updated.
Trace Level	lets you define the level of the trace. Network Protocol: all IPX, IP, AT, etc. protocols are traced. ISDN D channel: traces ISDN D channel information. PPP Protocol: traces information related to the PPP protocol.
Trace with Hex Dump	lets you enable Trace with Hex Dump.
Trace Dropped Packets	lets you exclude dropped packets from packet trace. Disabled: dropped packets are not traced. Enabled: dropped packets are traced.
Trace Packet Slice	lets you specify the slice of the packet to be traced. If you want to trace the packet headers only, specify 64 Bytes. 0 Bytes traces full packets. The header sizes for the single protocols are as follows: IPX: 30 Bytes IP: 20 Bytes SPX: 42 Bytes UDP/IP: 28 Bytes NCP: 36 Bytes TCP/IP: 40 Bytes SPX II: 44 Bytes ARP/RARP: 28 Bytes

"View File": Viewing Log Files and Trace Files

Selecting this item displays a list of ISDN Log and Trace Files. The ISDN log files of the current day are marked with an asterisk (*). Select the file you want to view from the list and press <Enter>.

Use the cursor keys and the <PgDn> and <PgUp> keys to scroll through the files.

Use the <Del> key to delete the highlighted file.

Log, accounting and trace files can also be viewed with the help of the ISDNVIEW.NLM. Specify the respective file you want to view when loading ISDNVIEW.NLM:

```
load ISDNVIEW isdn01.log <RETURN>
```

Limiting ISDN Connections

Normally, the network administrator should monitor ISDN connections daily, using ISDN Console (see above) or an SNMP-based management console such as AVM´s MPR for ISDN Router Manager, to detect aberrant situations and to avoid unnecessary connection charges by immediately sorting out the cause for such situations.

For situations where daily monitoring is not possible for whatever reason, the NetWare MultiProtocol Router for ISDN 3.1 provides two useful mechanisms to limit connection charges: the ISDN Connection Monitor, which was already introduced with version 3.0, and the new ISDN Budget Manager.

ISDN Budget Manager

The ISDN Budget Manager allows configuration of the maximum amount of money or the maximum number of charge units you want to spend for a call destination per month, week and day.

When one of the maximum values is reached, the connection to the remote site is cleared and incoming and outgoing connections to this call destination are no longer allowed. To allow connections again, either set the expired budget value to (None) or configure a higher value. The current values are not reset when one of the maximum values is reached!

For information on how to configure the Budget, refer to Chapter 7, "Configuring ISDN Call Destinations".

ISDN Connection Monitor

The ISDN Connection Monitor is activated automatically whenever the router is started. It provides default values, but also allows you to configure threshold values for the maximum physical up-time, the maximum outgoing calls and the maximum charge units allowed on each interface of an ISDN-Controller.

The default values are as follows:

Maximum Physical Up-Time:	40 min
Maximum Outgoing Calls:	200
Maximum Charge Units:	200

They were calculated according to the new tariffs of Deutsche Telekom AG (as of January 1996):

Maximum amount of money allowed on each interface per day:	DM 24
Meter clock pulse Fernzone/Region 20 between 9 a.m. and 12 a.m.:	appr. 12 sec
One charge unit costs:	DM 0.12

--> Maximum Charge Units = DM 24 : DM 0.12 = 200

--> Maximum Physical Up-Time = (DM 24 : DM 0.12) x 12 sec = 2400 sec = 40 min

As soon as the threshold value for an interface is reached, an alert is generated 3 times in 1-minute intervals, printed on the system console and sent via Trap. After that, the respective interface is automatically barred; i.e., all connections set up over this interface are cleared, no outgoing calls can be established over it and incoming calls on the ISDN-Controller are rejected if addressed to this interface until the administrator removes this bar. If the barred interface is a member of an Interface Group, all other interfaces of this group are barred as well to avoid that outgoing calls are simply performed over a different interface.

To remove a bar, do one of the following:

- Load the ISDN Console (ISDNCON.NLM), go to *Interfaces* and press <Del> on the barred interface. The threshold value(s) will be reset and the interface released.

OR

- Reconfigure threshold values in the Expert Configuration of the barred interface and enter "reinitialize system" at the system console prompt to bring changes into effect.

Barring interfaces is or course a very drastic measure. Since all WAN connections over such an interface are cut off and users cannot access distant networks any more, problems with routine processes and existing sessions could arise. Therefore, this should be the last measure you take, and the threshold values should be as high as your situation allows.

Important

If you want to use the ISDN Connection Monitor, you should make sure that it is used on all servers/routers in a WAN. If, for example, an interface of an ISDN-Controller in a router is barred after a timeout expired, an incoming call will be switched through to the ISDN-Controller by the local exchange and will only be rejected by the barred interface itself.
Thus, if a remote router is configured to set up ISDN calls automatically, it will perform endless attempts to set up a call to such a barred interface, which will result in a high number of charge units within a very short time!

NDS over ISDN Console - Monitoring NDS Traffic

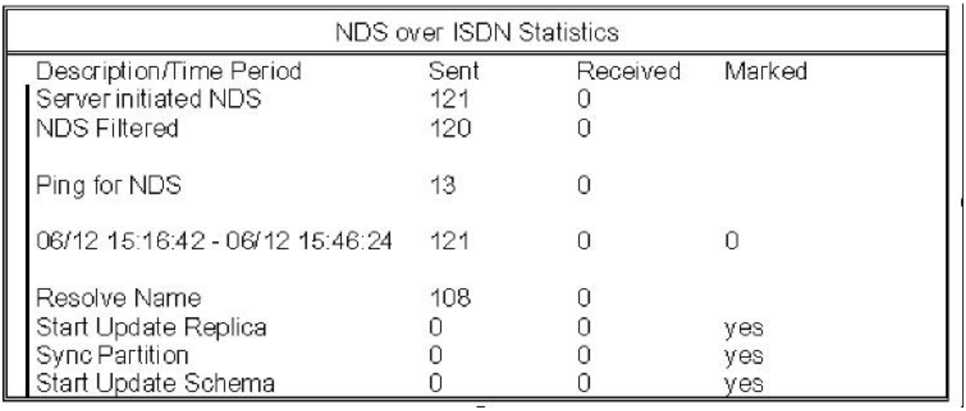
The NDS over ISDN Console monitors NDS traffic on ISDN lines. NDS traffic can be divided in client-to-server traffic and server-to-server traffic. Client-to-server traffic is caused when a client performs a login in the network or executes nwadmin. Server-to-server traffic is caused by NDS updates and time synchronization.

The NDS over ISDN Console is realized in the form of a NetWare Loadable Module™ (NLM™). To load the NDS over ISDN Console, enter the following command at the server console prompt:

```
load ndscon <Enter>
```

The following screen appears:

Figure 18-9:
NDS over ISDN Console



NDS over ISDN Statistics

Description/Time Period	Sent	Received	Marked
Server initiated NDS	121	0	
NDS Filtered	120	0	
Ping for NDS	13	0	
06/12 15:16:42 - 06/12 15:46:24	121	0	0
Resolve Name	108	0	
Start Update Replica	0	0	yes
Sync Partition	0	0	yes
Start Update Schema	0	0	yes

The NDS over ISDN Console contains the following information:

The upper part displays the number NDS packets initiated by clients and servers, the number of Time Synchronization packets, the number of NDS packets spoofed and filtered and the number of Time Synchronization packets filtered by the NetWare MultiProtocol Router for ISDN:

Server initiated NDS - number of NDS packets sent/received by a server.

Client initiated NDS - number of NDS packets sent/received by a client.

Exchange Time - number of Time Synchronization packets sent/received by a server.

NDS Spoofed - number of NDS packets spoofed.

NDS Filtered - number of NDS packets filtered.

Time Exchange Filtered - number of Time Synchronization packets filtered.

Ping for NDS - number of Ping for NDS packets sent/received.

The middle part shows the amount of NDS traffic during the specified period.

The lower part lists the NDS traffic according to the NDS process that initiates it.

appendix A *System and Error Messages*

ISDN Error Messages

Error Causes Sent by the Local Exchange

0x3401 **Invalid call reference [#3401]. Unexpected protocol element processing on the D or B channel. Check if the correct D Channel protocol for your line is used.**

0x3403 **Bearer service not implemented [#3403]. The service is not accepted by your local exchange. The service indicator has not been set to the correct value or is not subscribed at the remote site.**

0x3407 **Call identity does not exist [#3407]. Unexpected protocol element processing on the D or B channel. Check if the correct D Channel protocol for your line is used.**

0x3408 **Call identity in use [#3408]. Unexpected protocol processing on the D or B channel. Check if the correct D Channel Protocol for your line is used.**

0x340A **No channel available [#340A]. All channels of your ISDN access are occupied by other users.**

0x340F **Call clearing [#340F]. Your call was disconnected by the remote site.**

0x3410 **Requested facility not implemented [#3410]. The facility requested is currently not implemented in ISDN.**

0x3411 **Requested facility not subscribed [#3411]. The facility requested is currently not implemented in ISDN.**

0x3420 **Outgoing calls barred [#3420]. Your ISDN access is barred for outgoing calls.**

0x3421 **User access busy [#3421]. The local exchange is congested. The accesses are busy.**

0x3422 **Negative CUG comparison [#3422]. Connection is not possible because of non-membership in a closed user group.**

0x3423 **Non-existent CUG [#3423]. The specified closed user group does not exist.**

0x3425 **Semi-permanent connection not possible [#3425]. The facility requested is currently not available in ISDN.**

0x3429 **Temporary failure [#3429]. Temporary failure in ISDN.**

0x3430 **Reverse charging not allowed (ORG) [#3430]. Reverse charging is not possible from this access.**

0x3432 **Reverse charging rejected [#3432]. Reverse charging was rejected by the remote site.**

0x3435 **Destination not obtainable [#3435]. Connection cannot be established because of incorrect number, service or service indicator.**

0x3438 **Number changed [#3438]. The number entered is no longer correct.**

0x3439 **Remote user not ready [#3439]. The TE at the remote site is not ready for use.**

0x343A **No user responding [#343A]. The remote site has not confirmed the incoming call or the call set-up was aborted.**

0x343B **User busy [#343B]. The remote access is busy.**

0x343D **Incoming calls barred [#343D]. The user called is barred for incoming calls or the requested service is not subscribed at the remote site.**

0x343E **Call rejected [#343E]. The call was rejected by the remote site.**

0x3458 **Incompatible destination [#3458]. The dialed number does not comply with international conventions.**

0x3459 **Network congestion [#3459]. Congestion in ISDN. Try again.**

0x345A **Remote user initiated [#345A]. Rejected or initiated by the remote user or the local exchange.**

0x3460 **Mandatory information elements missing [#3460]. The dialed number does not comply with international conventions.**

0x3464 **Invalid information element contents [#3464]. The dialed number does not comply with international conventions.**

0x3470 **Local procedure error [#3470]. Caused by a local error, e.g. a timeout.**

0x3471 **Remote procedure error [#3471]. Caused by an error at the remote site.**

0x3472 **Remote user suspended [#3472]. Initiated or rejected by the remote user.**

0x3473 **Remote user ready again [#3473]. At the remote site, the connection is no longer in the state of "holding", "suspend" or "conference".**

0x347F **D channel user info not implemented [#347F]. Protocol error during call set-up or clear-down between controller and ISDN.**

0x34xx **Unknown ISDN error message [#34xx]. The local exchange sent an unknown error message. Please contact AVM technical support.**

Error Messages Created by the ISDN-Controller

0x3202 **The configured EAZ/MSN is already used by another application [#3202].**

Configure a different EAZ or MSN for the specified interface of the NetWare MultiProtocol Router for ISDN.

0x8001 **The configured MSN cannot be used [#8001].**

The configured MSN cannot be adjusted in the controller software. Use a different MSN.

0x3301 **No connection to ISDN [#3301].**

A connection could not be established from the terminal equipment to the NT (Network Terminator) and / or the local switching station. The call set-up failed at Layer 1 of the ISDN protocol: the necessary physical signals could not be exchanged between the terminal equipment and the NT / local switching station. Possible causes include:

- cable not connected or incorrectly connected
- cable connectors miswired or wrong sockets used
- NT is not correctly activated or has a faulty connection to the switching station
- a defective TE elsewhere on the bus is blocking communication.

0x3302 **No connection to ISDN [#3302].**

A connection could not be established from the terminal equipment to the NT and / or the switching station. The call set-up failed at Layer 2 of the ISDN protocol: no messages could be exchanged between the terminal equipment and the switching station. Possible causes include:

- the access to the switching station is not activated
- an incorrect or unexpected D channel protocol is being used at this access.

0x3303 **Error during call set-up to ISDN user [#3303].**

A data connection could not be established from the terminal equipment to the remote station called. The call set-up failed on attempting to establish the data communication channel (B channel). Possible causes include:

- the B channel requested was not switched through by the switching station
- the necessary signals (flags) for call set-up were not present.

0x3304

Error during call set-up to ISDN user [#3304].

A data connection could not be established from the terminal equipment to the remote station called. The call set-up failed on attempting to establish the data communication channel (B channel). Possible causes include:

- the B channel requested was not switched through by the switching station
- the necessary signals (flags) for call set-up were not present.

0x3305

Connection to ISDN aborted (D channel) [#3305].

An existing connection to the NT / switching station was terminated. Possible causes include:

- an unstable ISDN connection to the NT, possibly caused by:
- excessive cable length
- incorrect cable routing
- faulty wiring connections.

0x3306

Connection to ISDN aborted (D channel) [#3306].

An existing connection or a call set-up in progress to the NT / switching station was terminated. Possible causes include:

- an unstable ISDN connection to the NT, possibly caused by:
- excessive cable length
- incorrect cable routing
- faulty wiring connections
- user termination of call set-up
- malfunction of the NT / switching station.

0x3307

Connection to ISDN aborted (D channel) [#3307].

An existing connection or a call set-up in progress to the NT / switching station was terminated. Possible causes include:

- termination of call set-up by the user
- malfunction of the NT / switching station
- error in the Layer 2 protocol.

0x3308

Connection to ISDN aborted (B channel) [#3308].

An existing connection to the remote station was terminated. Possible causes include:

- an unstable ISDN connection to the NT, possibly caused by:
- excessive cable length
- incorrect cable routing
- faulty wiring connections.

0x3309

Connection to ISDN aborted (B channel) [#3309].

An existing connection or a call set-up in progress to the remote station was terminated. Possible causes include:

- termination of call set-up by the user
- the remote TE called does not conform to the protocol or service definition.

0x330A

Connection to ISDN aborted (B channel) [#330A].

An existing connection or a call set-up in progress to the remote station was terminated. Possible causes include:

- user termination of call set-up
- the remote TE called does not conform to the protocol or service definition
- the remote TE called uses an incompatible Layer 3 protocol.

0x330B

Connection to ISDN aborted (B channel) [#330B].

An existing connection or a call set-up in progress was aborted and had to be re-established. Data loss may have occurred. Possible causes include:

- the remote TE called does not conform to the protocol or service definition
- an interrupted connection is being resumed (not currently implemented).

0x330C **Re-establish connection, B channel layer 3 [#330C].**

An existing connection or a call set-up in progress was aborted and had to be re-established. Data loss may have occurred. Possible causes include:

- the remote TE called does not conform to the protocol or service definition
- an interrupted connection is being resumed (not currently implemented).

ISDN Line Management Messages

Messages Indicating Actions or Status Changes

All the following messages are displayed as follows:

```
<Date> <Time> <Board Name_Interface Number>:
<Message>
```

Example:

95/06/10 13:29:50 AVM-B1_1: Connection to 03046707219 subaddress 1 established (outgoing).

Incoming call from <Number>.

indicates that a call is coming in from the specified ISDN number.

Create connection to <Number>.

indicates that a connection to the specified ISDN number is initiated.

Connection to <Number> established (incoming).

indicates that an incoming call request has been accepted and a physical ISDN connection has been established to the specified ISDN number.

Connection to <Number> established (outgoing).

indicates that an outgoing call request has been accepted by the remote site and a physical connection has been established to the specified ISDN number.

B channel up-time to <Number>: x y.

displays statistics information on the currently inactive B channel, based on the duration and, for outgoing calls, the number of charge units accrued for this connection. If AOCD (Advice On Charge During Call) is not activated at the ISDN access, no charge units will be displayed for outgoing calls.

Connection to <Number> down.

indicates that a physical ISDN connection to the specified ISDN number has been disconnected. See also "ISDN Error Messages" in this Chapter.

Inactivity timeout expired.

indicates that the Inactivity Timeout configured for the current ISDN call destination elapsed and the ISDN connection was physically deactivated.

Disconnect timeout expired.

indicates that the Disconnect Timeout configured for the current ISDN call destination elapsed and the ISDN connection was cleared physically and logically.

Messages Indicating Why an Incoming/Outgoing Call Was Rejected

All the following messages are displayed as follows:

```
<Date> <Time> <Board Name_Interface Number>:
<Message>
```

ISDN-9: Physical up-time threshold reached.

Warning issued by the ISDN Connection Monitor indicating that the Physical Up-Time Threshold was reached.

ISDN-9: Outgoing calls threshold reached.

Warning issued by the ISDN Connection Monitor indicating that the Outgoing Calls Threshold was reached.

ISDN-9: Charging threshold reached.

Warning issued by the ISDN Connection Monitor indicating that the Charging Threshold was reached.

ISDN-10: Interface barred - physical up-time threshold reached.

indicates that the specified interface is barred because the maximum physical up-time threshold was exceeded. To enable the interface again, unload ISDNCMON and load it again.

ISDN-10: Interface barred - outgoing calls threshold reached.

indicates that the specified interface is barred because the maximum outgoing calls threshold was exceeded. To enable the interface again, unload ISDNCMON and load it again.

ISDN-10: Interface barred - charging threshold reached.

indicates that the specified interface is barred because the maximum charging threshold was exceeded. To enable the interface again, unload ISDNCMON and load it again.

ISDN-13: Incoming call from <Number> not acceptable - all B channels are busy.

indicates that an incoming call cannot be accepted because all B channels are already in use at your side at the specified time.

ISDN-16: Outgoing Call to <Number> failed - Interface barred for outgoing calls.

indicates that the interface cannot be used to perform outgoing calls, because Outbound Call Processing is disabled on the interface, the Interface Status is disabled or COSO is set to No Dial-Out for the call destination.

ISDN-17: Outgoing call to <Number> subaddress <x> failed - All B channels are busy.

indicates that an outgoing call to the specified number cannot be established because all B channels are already in use at your side.

ISDN-19: Outgoing call to <Number> subaddress <x> rejected because the local WAN call destination version must match.

indicates that the ISDN Call Destination Configuration for this call destination is incorrect. Check it or, if you are upgrading from NetWare MultiProtocol Router for ISDN v2.x or 3.0, load ISDNCONV.NLM to convert database entries to version 3.1.

ISDN-20: Outgoing call to <Number> subaddress <x> rejected because the local interface is still in use to <Number> subaddress <x>.

indicates that this interface is already used for a different ISDN connection. If both numbers displayed are equal, check the configuration of Local System ID and Remote System ID.

ISDN-21: Outgoing call to <Number> subaddress <x> rejected because the "Call Status" is set to "Disabled".

indicates that you set the Call Status parameter in the "ISDN Call Destination Configuration" to Disabled. Thus, outgoing calls to this call destination are not allowed over the interface. If you want to allow outgoing calls to this destination, you have to change the Call Status and set it to Enabled.

ISDN-22: Outgoing call to <Number> subaddress <x> rejected because "Outbound Call Processing" is set to "Disabled".

Since the interface cannot process outgoing calls, the call was rejected.

ISDN-23: Incoming call from <Number> subaddress <x> rejected because "Call Acceptance" is set to "Only Registered Numbers: CLI" or "...: CLI and Caller-Specified" and this number (CLI) is not or not properly configured to be accepted.

indicates that the CLI number delivered over the D channel by the remote site is not configured or not configured properly in the Call Acceptance Database.

ISDN-24: Call to <Number> subaddress <x> rejected because the PPP LCP negotiation failed.

indicates that the router was not able to negotiate the PPP LCP with a remote site and therefore the call was rejected.

ISDN-25: Starvation timeout expired.

indicates that the remote peer of a connection is not answering.

ISDN-26: Calculated self-learning timeout <Period>.

shows the calculated selflearning timeout when

- you set up a physical connection and the selflearning timeout has been calculated for the first time.

- the meter clock pulse changed and a new selflearning timeout has been calculated anew.

ISDN-27: Incoming call from <Number> subaddress <x> rejected because the "Call Status" is set to "Disabled".

indicates that the Call Status of this call destination is disabled and no outgoing and incoming calls are allowed to and from this remote site.

ISDN-28: Incoming call from <Number> rejected because the budget is reached.

indicates that one of the budget values configured for this call destination was reached and the call destination was barred for outgoing and incoming calls. Either set the budget value to (None) or enter a higher value.

ISDN-29: Outgoing call to <Number> subaddress <x> rejected because the budget is reached.

indicates that one of the budget values configured for this call destination was reached and the call destination was barred for outgoing and incoming calls. Either set the budget value to (None) or enter a higher value.

ISDN-30: Call to <Number> cleared because the budget is reached.

indicates that one of the budget values configured for this call destination was reached and the call was therefore cleared. No outgoing or incoming calls are allowed to or from this call destination. To use this destination again, either set the budget value to (None) or enter a higher value.

ISDN-31: COSO changed to "No Dial-Out".

indicates that COSO changed to No Dial-Out either because configured Time Restrictions came into effect or you set COSO to Remote and the remote site did not reject your call on the D channel. As a result, COSO changed to No Dial-Out.

ISDN-51: Outgoing call to <Number> subaddress <x> rejected because the local call number components are not configured properly.

indicates that either no ISDN number or, if a PBX is used, no PBX Extension has been configured. Enter the respective number in the ISDN-Controller Interface Configuration.

ISDN-52: Outgoing call to <Number> subaddress <x> rejected because the called subaddress <x> does not exist.

indicates that the Destination Subaddress you configured does not exist at the remote site. Ask the network administrator of the remote site which subaddress is assigned for your router to dial to and enter that subaddress in your ISDN Call Destination entry.

ISDN-53: Outgoing call to <Number> subaddress <x> rejected because the called subaddress <x> is configured for remote node access.

indicates that the interface you dialed at the remote router is configured for remote node access. When providing remote access for stand-alone PCs besides routing between LANs, the interface / interfaces configured for remote node access cannot be used concurrently to establish router connections. Ask the network administrator of the remote site which Destination Subaddress is to be configured in your ISDN Call Destination entry.

ISDN-54: Outgoing call to <Number> subaddress <x> rejected because the called subaddress <x> is busy.

indicates that the addressed logical interface of the ISDN-Controller on the remote site is in use, and therefore the call is rejected by the ISDN-Controller.

ISDN-55: Outgoing call to <Number> subaddress <x> rejected because the remote router did not set "Call Acceptance" to "All Numbers" and this number (Caller-Specified) is not registered to be accepted.

indicates that the outgoing call has not passed the security mechanism of the remote router. Ask the network administrator of the remote site for information on how to configure your ISDN Call Destination entry properly to get access, since he has assigned an interface for your router to dial to.

ISDN-56: Outgoing call to <Number> subaddress <x> rejected because the called address does not match the call number components at the remote site.

indicates that the number entered for Destination Address on your local router is not configured properly to reach the remote router.

ISDN-72: Outgoing call to <Number> subaddress <x> rejected because the interface is barred via "Time Restrictions".

indicates that the configured Interface Status time restrictions for this interface do not allow usage of the interface at that moment. The interface is barred for incoming as well as outgoing calls.

ISDN-73: Outgoing call to <Number> subaddress <x> rejected because the selected protocol is not configured at the remote site.

indicates that the selected network protocol is not configured at the remote site. Contact the remote network administrator for information on which network protocols are configured for WAN connections at the remote site.

ISDN-74: Call to <Number> subaddress <x> rejected because the PPP outbound authentication failed.

indicates that your router could not provide correct PPP outbound authentication so that the call was rejected.

ISDN-101: Incoming call from <Number> subaddress <x> rejected because of incorrect configured call number components at the remote site.

indicates that either no ISDN Number or, if a PBX is used, no PBX Extension are configured at the remote site. The incoming call is rejected, because your local router needs this information to properly calculate the number to call the remote router back.

ISDN-102: Incoming call from <Number> subaddress <x> rejected because the called subaddress <x> does not exist.

indicates that the subaddress entered for Destination Subaddress on the remote router to call your local router does not exist on your local router.

ISDN-103: Incoming call from <Number> subaddress <x> rejected because the called subaddress <x> is configured for remot node access.

When the Interface Usage is set to "Remote Node-LAN" to provide remote node acces from stand-alone PCs, the interface cannot be used at the same time to establish router connections. You can provide another interface for the remote site to dial to.

ISDN-104: Incoming call from <Number> subaddress <x> rejected because the called subaddress <x> is busy.

indicates that the addressed logical interface of the ISDN-Controller at your side is already in use, and therefore the call is rejected.

ISDN-105: Incoming call from <Number> subaddress <x> rejected because "Call Acceptance" is not set to "All Numbers" and this number is not or not properly configured as a destination to be accepted.

indicates that the incoming call has not passed the security mechanism of the router. If you want to allow this remote router access to your network, you have to create an entry in the Call Acceptance Database for that router. In doing so, you assign a specific interface of an ISDN-Controller for that router to get access to your LAN.

If you have already created such an Call Acceptance Database entry, make sure that the Destination Address and Subaddress entered there are configured properly to call that remote router. Further, make sure that the remote router's Destination Address and Subaddress in the ISDN Call Destination entry is configured properly to reach the interface you have assigned to this router.

ISDN-106: Incoming call from <Number> subaddress <x> rejected because the called address <Number> does not match the local call number components.

indicates that the number entered for Destination Address on the remote router is not configured properly to reach your local router. Your router therefore is not able to generate the correct number to call the remote router back, since it does not know where the incoming call came from (PBX or not, location, country, etc.).

ISDN-107: Incoming call from <Number> subaddress <x> rejected because the called subaddress <x> is not configured for remote node access.

indicates that a stand-alone PC tried to call an interface (a subaddress) that is not configured for remote node access.

You can configure that interface for remote node access as well as provide another interface for this remote PC to get access if you want to.

ISDN-120: Incoming call from <Number> subaddress <x> rejected because of lost logical connection or incorrect NetWAYS/ISDN driver at the remote site.

indicates that the Disconnect Timeout might have expired, that the remote client rebooted the system or an incorrect NetWAYS/ISDN driver is used at the remote site.

ISDN-122: Incoming call from <Number> subaddress <x> rejected because the interface is barred via "Time Restrictions".

indicates that the configured Interface Status time restrictions for this interface do not allow usage of the interface at that moment. The interface is barred for incoming as well as outgoing calls.

ISDN-123: Incoming call from <Number> subaddress <x> rejected because the requested protocol is not configured to be accepted.

indicates that the network protocol requested by the remote site is not configured for WAN connections in your router. Inform the remote site on which network protocols are configured for WAN connections at the your site.

ISDN-124: Call to <Number> subaddress <x> rejected because the PPP inbound authentication failed.

indicates that the remote router could not provide correct PPP inbound authentication so that the call was rejected.

appendix **B**

AVM Data Call Center

Since March 1996, AVM has provided 30 additional ISDN and Mobile ISDN dial-in points.

The dial-in points are configured for direct access from ISDN-Controllers, remote access with AVM NetWAYS/ISDN as well as access with routers and via the Internet.

At the AVM Data Call Center, customers can obtain information about AVM, download product enhancements and the latest drivers for the AVM ISDN-Controllers.

MPR for ISDN Server

The MPR for ISDN Server in the AVM Data Call Center (ADC) in Berlin can be used as a test destination, for example if you configure your first router and do not have an own remote site to connect to. You may further dial-up the AVM Data Call Center from time to time to check for any *news and downloads*, such as Release Notes on new products or enhancements to existing products.

To access the MPR for ISDN Server, you will need the following connection parameters:

♦ Calling information:

ISDN Number: 03039984350 (when calling from somewhere in Germany)

Subaddress: 1

For calls from outside Germany, complete the Destination Address by first entering your international dialing prefix and the country code "49" for Germany, and then continue with "3039984350".

♦ Protocol specifics

Currently, only IPX/SPX is enabled on this router. The internal network numbers of the intranet are 39984xxx. Do not configure this number on your router too if you want to connect to AVM’s ISDN

Service Router, since this number must be unique within a WAN. Further, make sure that it is not filtered.

Note

TCP/IP will be enabled in the future. Access information will then be given in the *Technical Note on NetWare MultiProtocol Router for ISDN 3.1*.

♦ Login information

Server: adc

User name: guest.avm

Password: no password required

AVM ISDN Server: +49(0)30 399 84 300

You can access the AVM ISDN Server from any stand-alone PC with the DOS based file transfer program “Connect”, with AVM´s IDtrans or with AVM´s FRITZ!data software. You can also access the AVM ISDN Server from within the LAN if you have NetWare Connect for ISDN installed and run either of the above three file transfer applications on one of your LAN workstations.

AVM NetWAYS/ISDN Remote Access: +49 (0)30 399 84 360, Subaddress 1

You can access the AVM NetWAYS/ISDN Remote Access server from any stand-alone PC equipped with NetWAYS/ISDN and one of AVM´s active or passive ISDN-Controllers for terestrial ISDN access.

AVM NetWAYS/Mobile ISDN Remote Access: +49 (0)30 399 84 370

You can access the AVM NetWAYS/Mobile ISDN Remote Access server from any stand-alone PC equipped with NetWAYS/ISDN and one of AVM´s Mobile ISDN-Controllers and a mobile telephone for access via GSM-based digital cellular networks.

AVM in the Internet: http://www.avm.de

You can access information about AVM, about our products and more also via the Internet.