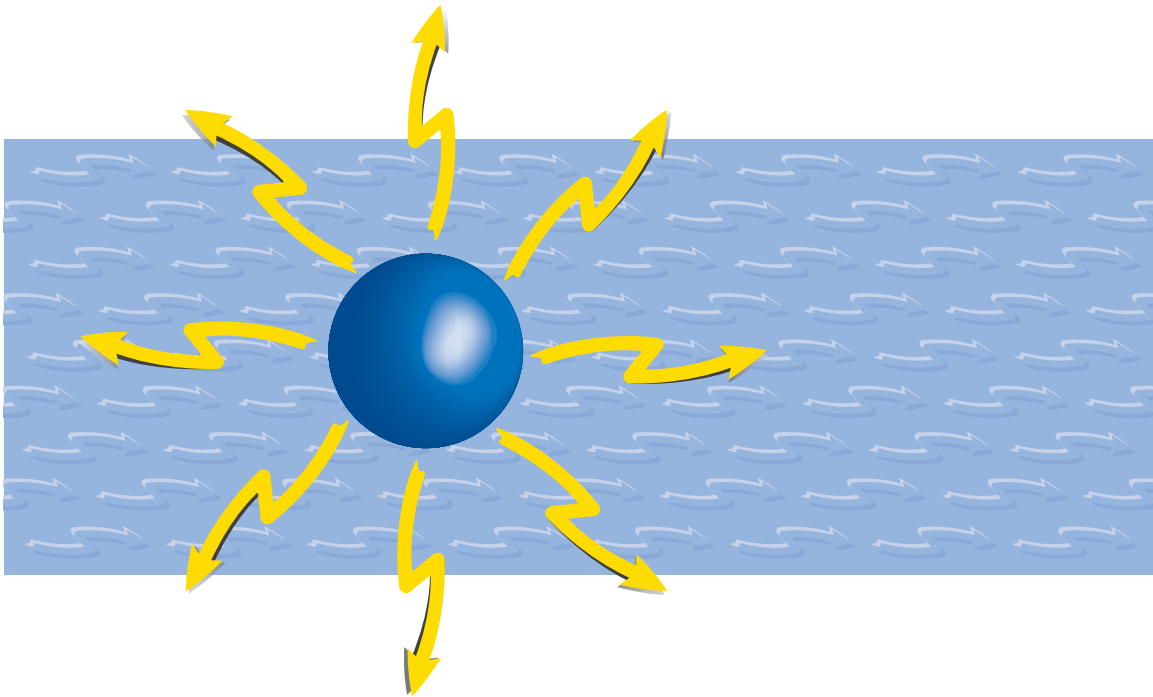
ISDN



AVM

ISDN MultiProtocol Router for Windows® 2000

ADSL

H a n d b u c h

Designed for Microsoft® BackOffice®

High-Performance ISDN by . . . AVM

AVM MultiProtocol Router for ISDN/DSL

Documentation release 02/2002

AVM Audiovisuelles Marketing
und Computersysteme GmbH
Alt-Moabit 95
10559 Berlin

AVM Computersysteme Vertriebs
GmbH
Alt-Moabit 95
10559 Berlin

AVM in the Internet: http://www.avm.de/en

Contents

Typographical Conventions

The following typographical conventions and symbols are used in this manual to make it more readable and to emphasize important information:

Highlighting

The following table presents a short overview of the highlighting conventions used in this manaul.

Highlighting	Function	Example
quotation marks	keys, buttons, program icons, settings pages, menus, commands	“Start / Programs” or “Enter”
capital letters	paths and files within floating text	DOCS\NTMPRI.PDF or CAPIPORT.HLP
pointed brackets	variables	‹CD-ROM drive›
typewriter characters	entries made using the keyboard	`a:\setup`
gray and italics	information, tips and warnings; always appear with the corresponding symbols	***... Controllers must be removed one at a time ...***

Symbols

The following symbols used in the manual always appear with gray, italicized text:

This symbol indicates useful tips and supplementary information.

The exclamation point designates sections which contain important information.

Indicates especially important instructions that absolutely must be observed to ensure correct functioning.

1 Introduction

Thank you for choosing the AVM MultiProtocol Router for ISDN/DSL (NT/MPRI). This product combines the advantages of ISDN and ADSL with those of the Microsoft operating systems Windows XP, Windows 2000 and Windows NT 4.0. As a multi-protocol router implementing highly developed technology, the NT/MPRI can be utilized in a wide variety of scenarios.

The AVM MultiProtocol Router for ISDN/DSL (NT/MPRI) allows physically separated networks to be connected to each other. The powerful ISDN and ADSK router also makes the Internet connection available to the entire LAN/WAN while effectively protecting it from unauthorized access. The NT/MPRI functions in complete accordance with open standards for Internetworking, ISDN, ADSL and PCs and supports both dialed ISDN connections and ISDN leased lines.

AVM Network Services

The NT/MPRI belongs to the AVM Network Services, a product group which makes it possible for computers in networks to communicate with each other. AVM Network Services make ISDN, GSM and ADSL communication technologies available to all users in the network. Each of the three software products can be operated as well in systems with Windows XP (Home and Professional Edition), Windows 2000 Professional and Server as in those with Windows NT 4.0 Workstation and Server. All three software products function as applications for ISDN-Controllers.

ISDN Access Server for ISDN/GSM: ISDN/GSM link-up from single workplace PCs to the local network

The ISDN Access Server guarantees fast and economical access to the company network for remote computers. This means that telecommuters and sales representatives can work with the resources of the central company network.

AVM MultiProtocol Router for ISDN/DSL: ISDN/ADSL link-up from networks and the Internet to the local network

The NT/MPRI offers professional ISDN routing for Microsoft networks and allows Wide Area Networks (WANs) and links to the Internet to be established. Now ADSL Internet routing is available thanks to support for ADSL.

Network Distributed ISDN: Central ISDN access for all PCs in the local network

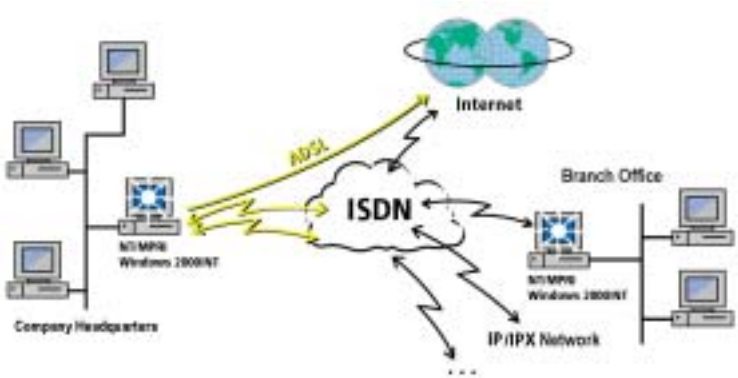
With NDI all users in the Microsoft network can use the ISDN hardware centrally administered in the server. For all workstations in the network, a CAPI 2.0 interface is available to enable ISDN functions like fax, file transfer, Internet access and on-line services.

AVM Network Services are remarkable for their rigorous utilization of ISDN and ADSL technology, simple installation, flexible administration and effective access protection. The products are Windows XP/2000/NT-based applications based on CAPI 2.0, the standardized application interface for ISDN-Controllers. Whenever the communications needs of your company grow, additional ISDN-Controllers are simply installed in the server. Thanks to CAPI, these controllers then are recognized and used automatically. This means long-term protection of your ISDN investment and optimum use of your server's capacity.

1.1 What Does the AVM MultiProtocol Router for ISDN/DSL (NT/MPRI) Offer?

Along with Internet access, the networking of physically separate local networks to a company wide-area network (WAN) plays an increasingly important role in modern corporate communications. The NT/MPRI allows ISDN links from Windows XP/2000/NT networks to other networks over TCP/IP and IPX/SPX as well as Internet access over ISDN and ADSL.

The NT/MPRI is installed on a Windows XP, Windows 2000 or Windows NT computer in the network.



Potential implementations of the NT/MPRI

The AVM MultiProtocol Router for ISDN/DSL connects physically distant networks. LAN resources at the central office, such as the servers, mainframes, SAP R/3 systems or databases, are thus also available at branch offices of all sizes. A great advantage is that the NT/MPRI automatically takes over any necessary routing activities like connection control so that no additional tasks must be performed by the user.

Communication in the other direction is also possible, of course, such that the local networks of the branch offices can be accessed from headquarters, for instance, to administer the network or to update the databases stored there.

The NT/MPRI also supports access to the Internet in a variety of ways, granting to all users in the LAN and the WAN access to Internet resources like E-mail, World Wide Web, news and more through one or multiple dial-in or leased ISDN lines or via ADSL. The NT/MPRI also supports combinations with E-mail servers, proxies or Web servers.

The NT/MPRI supports the open standard PPP over ISDN (**P**oint-to-**P**oint **P**rotocol) for ISDN connections from local networks. This means that the NT/MPRI can establish connections with all other ISDN routers that support this standard. For ADSL Internet routing, PPPoE (**PPP o**ver **E**thernet) is supported.

1.2 The individual features of the NT/MPRI

The following section offers a short overview of the features of the NT/MPRI.

Optimum ISDN Utilization

The ISDN digital communications network provides a number of features which offer enormous advantages for connecting to networks and to the Internet. The NT/MPRI exploits these features optimally.

The fast connections times in ISDN of less than one second allow the dynamic establishment and clearing of ISDN connections in the background, thus saving connection costs.

The ISDN feature “CLIP” (**C**alling **L**ine **I**dentification **P**resentation), the transmission of a caller’s ISDN number over the D channel, allows the NT/MPRI to check the identity of the remote site.

The ISDN B channels can be bundled in order to increase transmission speeds; channels can even be combined from multiple ISDN-Controllers. Because one to four AVM ISDN-Controllers B1 or one ISDN Control-

ler C4 is supported at the basis rate interface (BRI), the BRI version of the NT/MPRI can be expanded to up to eight channels. In the version for the primary rate interface (PRI) up to 120 B channels can be used.

The driver software for the AVM ISDN-Controller in Windows XP/Windows 2000/NT computers is included in the NT/MPRI package. It is located on a separate CD entitled "Server Edition". The driver software supports the DSS1 (Euro ISDN) D-channel protocol as well as the common national protocols.

The NT/MPRI uses and controls the ISDN connection through AVM ISDN-Controllers, over which it can be operated either directly on the public ISDN network (point-to-multipoint or point-to-point access) or at a Private Branch Exchange (PBX).

The following types of leased lines are also supported (designations of the Deutsche Telekom AG):

- Digital 64S (B channel 1x64 Kbit/s)
- Digital $64S_2$ (B channel 2x64Kbit/s)
- Double-switching Digital 64S (B channel 2x64Kbit/s, split between two users with 1x64Kbit/s each)
- Digital S_0/TS_{02} (B channel 2x64 Kbit/s + D channel 1x16 Kbit/s)

The AVM ISDN-Controllers B1, C4 and T1-B offer support for GSM in accordance with the Mobile ISDN standard (GSM 07.08), enabling reliable and seamless network connections over ISDN even via GSM and HSDCSD (**H**igh-**S**peed **C**ircuit-**S**witched **D**ata).

Optimum ADSL Utilization

ADSL (**A**symmetric **D**igital **S**ubscriber **L**ine) is a technology which makes Internet access at a high bandwidth possible using normal telephone lines. ISDN and ADSL use different frequency ranges, enabling parallel operation free of interference.

Transmission Features

For optimum utilization of the ISDN bandwidth and to increase transmission performance, the NT/MPRI offers the following functions:

- data compression (in accordance with the V.42bis CAPI standard, Stac LZS and MPPC)
- header compression for IP and IPX (Van Jacobson TCP/IP header compression, CIPX header compression)
- channel bundling (in accordance with the CAPI standard as well as static and dynamic over PPP Multilink)

Reducing and Limiting Connection Charges

Through its intelligent connection management, NT/MPRI makes sure that the costs for ISDN connections to remote networks are reduced to a minimum. The following features ensure this:

- The NT/MPRI differentiates between logical and physical ISDN connections. A logical ISDN connection is produced when the first physical connection is established over ISDN and the corresponding connection parameters are negotiated. These include the network protocols used, authentication, spoofing mechanisms and channel bundling.

  For the physical ISDN connection one or more B channels are actually connected, and connection charges are incurred. If no data are being transmitted on the ISDN line, the NT/MPRI can clear the physical connection automatically to reduce connection costs. Depending on the configuration of the corresponding destination, the logical connection can be maintained in the NT/MPRI so that the remote site is registered in the network and resources remain reserved for it there. As soon as data transmission resumes, the NT/MPRI or the remote site re-establishes the physical connection.

- The period of time until the physical connection is cleared can be adapted dynamically to the current charge rates using charge profiles. Charge profiles contain information about the various charge rates for different area codes and times of day. The charge impulse transmitted on the ISDN line also can be used to control the clear-down process or to set a charge limit at which the physical connection is automatically cleared.

The NT/MPRI does not establish a DSL connection until Internet services are actually requested. During inactive periods the NT/MPRI clears the connection after completing the last 60-second phase begun.

- Tried and true filters and spoofing mechanisms intercept certain protocol packets and prevent their unnecessary transmission over ISDN to reduce the duration of the physical connection. The NT/MPRI thus makes sure that the ISDN line is established almost exclusively for effective data and keeps most of the background data traffic in the LAN away from ISDN.
- Adjustable threshold values (per day, week and month) for the maximum budget, maximum duration of the physical connection and the maximum number of outgoing calls.
- Budgets definable for each destination.
- Cost assignment (COSO=**C**harge **O**ne **S**ite **O**nly), for instance, having company headquarters take on all of the costs for connection to the network.

Security Functions

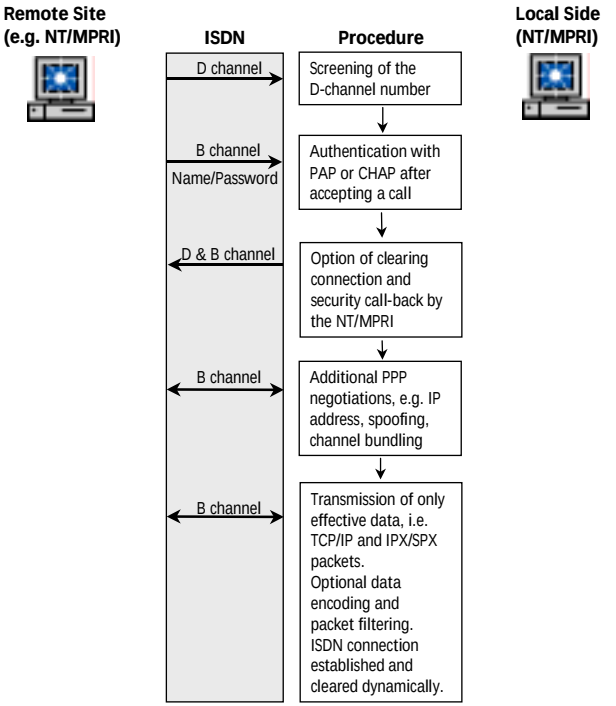
The NT/MPRI offers security functions on two different levels. Through its sophisticated **access protection** the NT/MPRI makes sure that only authorized remote sites can access the LAN over ISDN. **Data protection** ensures that no unauthorized access to the data occurs during transmission.

Access Protection

The following functions are available:

- screening of the D-channel number of the calling side
- authentication with the PPP protocols PAP or CHAP.
  The NT/MPRI supports authentication both on the local end and at the remote site. Different passwords can be used on each end.
- security call-back for incoming calls
- firewall functions through preset and configurable IP filter profiles
- IP masquerading/Network Address Translation (NAT)
- configurable IPX RIP/SAP filters

The security checks which can be activated for an incoming call from a remote user are illustrated in the following figure:



Security mechanisms of the NT/MPRI: example of establishing a connection

Data Protection

The NT/MPRI offers the option of data encoding to protect data packets from unauthorized access during transmission. The ECP (**E**ncryption **C**ontrol **P**rotocol), the symmetrical Twofish encoding algorithm and the Routing and Remote-Access API expanded by the Crypt Provider API guarantee an extremely high level of data protection on the ISDN line.

Simple Installation and Operation

Installation of the NT/MPRI is simple and menu-driven.

The NT/MPRI is configured and managed entirely via HTTP using a standard browser like the Microsoft Internet Explorer or Netscape Navigator. This means that the router can be operated and managed at any time from any computer in the local network. The HTTP access is password-protected.

The predefined profiles for destinations (IP, IPX, IP+IPX and Internet) can be used to simplify the administrator's task of configuration.

All configuration information is written in a special configuration database, NTR.MDB. This database is located in the installation directory of the NT/MPRI and can be viewed with Microsoft Access.

Static and Dynamic Routing

Like any router, the NT/MPRI functions on the network protocol level (layer 3 of the ISO/OSI reference model) and forwards incoming data packets to other networks connected to the router. For this the following information is required:

- the logical address of the destination
- the path to the destination

Every network protocol uses its own kind of address. A comprehensive explanation of TCP/IP addresses is presented in the glossary at "TCP/IP Addresses" on page 123.

Information about the possible paths of data packets are summarized in what is known as a "routing table". Routing tables can be generated statically or dynamically:

- **Static**:
  In static routing all destination networks and the corresponding information are configured manually and will not be changed automatically.
- **Dynamic**:
  In dynamic routing a routing protocol is used which routers in the entire network use to announce at regular intervals changes in their routing tables.

The NT/MPRI uses the following kinds of routing:

- for IP:
  dynamic routing with RIP 2 on the LAN end and static routes over ISDN

  Static routes over ISDN excludes the possibility of connections being established through the dynamic exchange of RIP packets. During configuration it can be specified whether a static route should always be known in the WAN or whether it should not be made known until the administrator establishes a logical ISDN connection. In the former case the logical ISDN connection is es-

tablished automatically by a packet intended for a destination outside the LAN. In the latter case, packets can only be sent to a destination for which the route is known, i.e. for those to which a logical ISDN connection exists.

- for IPX:
  dynamic routing with IPX RIP and SAP on the LAN side and over ISDN. When a logical connection over ISDN is established for the first time, RIP/SAP is exchanged and the possible routes in the network are announced. RIP/SAP is used as long as a logical ISDN connection exists. NT/MPRI reduces costs by only sending RIP/SAP updates when changes are implemented.

  A static route over ISDN to a Netware server can also be defined. This had the advantage that the external server is always known in the local network, even if no logical ISDN connection exists. If data packets are awaiting transmission to the remote router, the physical ISDN connection will be established automatically.

Records and Log Functions

Comprehensive records and log functions allow the exact assessment of all actions on the router:

- status information at
  - the NT/MPRI and the ISDN and ADSL-Controller
  - the available IP and IPX routes and SAP services as well as the ARP table
  - the physically active ISDN connections
- data about the cost and use for connections as a daily overview or selected according to specific criteria such as certain destinations
- recording events as a daily overview or selected according to specific criteria like the “Information” message type
- packet recording with PPP decoding

Interoperability over ISDN

Through support of the interoperability standard PPP over ISDN along with many other PPP standards, described in what are called RCFs, connections are possible to all remote sites that also support these standards.

In addition to the RFCs, newer, not yet generally recognized PPP standards, known as “drafts” are implemented in the NT/MPRI. AVM also has developed various spoofing procedures which are implemented in the NT/MPRI on the basis of the PSCP draft. The NT/MPRI supports the following RFCs and RFC drafts:

RFC 1144	Compressing TCP/IP Headers for Low-Speed Serial Links
RFC 1332	The PPP Internet Protocol Control Protocol (IPCP)
RFC 1334	PPP Authentication Protocols (PAP)
RFC 1552	The PPP Internetwork Packet Exchange Control Protocol (IPX-CP)
RFC 1553	Compressing IPX Headers Over WAN Media (CIPX)
RFC 1570	PPP LCP Extensions
RFC 1618	PPP over ISDN
RFC 1631	The IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1662	PPP in HDLC-like Framing
RFC 1962	The PPP Compression Control Protocol (CCP)
RFC 1974	PPP Stack LZS Compression Protocol
RFC 1990	The PPP Multilink Protocol (MP)
RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 1986	The PPP Encryption Control Protocol (ECP)
RFC 1989	PPP Link Quality Monitoring
RFC 2118	Microsoft Point-to-Point Compression (MPPC) Protocol
RFC 2284	PPP Extensible Authentication Protocol (EAP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
Draft	PPP Callback Control Protocol
Draft	PPP Protocol Spoofing Control Protocol (PSCP)
Draft	The PPP Bandwidth Allocation Protocol (BAP)
	The PPP Bandwidth Allocation Control Protocol (BACP)

Connection Control

Generally ISDN connections are established automatically on the service channel when resources of the remote site are accessed. If needed, connections can be established and cleared automatically from the NT/MPRI interface.

The connection control also presents detailed information about the logical ISDN connections currently active and the negotiated connection parameters.

The CICC.EXE program which runs on the same computer as the NT/MPRI allows batch-controlled IP or IPX connections to be established in order to realize dial-around scenarios.

Routing and Remote Access API

Routing and Remote Access API by AVM is a programming interface and allows the NT/MPRI to be controlled through software. This means that certain tasks or processes can be combined with functions of the NT/MPRI and automated. Examples include the definition of dial-around routines for the automatic transfer of database updates to branch offices at the most economic rates or the integration of additional security mechanisms like chip cards and thus intervention into PPP authentication.

Comprehensive additional information about using the API (test programs including source and libraries) is available on the CD in the folder UTILS\API\AVMNWAPI.

Crypt Provider API

Crypt Provider API is a programming interface for user-specific adaptation of data encoding. The codes used to encrypt the data to be transmitted are generated anew and transferred to the remote site each time a connection is established. For security reasons these codes must be transmitted in encrypted form. The encryption is performed by Crypt Provider, which is programmed specifically for each application (Smart Card, PIN, Biometrie, etc.). Crypt Provider API is the interface to the NT/MPRI which accesses the algorithms in the Crypt Provider.

Comprehensive additional information about using the Crypt Provider API (test programs including source and libraries) is available on the CD in the folder UTILS\API\AVMNWAPI.

Installation Together with Other CAPI 2.0 Applications

Meaningful and cost-effective use of multiple ISDN-Controllers is ensured by combining the installed ISDN-Controllers with the two AVM products: ISDN Access Server and NDI. Certain B channels can be reserved for the AVM Network Services products to guarantee smooth assignment of the ISDN lines when these products are used simultaneously.

The ISDN-Controllers can be used by other CAPI 2.0 applications as well, such as fax transmission. If other CAPI 2.0 applications which use the same ISDN service as the NT/MPRI (such as file transfer software in server mode) are installed on the same computer, it must be ensured that all applications are addressed unambiguously for incoming calls to be assigned correctly. The CAPI 2.0 standard furnishes with multiple subscriber numbers (MSNs) at the basic access and suffixes (DDI) at the primary rate access to allow unambiguous assignment in such cases.

1.3 Package Contents

The following contents are included in the AVM MultiProtocol Router for ISDN/DSL package:

- "AVM MultiProtocol Router for ISDN/DSL" CD including a CD key
- "Server Edition" CD with drivers for the AVM ISDN-Controller B1, C4 and T1 or T1-B for Windows XP/Windows 2000/NT
- AVM MultiProtocol Router for ISDN/DSL manual

Two variants of the product are available: the BRI version (1-8 B channels), and the PRI version (1-120 B channels).

If any of these contents are missing, please contact your vendor.

2 Installation and First Steps

This chapter first explains how to prepare your local network for installation of the NT/MPRI. In the next sections the installation and operation of the NT/MPRI are described.

After installation, first familiarize yourself with operation of the NT/MPRI and then establish a first ISDN connection to a reference router at the AVM Data Call Center (ADC) in Berlin. Instructions for this test connection are also included in this chapter.

2.1 Installation Requirements

Computer Hardware for the NT/MPRI

The requirements for the operating system Windows XP, Windows 2000 or Windows NT must be fulfilled; at a minimum

- Intel Pentium® 90 MHz or higher
- at least 50 MB free memory on the hard drive
- at least 32 MB RAM
- Ethernet or Token-Ring network adapter(s) certified for Windows XP/2000/NT
- If an ISDN access is to be used, an AVM ISDN-Controller B1, C4,T1 or T1-B is required.

  The BRI version can be installed on an AVM ISDN-Controller T1 or T1-B. In this case, however, only eight B channels can be used for the NT/MPRI.
- If an ADSL access is to be used, an additional network adapter or an AVM ADSL/ISDN-Controller is required to connect the computer to the ADSL access.
- The network adapters for connecting the computer to the LAN already must be ready for operation, i.e., fully installed in Windows XP/2000/NT and configured for TCP/IP.

Computer Software for the NT/MPRI

- Windows XP/2000 Professional or Server with the corresponding current Service Pack, or Windows NT Server or Workstation with the corresponding current Service Pack.
- Browser: Microsoft Internet Explorer (included in the NT/MPRI package) or Netscape Navigator.

ISDN Line

The following features should be enabled on your ISDN line to take advantage of all functions of the NT/MPRI:

- AOCD

  Charge information during the connection in accordance with the European standard AOCD: Advice On Charge During Call, which is used for clearing the physical connection automatically and for monitoring costs with budgets.

- CLIP

  Transmission of the caller's number on the D channel. CLIP is used to monitor telephone numbers and to identify incoming calls.

ADSL Line

To use the ADSL functions, the following is required:

- An ADSL line so that PPPoE is available over a network interface.

2.2 Preparations for Installation

Installation requirements as well as the hardware and software demands are listed in the section "Installation Requirements" on page 18.

Local Network

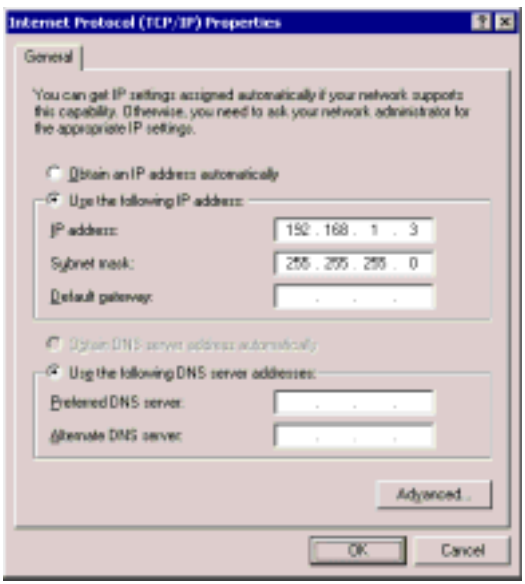
Your local network must be in working order before installing the NT/MPRI. This means that all servers and workstations must be addressed unambiguously and that the error-free exchange of information must be ensured.

TCP/IP Settings

If you use TCP/IP in the local network, each workstation, including the computer on which the NT/MPRI is to be installed, requires an unambiguous IP address. It is important that the NT/MPRI computer receive a static IP address, even if the rest of the network receives addresses assigned by DHCP.

In Windows XP an IP address must be entered manually as a standard gateway in the properties of the TCP/IP protocol under “Start / Network Connections”. This IP address must differ from the IP address of the computer. In our example, the IP address 192.168.1.1 is a possible value (see the figure below).

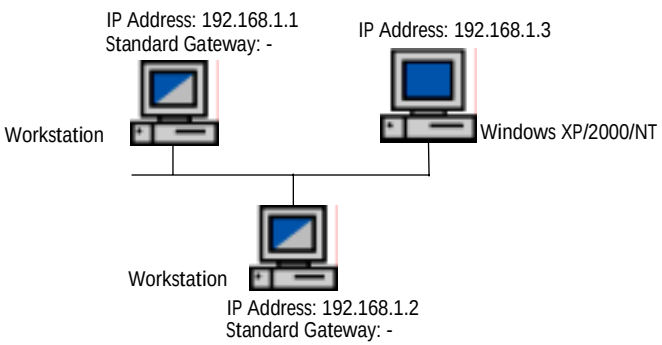
In Windows 2000 an IP address must be entered manually as a standard gateway in the properties of the TCP/IP protocol under “Start / Settings / Network and Dial-up Connections”. This IP address must differ from the IP address of the computer. In our example, the IP address 192.168.1.1 is a possible value (see the figure below).



TCP/IP settings in Windows 2000 on the computer on which the NT/MPRI is to be installed; IP address example

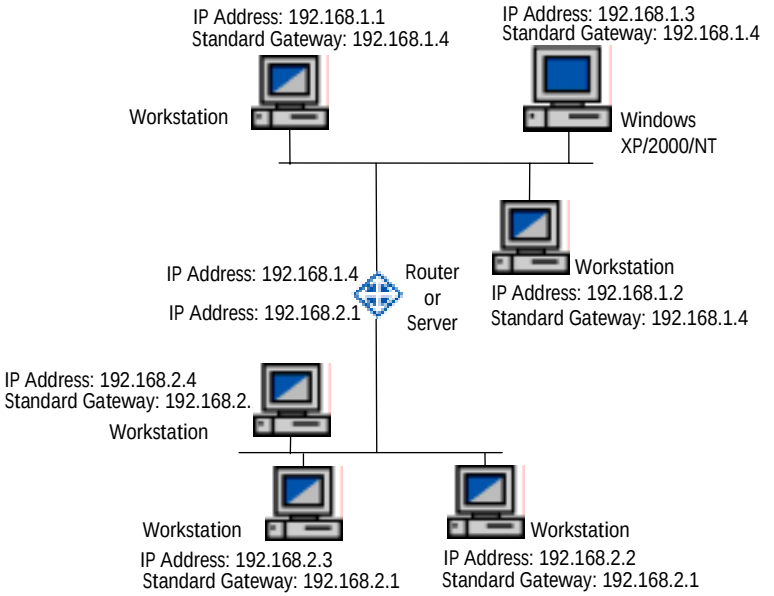
Below the computer with the example IP address 192.168.1.3 is prepared to utilize ISDN and then the NT/MPRI is added.

If your LAN consists of just one local network, make sure that the IP address is registered on all workstations. It is not necessary to have a standard gateway registered before installation.



IP address assignments before installing the NT/MPRI: small network

If your network consists of multiple segments connected to each other via routers, enter the IP address of each segment's router as the standard gateway on all of the computers in the segment.



IP address assignments before installing the NT/MPRI: large network

IPX Settings

If you use IPX in the LAN, the computer on which the NT/MPRI is to be installed requires an unambiguous internal IPX network number. It is also possible to register this internal network number in the NT/MPRI Manager after installation. The NT/MPRI accepts the frame type settings “Auto Frame Type Detection” and “Manual Frame Type Detection”.

Settings for the ISDN-Controllers and ADSL-Controllers

ISDN-Controllers

Once the ISDN-Controller has been installed in your computer, it will be recognized by Windows XP/2000 automatically as a Plug & Play device. Follow the instructions on the screen.

In Windows NT, install the driver software for your ISDN-Controller(s) from the “Server-Edition” CD included in the package.

The ISDN-Controllers are managed in the NT/MPRI using the controller number assigned during installation of the driver software (CAPI). If multiple ISDN-Controllers are to be used, make a note of the number assigned to each ISDN-Controller during installation.

The driver software for the AVM ISDN-Controller(s) must be loaded automatically when Windows XP/2000/NT is started! For more information see the controller manual or the corresponding Readme.

Once the ISDN-Controller(s) have been installed, use the program Connect32, included in every AVM ISDN-Controller package, to establish a test connection to the AVM Data Call Center (ADC) and check that your ISDN line and the controller(s) function properly.

ADSL-Controllers

An additional network adapter is recommended to connect the computer to an ADSL modem. The ADSL modem then will be connected to this free network adapter. It is not necessary to bind TCP/IP to this new network adapter, as PPPoE packets are exchanged with the ADSL modem rather than IP packets.

Next the DNS server of the new network adapter must be registered in the network settings:

Windows XP

1. In “Start / Network Connections”, click the LAN connection with the right mouse button and select “Properties” from the context menu.
2. On the “General” settings page, select from the “This connection uses the following items” list the entry “Internet Protocol (TCP/IP)” and click the “Properties” button.
3. Select “Use the following DNS server addresses” and enter the IP address of the DNS server of the new network adapter in the “Preferred DNS server:” field.

Windows 2000

1. In “Start / Settings / Network and Dial-Up Connections”, click the LAN connection with the right mouse button and select “Properties” from the context menu.
2. On the “General” settings page, select from the “Components checked are used by this connection” list the entry “Internet Protocol (TCP/IP)” and click the “Properties” button.
3. Select “Use the following DNS server addresses” and enter the IP address of the DNS server of the new network adapter in the “Preferred DNS server:” field.

Windows NT

1. In “Start / Settings / Control Panel / Network”, go to the “Protocols” settings page and select the “TCP/IP Protocol” and click the “Properties” button.
2. On the “DNS” settings page, add the IP address of the DNS server of the new network adapter to the “DNS Service Search Order” list.

Once these preparations are complete, the NT/MPRI may be installed.

2.3 Installing the NT/MPRI

The following components are installed on your computer during installation:

- AVM MultiProtocol Router for ISDN/DSL
- AVM WebServer (for HTTP communication between the NT/MPRI and the browser)

Proceed as follows to install the NT/MPRI:

1. Insert the NT/MPRI CD in your CD-ROM drive.
2. A CD introduction appears automatically. Start the installation program and then follow the instructions on the screen.

   The welcome screen of the installation program appears.
3. Click “Next” to continue with installation.
4. Enter the CD key. This code is located on the CD cover.

   Confirm your entries by clicking “OK”.
5. Confirm that the NT/MPRI is to be installed by clicking “OK”.
6. The next step is to enter the folder in which the NT/MPRI is to be installed.

   If the AVM ISDN Access Server is already installed on the computer, the NT/MPRI files will be copied to the same folder.

   Otherwise the path C:\PROGRAM FILES\AVM\ISDN MULTIPROTOCOL ROUTER is suggested by default. Any other path desired may be specified. Confirm the path for installation by clicking “Next”.

   The program files for the NT/MPRI will be installed now.

As a final installation step, a new program called “AVM NT-MPRI Manager” is added to the Windows XP/2000/NT Start menu. Use this icon to start the standard browser you configured as well as the NT/MPRI’s HTML interface.

7. Re-install the Microsoft Service Pack now. Answer the question about whether newer files should be overwritten with “No”.

   The latest Service Pack at the time the CD was produced can be found in the UTILS directory on the CD.

   The latest Service Pack at the time of installation is located on the Microsoft Internet site.

8. Restart Windows XP/2000/NT to conclude installation.

Modifications to Windows

The following changes have been made In Windows XP/2000/NT:

- The services “AVM NT/MPRI” and “AVM WebServer” were integrated into Windows XP/2000/NT.
- The protocol “ISDN Service Wrapper” was added.

  The ISDN Service Wrapper switches between the network adapters, the network protocols and the Windows XP/2000/NT Service “AVM NT/MPRI”.
- The existing protocol bindings from TCP/IP and IPX to the network adapters were removed. TCP/IP and IPX have been linked to the ISDN Service Wrapper instead.
- If no standard gateway was registered in Windows NT before the installation, an entry is registered after installation.

Proceed as follows to check whether the NT/MPRI is started:

1. In the Windows XP Start menu, click “Settings / Administrative Tools”.

   In the Windows 2000 Start menu, click “Settings / Control Panel / Administrative Tools”.

   In the Windows NT Start menu, select “Settings / Control Panel”.

2. Double-click the “Services” icon.

   The list includes the service “AVM NT/MPRI”. If the NT/MPRI was started successfully, the “Status” column contains the message “Started”.

   The “Startup Type” column entry reads “Automatic”, meaning that the NT/MPRI will be started automatically every time Windows XP/2000/NT is started.

2.4 The NT/MPRI Manager

The NT/MPRI Manager is the web-based user interface of the NT/MPRI for the administrator.

The NT/MPRI Manager can be opened directly on the NT/MPRI computer or from any computer in the network that is linked with the NT/MPRI via TCP/IP.

To start the program on the NT/MPRI computer itself, select “Programs / AVM NT-MPRI Manager” from the Windows XP/2000/NT Start menu. The web browser configured as your standard browser is started and the selection page with the languages supported by the NT/MPRI Managers displayed.

To access the NT/MPRI from another computer in the network, start the standard web browser configured there and enter the URL of the start page:

http://<IP address>:4000/ntmpri.html

(IP address=IP address of the NT/MPRI computer)

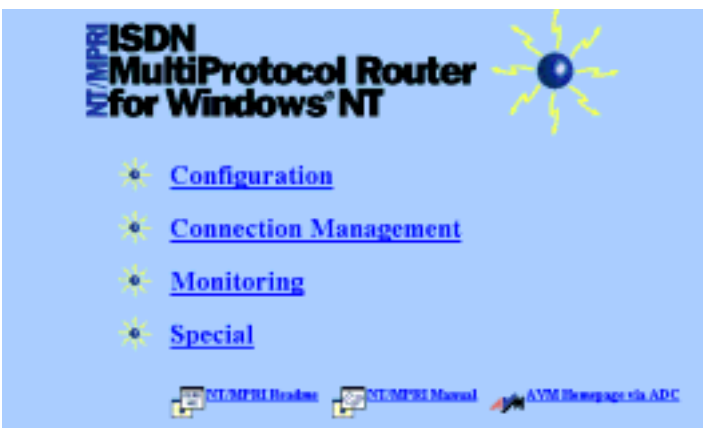
If a domain name server is installed in your network, the NT/MPRI Manager also can be started as follows:

http://<Name>:4000/ntmpri.html

(Name=name of the NT/MPRI computer in the domain)

First select the language in which the NT/MPRI is to be administered. Since access to the NT/MPRI is protected, the user name and password of a user with administrator rights on the Windows XP/2000/NT computer must be entered here. Then click “OK”.

Now the start page of the NT/MPRI appears:



Start page of the NT/MPRI

This start page provides access to all functions required for the configuration and administration of the router:

- Configuration: calls up the settings and permits changes
- Connection Management: allows ISDN connections to be actively established and cleared
- Monitoring: presents detailed status and statistics information along with a packet trace function
- Special: allows the NT/MPRI service to be stopped and started in Windows XP/2000/NT, provides access to the routing adn RAS API, and enables the downloading of extensions and updates to the NT/MPRI over ftp.

- NT/MPRI Readme: displays the latest information about the NT/MPRI, as a supplement to the manual.

  The Readme file is displayed in its own browser window. To resume working with the NT/MPRI, close this window.

- NT/MPRI Manual: opens the PDF version of this manual.

  The manual is displayed in Acrobat Reader. To resume working with the NT/MPRI, close this window.

- AVM Home Page via ADC: connects to the AVM Intranet server using the pre configured call destination “ADC-IP”. This connection provides direct access to AVM’s Web site and product information.

- The detailed Online Help in HTML format is opened by clicking this button on any NT/MPRI page. The Help is opened in a second browser window.

Click this button to close the Help window.

Click Start Page to return to the Start page of the user interface.

Changes to the configuration, like adding new destinations, are not activated until the NT/MPRI service is restarted in Windows XP/2000/NT (“Special / Restart Service / Restart Service”).

Joint Installation of AVM Network Services

If multiple products from the AVM Network Services series are installed on your system, for instance, the NT/MPRI and the ISDN Access Server, the joint start page of both products can be used. Access this page at the following URL:

http://<Name> or <IP address>:4000

For a joint installation of the NT/MPRI and the ISDN Access Server, two different program icons are generated in the Windows XP/2000/NT Start menu, but the programs have the same interface. A number of the menus are valid for both products, including “Server Status”, “Settings for the ISDN-Controllers” and “Charge Profiles”. Other menus are valid for only one of these products, like “User” for the ISDN Access Server and “Call Destinations” for the NT/MPRI.

Changes made in a menu shared by both products thus are implemented for both the NT/MPRI and the ISDN Access Server.

If both program windows are opened at the same time, closing one window closes the other as well.

2.5 Test Connection with the AVM Data Call Center

Once the NT/MPRI has been installed and the Windows XP/2000/NT computer has been restarted, follow the instructions below to establish a test connection to a master router at the AVM Data Call Center (ADC):

1. Start the NT/MPRI Manager.
2. Check the settings for your ISDN-Controller(s) at “Configuration / Server Settings / ISDN-Controllers”.

   By default, the first ISDN-Controller is registered as “Used”. If additional ISDN-Controllers are installed in your computer, add them here. It may be necessary to define additional settings for the ISDN-Controllers, if you work at a PBX, for instance. See the Online Help for more instructions.
3. Check the pre-configured destination “ADC-IP” at “Configuration / Call Destinations / Configured Call Destinations / ADC-IP”.

   The following settings may require modification:

– Number: If you are calling from outside Germany, the number must be changed accordingly.

– Charge profile for estimating charges: Set the charge profile to correspond to your line charges.

The monthly budget for this connection is preset to 5 DM (2.5 EURO) to prevent high connection charges for this test connection.

4. Start the NT/MPRI by selecting “Restart Service”.

5. Open the “Connection Management” page and set up the desired test connection to the ADC.

6. Return to the NT/MPRI Start page and click “AVM Home Page via ADC” or check the connection by entering at the prompt **`ping 192.168.113.8`**.

General instructions for configuration are presented in the next chapter, “Configuration and Operation of the NT/MPRI: The Basics” from page 31. Detailed information about the parameters is available in the Online Help, accessible directly from the HTML interface.

This test connection confirms that the NT/MPRI is correctly configured for ISDN.

2.6 Uninstallation

Proceed as follows to remove the NT/MPRI:

Windows XP/2000

1. In “Start / (Settings) / Control Panel”, click the “Add/Remove Programs” icon.

2. In the left-hand side of the window, click “Change or Remove Programs” and then select the entry “AVM NT/MPRI” in the right-hand section.

3. Click the “Change/Remove” button.

   No confirmation dialog appears!

   The NT/MPRI now will be removed.

4. Restart Windows XP/2000.

Always restart a Windows XP/2000 computer between uninstallation and a new installation of the NT/MPRI to update the entries in the Windows XP/2000 registry!

Windows NT

1. In “Start / Settings / Control Panel”, click the “Add/Remove Programs” icon.
2. In the lower window, select the entry “AVM NT/MPRI” and click the “Add/Remove...” button.
3. Confirm that you wish to delete the application.

   The NT/MPRI now will be removed.
4. Restart Windows NT.

Always restart a Windows NT computer between uninstallation and a new installation of the NT/MPRI to update the entries in the Windows NT registry!

3 Configuration and Operation of the NT/MPRI: The Basics

Configuration of the NT/MPRI is performed in the following steps:

1. settings for the server
2. setting up call destinations
3. testing the connections to the call destinations
4. refining the settings

This chapter describes the first three steps. You will learn which settings must be performed in the NT/MPRI to connect two local networks to each other or to connect to the Internet. How to refine and specialize the defined settings is described in “Special NT/MPRI Settings” from page 53.

3.1 Settings for the Server

Global settings valid for the whole server are defined in the “Configuration / Server Settings” menu.

Settings for ISDN-Controllers

Settings for ISDN-Controllers are defined in the “Configuration / Server Settings / ISDN-Controllers” menu. Immediately after installation the settings of ISDN-Controller 1 are displayed. During installation of the NT/MPRI, ISDN-Controller 1 is registered as used by and configured for operation at a point-to-multipoint line by default. If multiple ISDN-Controllers are to used, you can add the other controllers here and change the default settings for Controller 1.

If an AVM ISDN-Controller C4 is installed in the NT/MPRI computer, it is important to note that the Controller C4 is represented by four single controllers in the computer. If all four controllers are to be used in the NT/MPRI, the three other controllers must be added and configured separately.

Follow the instructions below for the configuration of your ISDN-Controller(s):

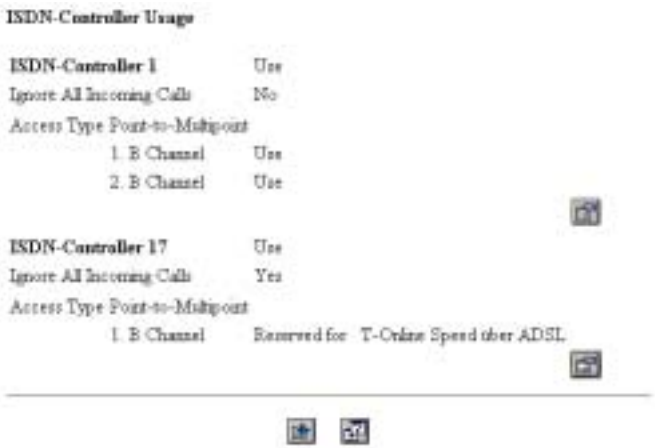
- First establish whether the ISDN-Controller is to be used. Specify whether the ISDN-Controller is connected to a PBX. If so, enter the information required, such as the outside dialing access and the minimum length of external numbers.
- Specify whether the ISDN-Controller is operated on a point-to-multipoint line, a point-to-point line or a primary rate access or whether it is used for a leased line. Comprehensive instructions for leased lines are presented in the section “Leased Lines” on page 64.
- If other CAPI-based applications are installed on the same computer as the NT/MPRI or are connected to the same S_0 bus, it is advisable to assign multiple subscriber numbers or suffixes for accepting incoming calls. This is the only way to ensure that incoming data calls are routed correctly.

Once these entries have been saved, the individual B channels of the ISDN-Controller are listed. These now can be registered as used or not used and reserved for a certain call destination or AVM Network Services product. For example, one B channel can be reserved for a certain call destination so that it can access your LAN at all times. In this case activate the “Reserved for” setting and select the call destination from the list.

Settings for ADSL-Controllers

After installation of the NT/MPRI, one controller is preset for the ADSL modem and designated as ADSL-Controller 17. Controller 17 is reserved for the call destination “UUNet over ADSL”. When a connection is established with this controller, the NT/MPRI automatically checks the installed network adapters to determine where the ADSL modem is connected.

To specify that a certain other network adapter in the NT/MPRI is to be addressed, select controller 18, 19 or 20. These controller numbers are assigned to the network adapters 1, 2 and 3.



Settings for the ISDN-Controller 1 and the ADSL-Controller 17

3.2 Setting up Call Destinations: Basic Settings

The term “call destinations” in the NT/MPRI refers to the routers in remote networks to be bound to the local network over ISDN. Setting up call destinations in the NT/MPRI primarily serves to:

- establish connections to remote routers
- identify and authenticate incoming calls

This section and the next describe how to set up a call destination, which parameters can be set up during configuration and what effects these settings have. Initially you will learn about the basic settings for a call destination, i.e., those which are necessary to create a connection to the call destination. The section “Configuring Call Destinations: Fine-Tuning the Settings” from page 47 explains the parameters with which settings like cost reduction, data security and data protection can be configured.

For the configuration of new call destinations, the NT/MPRI offers predefined profiles for Internet access, TCP/IP connections, IPX connections and connections which use both network protocols. For each of these connections there is one profile each for dial-up connections and leased lines.

In these profiles, only those parameters are displayed that are relevant for standard connections of the given type. A number of the parameters already have been assigned appropriate values. The profiles thus

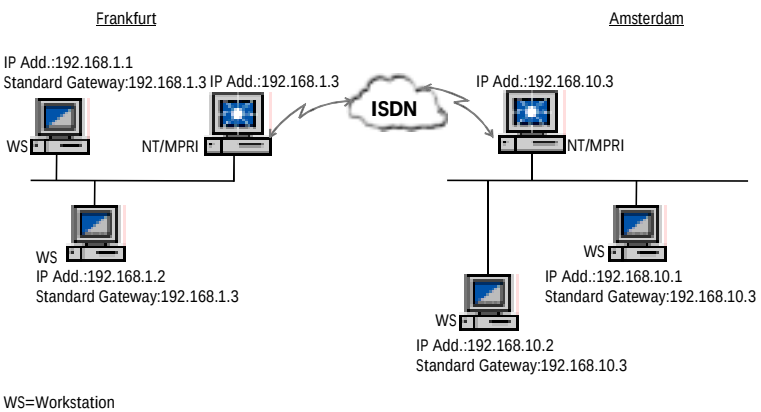
simplify configuration considerably, for once a call destination has been configured and saved, the given parameters can be adapted for additional call destinations. There is also the option of creating a call destination without a pre-defined profile; in this case all available parameters for the connection are listed in the input fields.

3.3 Connecting Two Networks with IP

The prerequisites and necessary settings in a TCP/IP network are illustrated with two examples here. In the first, simpler example, a small TCP/IP network is to be linked to another TCP/IP network over ISDN. In the second example, one network consists of multiple small networks connected to each other via a router.

For the sake of simplicity, here it is assumed that the NT/MPRI is used on both ends.

Example 1
A Small Network Link via ISDN



A small network link to ISDN

Step 1:

First, configure a new call destination designated “Amsterdam”. Since the two networks are to be lined over IP, select the pre-defined “IP” profile at “Configuration / Call Destinations / New Call Destination”. An input mask with the parameters generally required for IP dial-in connections opens. Make the following settings so that the connection can be established:

1. In the “Designation” field, enter “Amsterdam” as the name of the call destination.

   The NT/MPRI now will manage this call destination using the name “Amsterdam”.

2. In the “Number” field, enter 0031209876543 (example value) as the number of the router in the Amsterdam LAN.

3. In the line “Authentication at Remote Site” enter “Server Frankfurt” in the “Name” field and the password assigned in the “Password” field. These two values serve to identify you when you dial in to the Amsterdam LAN. Both values must be assigned from the network administrator of the remote site.

4. In the “Authentication at Local Site” line, select “PAP” or “CHAP” and “Always perform”. In the “Name” field, enter “Server Amsterdam” and the arranged password in the “Password” field. These two values serve to identify the remote site when it dials into the Frankfurt LAN. Both must be arranged with the network administrator of the remote site.

5. In the line “Inactivity Timeout”, select the option “Charge Profile” and select the charge profile “DT Deutschland” from the list.

6. In the “Network Address” field in the “Static Route” line, enter the IP address “192.168.10.0”. In the “Mask” field, enter the value “24” (corresponds to “255.255.255.0”, see “Subnet Masks (Masks)” on page 125) and a value of “1” in the “Metrics” field. All of these values can be obtained from the network administrator of the remote site.

7. Save the call destination.

Input mask for an IP dial-in connection with example files

8. Select the menu command “Special Settings / Restart Service” and click the “Restart Service” button.

9. Select the menu command “Connection Management”.

   In the list “Management of All Connections”, the newly configured call destination appears with the designation “Amsterdam”.

10. Click the “IP Ping” button in the “Action” column.

    A connection to the Amsterdam LAN is established briefly and then cleared.

Step 2:

On all workstations in the network, enter the IP address of the NT/MPRI computer, “192.168.1.3”, as the standard gateway. This ensures that all packets whose call destination address lies outside the local network are sent to the NT/MPRI.

Step 3:

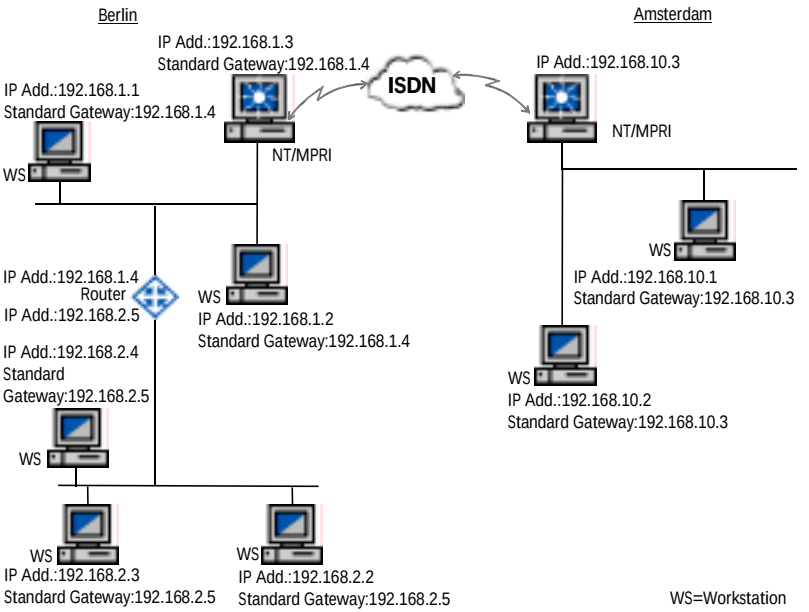
Define a call destination “Frankfurt” on the Amsterdam NT/MPRI and enter the following for “Static Route”: Network address “192.168.1.0”, Mask “24”. Here, too, the standard gateway, i.e., the IP address of the NT/MPRI computer in the local network, must be configured on all workstations.

No additional settings are required in the NT/MPRI in Amsterdam.

Step 4:

Test now whether ping can be transmitted from a workstation in the Frankfurt network to a workstation in the Amsterdam network. If you receive a reply, the network link has been configured correctly.

Example 2
Large Network with Multiple Segments



Large network with multiple segments

For this configuration it is important that the router in the LAN is informed about the networks available over ISDN. If RIP is used in the LAN, the router dynamically learns the routes available from the NT/MPRI. Otherwise static routes must be defined.

Similarly, the NT/MPRI must be informed about the network situated behind the other router in the LAN. Here, too, if RIP is not used, the route must be configured statically.

Step 1:

After installing the NT/MPRI, create a new call destination called “Amsterdam”. Under “Static Route”, enter the following values: network address “192.168.10.0”, mask “24”. This instructs the NT/MPRI to forward all packets with the IP addresses 192.168.10.x to the call destination “Amsterdam”.

Step 2:

If RIP is used no configuration is necessary in this step.

If no RIP is used in the network, first all local network segments must be registered as “Additional Local Routes for IP” in the LAN “Berlin” (“Server Settings / General / IP Routing over the LAN”) so that packets arriving over the ISDN link also can be forwarded to this goal. For each route, enter the network address, the mask, and, under “Next Hop”, the IP address of the local router (in this example: 192.168.1.4”).

On the other router in the LAN, define a route to the network address “192.168.10.0” and enter the IP address of the NT/MPRI computer as the next hop (in the example this is “192.168.1.3”).

Step 3:

Define a call destination “Berlin” on the Amsterdam NT/MPRI. In order for packets from Amsterdam to reach their destination in Berlin reliably, static routes must be defined for all network segments in Berlin. First enter the first WAN route at “Static Route” and then save the call destination. The remaining IP routes are entered in the IP settings (“IP” button).

A simpler solution is to accept the default route (network address 0.0.0.0, mask 0). This means that all packets for destinations outside the local network are sent to the call destination “Berlin” from where the Berlin NT/MPRI computer either delivers them to hosts in its own segments or forwards them to the next router.

Step 4:

Now test whether you can ping a workstation in the Amsterdam network from a workstation in the segment with two workstations. If you get a response, your configuration works.

3.4 Links from Microsoft Networks

As a router the NT/MPRI works independently of the network operating system present in its environment. Only a few NT/MPRI settings concern Microsoft networks directly.

The Microsoft network uses the protocol NetBIOS over IP. This protocol constitutes the foundation for “shares”, or the use of remote drives or network services.

Make the following settings in both LANs:

- Enable “NetBIOS over IP” as a network protocol.
- Configure the local and remote LANs as separate domains. Each domain should have the other entered as a “trusted domain”.
- Use WINS for NetBIOS name resolution by installing a WINS server in each LAN. At each site, enter the remote LAN’s WINS server for replication and set the replication interval to a high value to save ISDN costs. Finally, enter the local WINS server in each workstation’s network settings.
- On the NT/MPRI in each LAN, perform the following steps:
  - Create a new IP call destination.
  - Go to the IP settings of the call destination (“IP” button) and activate “NetBIOS Spoofing”. At the same time, deactivate the “NetBIOS Filter”.
  - Check whether IP routing via ISDN functions correctly, e.g. with “Ping”.

3.5 Connecting to the Internet

The NT/MPRI creates a PPP connection to what is called a PoP (**P**oint **o**f **P**resence) of an Internet provider. The connection between the PoP and your local network is established either via an ISDN dial-in connection, which is established and cleared automatically depending on the amount of data transferred; via an ISDN leased line or an ADSL connection. The NT/MPRI routes the data packets between your local network and the router of your Internet provider.

For connections to the Internet with the NT/MPRI, either access with a dynamic IP address or access with a static IP address can be used.

The connection between the NT/MPRI and the PoP of your Internet provider is generally initiated by the end at which data are awaiting transmission. This is imperative for certain applications like the E-mail server, which use SMTP.

In order for incoming calls to be recognized by your Internet provider, and assigned to a configured call destination, the local router also can require either an “Authentication at Local Site” with PAP or CHAP or the D-channel number transmitted by the remote site.

If the Internet provider requires authentication from your site, simply activate the function “Authentication at Remote Site” in the NT/MPRI. Here, too, the PAP and CHAP procedures are supported.

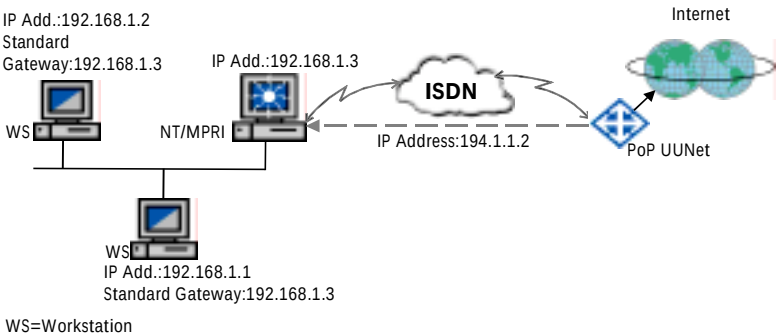
Access with a Dynamic IP Address

Accesses with a dynamic IP address are generally more economical than accesses with a static IP address, as an Internet-compliant IP address is assigned by the Internet provider each time a connection is established. This IP address is supplied to the NT/MPRI during PPP negotiation. In order to guarantee access to the Internet for all computers in the local network, “IP Masquerading” must be activated in the call destination settings. Masquerading is the process of hiding an internal network and mapping all IP addresses in the LAN to a single IP address so that the same IP address is used for all requests from the Internet.

The connection is initiated only by the NT/MPRI.

As an example, this section describes access via UUNet and ISDN as well as UUNet and ADSL. In both cases a dynamic IP address is assigned each time a connection is established to UUNet.

Access via UUNet and ISDN



Connecting to the Internet via access with a dynamic IP address

The following information is required from UUNet:

- telephone number of UUNet
- your user name (PAP/CHAP)
- your password

Step 1:

1. To configure a new call destination as an Internet dial-in connection, select the menu command “Configuration / Call Destinations / New Call Destination / Internet”.

   An input mask with the parameters required for Internet dial-in connections is opened.

2. In the “Destination Name” field, enter “Internet UUNet” as the name of the new call destination. The NT/MPRI call destination is managed using this name.

3. In the “ISDN Number” field, enter the number of UUNet.

4. In the line “Authentication at Remote Site”, enter the user name and password received from UUNet in the fields “Name” and “Password”.

5. At “Inactivity Timeout”, activate the selection “Disconnect after” and enter the value 60 seconds.

6. Save the call destination.

7. Next, select the menu command “Special / Restart Service” and click the “Restart Services” button.

Step 2:

Select the menu command “Connection Management”. In the new call destination “Internet UUNet”, click the “IP” button in the “Action” column.

The connection to the Internet provider is established. Use the browser to visit any Internet sites of interest. Click the “IP” button again to clear the connection.

Step 3:

Configure DNS resolution at all workstations in the network by entering the DNS server of UUNet. Alternatively, enter the IP address of the proxy servers of UUNet in the web browser.

Step 4:

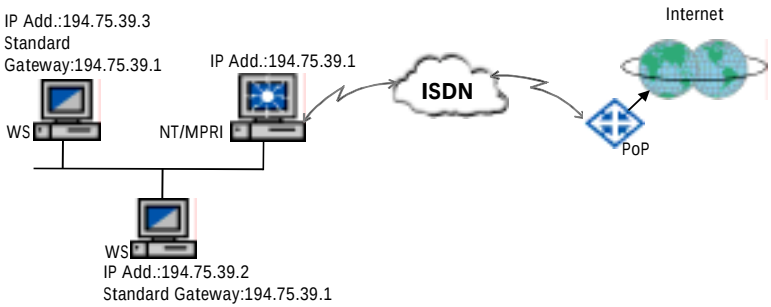
Send a ping from a workstation in the network to the domain name server of UUNet:

```
ping <DNS Server of UUNet> -w 5000
```

If you receive a reply, the connection has been configured correctly.

Access with a Static IP Address

For access with a fixed IP address, generally a fixed IP address range is assigned for your LAN. From this pool of IP addresses, each computer in the network and the NT/MPRI receive a static address.



Connection to the Internet via access with a static IP address

Before configuring the Internet access, the following information is required from your Internet provider:

- IP information like the domain name, domain name server and any E-mail server used
- Internet-compliant IP address range
- telephone number of the PoP
- data for authentication (name, password)

Your Internet provider requires the following information from you:

- the telephone number of your NT/MPRI

Step 1:

Before installing the NT/MPRI, assign the first address from the IP address range to the computer on which the NT/MPRI is to be installed. The other workstations in the network each receive an IP address from the assigned IP address range.

Install the NT/MPRI.

Step 2:

Select the menu command “Configuration / Call Destination / New Call Destination / Internet”. An input mask with the parameters required for dial-in Internet connections is opened.

Configure a new call destination as an Internet dial-in connection with the following information:

Parameter	Action
Name:	Enter “Internet”
Number:	Enter the [Telephone number of the PoP of your Internet provider]
Authentication at Remote Site:	Enter the [Name]
Password:	Enter the [Password]
Inactivity Timeout:	Choose “Charge Profile DT City-Call”

Keep the standard settings for all other parameters.

Save this call destination, re-open it and deactivate IP masquerading. Then restart the NT/MPRI service by selecting “Special / Restart Service”.

Step 3:

Next, enter the following information on all workstations in the network:

- domain name (“Network Settings / TCP/IP”)
- name server used (“Network Settings / TCP/IP”)
- mail server used (browser or mail program)

Internet Access via ADSL

If your system is equipped with an ADSL access, this can be used for access to the Internet.

If the ADSL access is to be used, first check the configuration and make any necessary modifications.

The following information is required from UUNet:

- your user name, composed of the line ID, your telephone number and your co-user suffix
- your password

Step 1:

Open the pre-configured call destination “UUNet over ADSL”. A mask opens in which the pre-configured data can be changed. Check the information and add the following if necessary:

Parameter	Action
Name:	Enter “UUNet over ADSL”
Number:	Enter the [Telephone number the PoP of UUNet]
Authentication at Remote Site:	Enter the [line ID][telephone no.][co-user suffix]
Password:	Enter [UUNet Password of the co-user]
Inactivity Timeout:	Enable “Always after 60 seconds”
Status of this configuration:	Active

The pre-set budget is set to a low monthly value. This value should probably be changed for normal operation. The status of this setting is set to “Only configured, not active”. Set this setting to “Active”.

To ensure that the ADSL access is used when a connection to this call destination is established, the ADSL-Controller must be linked to this call destination. The ADSL-Controller is linked by reserving the PPPoE channel of the ADSL-Controller for the call destination “UUNet over ADSL” under “Configuration / Server Settings / ISDN- and ADSL-Controllers”.

If you have made any changes to the configuration, save them now. Then select the menu command “Special / Restart Service” and click the button “Restart Service”.

Step 2:

Next select the menu command “Connection Management”. In the destination “UUNet over ADSL”, click the “IP” button in the “Action” column.

A connection to the Internet provider is established. Use the web browser to visit any Internet sites of interest. Click the “IP” button again to clear the connection.

Step 3:

Set DNS name resolution on all workstations in the network by entering the DNS server of UUNet. Alternatively, enter the IP address of the proxy server of UUNet in the browser.

Step 4:

Send a ping from a workstation in the network to the domain name server of UUNet:

```
ping <DNS Server of UUNet> -w 5000
```

If you receive a reply, the connection has been configured correctly.

3.6 Settings for Routing

The following section explains which routing protocols of the NT/MPRI should be used and what to keep in mind when assigning these protocols to the call destinations.

IP Settings

The NT/MPRI uses the routing protocol RIP2 in the LAN and static routing over ISDN. This prevents frequent calls for the purpose of exchanging RIP packets over ISDN.

When configuring a call destination, select via RIP2 whether the static route to this call destination should always be known to the LAN or whether it is to be reported after a logical ISDN connection is established. In the first case, a logical ISDN connection is established by any packet intended for a call destination outside of the LAN. In the latter, packets only can be sent to a call destination when a logical ISDN connection to this call destination exists and the route thus is known in the LAN.

IPX Settings

For IPX, the NT/MPRI uses dynamic routing with IPX RIP and SAP in the LAN and over ISDN. RIP/SAP is exchanged the first time a logical connection is established over ISDN and made known to all possible routes in the network. RIP/SAP is used as long as a logical ISDN connection exists.

In order to keep costs at a minimum for such connections, the NT/MPRI is configured by default to send RIP/SAP only when changes occur in the call settings (“Call Destination Configuration / RIP/SAP Updates: Only On Change”). Do not change this setting.

Static routes to NetWare servers in a remote network also can be defined over ISDN (“Call Destination Configuration / IPX / IPX Routes for this Call Destination”). This has the advantage of always advertising the remote server in the local network, even when no logical ISDN connection exists. When data packets are queued for transmission, the physical ISDN connection is set up automatically.

3.7 Configuring Call Destinations: Fine-Tuning the Settings

The following section primarily discusses the configuration of call destinations for dial-in connections with regard to cost reduction, security and network protocols used. Comprehensive information about leased lines is available in the chapter “Special Settings”.

Reducing Connection Costs

This section discusses the many functions and mechanisms the NT/MPRI offers to reduce connection costs.

Automatic Disconnect for Idle ISDN Connections

The NT/MPRI distinguishes between logical and physical ISDN connections. Only for an active physical connection is a B channel in use and charges incurred.

A physical ISDN connection must not be maintained for the entire period between establishing a connection and disconnection by the remote site. Compared with analog networks, ISDN offers such fast connection times that idle physical ISDN connections can be cleared and re-established quickly to reduce costs. In most cases, the transmission of useful data over ISDN is sporadic at best. Even when the physical connection is cleared, the logical connection can remain active. As long as a logical connection is maintained, connection parameters such as spoofing (see below) remain active.

For an ISDN connection to be maintained logically but cleared physically, the remote site must be equipped with a router that supports the concept of a logical connection and can re-establish the physical ISDN connection as needed.

The “Disconnect Timeout” and “Inactivity Timeout” can be set for each call destination in the NT/MPRI. The “Inactivity Timeout” is the length of time after which an idle physical connection is cleared; the “Disconnect Timeout” is the length of time without transmission activity for which a logical connection is maintained. These settings are entered in the configuration of the call destination.

Special Filters and Spoofing Mechanisms

Special filters and “spoofing” mechanisms prevent network packets which contain information for network protocols and/or operating systems, but no data of interest to the user, from being transmitted over ISDN. In the local network such packets are no problem, but transmission over ISDN would entail significantly higher connection costs.

Special Filters: A number of applications constantly exchange packets, often leading to frequent and superfluous connection setups. For this reason the NT/MPRI contains a number of special packet filters for TCP/IP and IPX/SPX which are activated by default. For instance, SNMP traps can be filtered out by SNMP filters for IP or IPX to prevent frequent ISDN calls.

These filters can be activated and deactivated in the call destination settings (“IP” and “IPX” buttons).

Spoofing Mechanisms: In Microsoft networks, NetBIOS packets are exchanged at regular intervals once a client has logged on to a Windows XP/2000/NT server. This traffic cannot be simply filtered out by the NT/MPRI, since this would interrupt the client-server connection. The NT/MPRI therefore answers such packets locally, simulating a response from the client. In this way the NT/MPRI supports spoofing of NetBIOS session keep-alive packets and SMB echo packets (SMB in NetBIOS).

In the NetWare environment too, certain types of packets which are exchanged between NetWare clients and servers, or the server/host part of distributed applications, require an acknowledgement from the remote station. If these packets were simply filtered out, the communications link between the client and the host of a service or application would no longer function.

Example: If Watchdog packets which a NetWare server sends to a client for confirmation were simply filtered out and not acknowledged locally by the NT/MPRI, the NetWare server would assume that the client is no longer connected. Thus the server database designates the client as non-existent, even though it is still logically connected.

When spoofing is used in Novell NetWare environments, the NT/MPRI locally answers the packets sent to a remote client by the host part of a service or application, such as the IPX watchdog packets sent by the NetWare server or the SPX watchdog packets sent by the host part of an application.

When an ISDN connection has been set up and spoofing negotiated between the two systems, the spoofing is performed for the entire duration of the logical connection.

Spoofing must be supported and activated at both ends of the connection.

Thresholds and Budgets

To control ISDN costs the NT/MPRI offers the option of setting limits on ISDN charges and on the number of outgoing calls.

These limits are defined using the command “Configuration / Server Settings / Thresholds”. These settings are valid for the entire router and serve to limit global maximum values on ISDN charges (Budget), the duration of physical connections and the number of outgoing calls (including failed attempts and D-channel signaling). The limits set here apply to all outgoing dial-up connections of the NT/MPRI and are designed to prevent unexpected ISDN connection costs. When a global threshold is reached, the NT/MPRI clears down all existing outgoing physical connections and blocks all further outgoing calls.

An individual budget may also be specified for each call destination. A call destination budget specifies the maximum charges per day, week or month which may incur for connections to this destination. It is not necessary to enter all three values. As soon as the charges calculated by the NT/MPRI exceed one of the configured budget limits, the physical ISDN connection is immediately cleared down, and further calls to the call destination (including D-channel signaling) are blocked. The logical ISDN connection is not automatically cleared down, however: if packets need to be transmitted to the call destination, as many attempts are made to dial up the physical connection as you specified under “Redialing”.

If charge information is received from your ISDN line or PBX extension during the connection (in accordance with the European standard AOCD = **A**dvice **O**n **C**harge **D**uring Call), the NT/MPRI uses this information to calculate the charges incurred and compares the result with the configured limit. If your ISDN line or PBX extension does not communi-

cate charge information, you should select a charge profile for estimating charges. Then the charges incurred are estimated based on connection time. This estimate is compared with the configured limit.

New charge profiles can be created and added using the "Special / Charge Profiles" command.

To re-enable outgoing connections after a global or call destination limit has been reached, increase the configured limit.

Access Protection and Security Mechanisms

The NT/MPRI provides a multi-stage security concept which reliably prevents unauthorized access to the local network.

The security functions can be configured at various levels:

- globally for the entire router (CLI number check, global IP filters)
- individually for specific call destinations (authentication, destination-specific IP filters, IP masquerading/NAT)

Comprehensive information about global and destination-specific IP filters is presented in the section "IP Filters (Firewall)" on page 53.

The various functions and concepts are presented below along with tips for configuration.

CLI Number Check

To protect the network against unauthorized access, the NT/MPRI offers the option of checking the CLI number (transmitted on the D channel) against the list of numbers authorized to dial in.

To use this feature, select the menu command "Configuration / Security / CLI Number Check" and set the option at the line "Activate CLI Number Check" to "Yes". Then enter for each call destination the CLI number transmitted on the D channel. If CLI numbers already were defined during configuration of the call destinations, these numbers are listed here.

If a remote router has a B channel pool and dials in from various numbers, you must enter all the CLI numbers of the pool.

The CLI number of each incoming call is checked against the numbers defined in the CLI number database. If the number is listed the incoming call is provisionally accepted, subject to further security mechanisms.

PAP or CHAP Authentication

For each call destination you may require that the remote site authenticate itself to the local router (“Authentication at Local Site”). This authentication is performed in accordance with the PAP and CHAP protocols (RFCs 1334 and 1994, respectively). Both procedures require the configuration of a name and password.

In PAP authentication, the name and password are transmitted in plain text, and the local site checks whether these match its own settings. If so, the call is accepted.

Under CHAP, the remote site uses a defined encryption algorithm to generate a message from the name and a random value, and sends the message to the local site. The local site generates a new value from the message and the password, also using a predefined algorithm, and sends this message back. The remote site then checks whether the value it produced from the original message and password agrees with the value sent back by the local site. If so, the call is accepted.

If the remote site also requires authentication, the name and password received from the administrator of the remote site can be entered in the call destination settings (“Authentication at Remote Site”).

Authentication also serves to identify the remote site when the CLI number check is not activated.

Security Call-back

In order to further increase LAN access security, a security call-back can be required for each call destination in accordance with the LCP Extensions (RFC 1570) or the Draft RFC “PPP Call-Back Control Protocol”. This is specified in the call destination settings.

The call-back takes place after the call has been accepted and after PAP/CHAP authentication, should one of these protocols be activated. The number dialed for the security call-back is the one entered in the call destination settings.

When a logical ISDN connection remains active after an inactivity timeout, the security call-back is repeated each time the physical connection is restored.

IP Masquerading/Network Address Resolution (NAT)

IP masquerading fulfills two important functions for Internet connections: protection from undesired external access and the mapping of all IP addresses in the LAN to a single, Internet-compliant IP address.

With IP masquerading, one “official” IP address is sufficient for all communication between a private LAN and the public Internet. The NT/MPRI processes the IP addresses in the TCP, UDP and ICMP packets such that only one IP address is visible to the Internet. Hosts in a private LAN thus can continue using their internal (“unofficial”) IP addresses for communication with the Internet. A system shielded in this manner is significantly more difficult to break through than a packet-filter firewall.

The NT/MPRI automatically updates its internal IP address translation table upon outgoing TCP and UDP connections. Dynamically generated port or ICMP sequence numbers are used to map the private LAN host unambiguously. FTP also is supported fully with IP masquerading.

IP masquerading is activated in the IP settings of a call destination (“IP” button).

Although classical IP masquerading only permits outbound TCP connections from the local network, the NT/MPRI can extend masquerading, if desired, so that incoming TCP, UDP and ICMP connections are forwarded to certain hosts in the LAN. For this the NT/MPRI uses “Masquerading Profiles”, fixed rules for bidirectional mapping of external IP address/port combinations to internal IP addresses and ports. If the port is specified as “0”, then static Network Address Translation (NAT) is performed in accordance with RFC 1631.

Masquerading Profiles are configured at “Configuration / Security / IP Masquerading/NAT”. In the IP settings of a call destination, click the “IP” button to select a configured profile.

In this way the NT/MPRI can forward incoming E-mail (SMTP) to specified hosts in a private LAN.

Incoming Calls

The NT/MPRI only accepts calls from “known” remote sites, i.e., those sites for which call destination settings have been configured.

The NT/MPRI assigns an incoming call to a local call destination based on one of the following methods:

- The CLI number (CLIP=**C**alling **L**ine **I**dentification **P**resentation)

  Prerequisite for this method is that the caller’s number is transmitted over the D-channel. This service must be requested from and enabled by your ISDN provider. In addition, a call destination must be associated with this CLI number. This is ensured either by

entering the number directly in the Call Destination settings (at the parameter “CLI Number for Assigning Incoming Calls”) or in the CLI Number Check configuration (“Configuration / Security / CLI Number Check / Authorized Numbers for Dial-In”).

Call identification by CLI number is necessary whenever “Allocate Costs to Local Site” or “Security Call-Back” has been activated in any call destination configuration.

Some remote sites may dial in from multiple ISDN lines configured as a B-channel pool. In this case you must enter all of the CLI numbers of the remote pool (“ISDN” button in the Call Destination settings).

- PAP or CHAP authentication information, which the remote site must send when a connection is established on the ISDN B channel if so required in the Call Destination settings.

  For this purpose the option “Authentication at Local Site” by PAP or CHAP must be activated in the local settings and a name and password assigned to the Call Destination. Only the Call Destination Name is used to identify the incoming call.

Both the call destination name and the CLI number must be unique. In other words, no two call destinations may use the same name or CLI number.

4 Special NT/MPRI Settings

This chapter contains information on NT/MPRI settings which are not necessary for smooth operation or which apply only to certain types of applications.

First the variety of filters that can help you protect your network against unauthorized access is discussed. Later in this section you will find instructions for using the NT/MPRI with leased lines.

4.1 Filters

Filters are used both to prevent unauthorized intrusion into the network—from the Internet, for example—and to select which data and services are available for access from outside the LAN. This selective access also helps to minimize connection costs. The NT/MPRI offers extensive filtering options in the “Security” menu.

The various filter options for IP and IPX are explained in more detail in the following section.

IP Filters (Firewall)

The NT/MPRI offers the following packet filtering instances for your IP network: global input and output filters, destination-specific input and output filters, and the forwarding filter. In each of these instances rules can be set to define how the NT/MPRI handles incoming and outgoing packets and packets to be forwarded to other networks. The possible actions in each case are “Deny”, “Reject” or “Accept”. Thus communication can be limited to certain specified stations. The use of certain services, like “WWW” for access to the World Wide Web, can also be limited to specified stations in the network.

Because filters definitions are constructed of multiple instances, they provide extremely flexible and far-reaching protection. The kind of packet filtering in the NT/MPRI is one approach to constructing what is known as a firewall, a protective screen around your network.

The filter instances of the NT/MPRI have the following duties:

- Destination Input Filter: checks packets arriving at the NT/MPRI from a certain call destination over ISDN.
- Destination Output Filter: checks packets about to be sent from the NT/MPRI to a certain call destination.

- Global Input Filter: checks packets arriving at the NT/MPRI from any direction (from the LAN or from ISDN).
- Global Output Filter: checks packets about to be sent from the NT/MPRI in any direction (to the LAN or to ISDN).
- Forwarding Filter: checks all packets being forwarded in the NT/MPRI from one network to another (e.g. from the LAN to a remote destination network or from one remote network to another).

An illustration of the various filter instances is presented from page 53.

Filters and Rules

A **filter** is composed of the following components:

- An ordered sequence of rules.
- A default action which is performed on all packets for which no rule in a profile applies.
- A logging instruction for packets handled by this rule. Log information is used primarily to record attempts to “break into” the LAN and, if possible, to trace the culprit.

Rules always consist of the following components:

- A description of the packet type to which the rule applies. This description entails three criteria which the NT/MPRI uses to check whether the rule applies to a packet:
  - Service: here you can specify all IP services, only certain services (such as ftp or telnet), or just specific actions (such as ftp access to the LAN from the Internet) as criteria.
  - Source of the packet: defined as a particular network or a concrete host address.
  - Destination of the packet: defined in the same way as the source.
- One of three actions to be performed on packets to which the rule applies:
  - Accept: the packet is sent to the destination address specified in the header or passed to the next filter.
  - Deny: the packet is not sent on, but simply discarded.

– Reject: the packet is not sent on. The error message “Destination not reachable” is sent back to the source address.

Each packet is compared with the criteria of each rule in succession until the first rule is found which applies to it. If the applicable action is “Deny” or “Reject” the filtering process for this packet is concluded.

If no rule applying to this packet is found, or if the default action is “Accept”, the packet is sent on to the next filter instance.

Bear in mind the two following aspects when creating a filter:

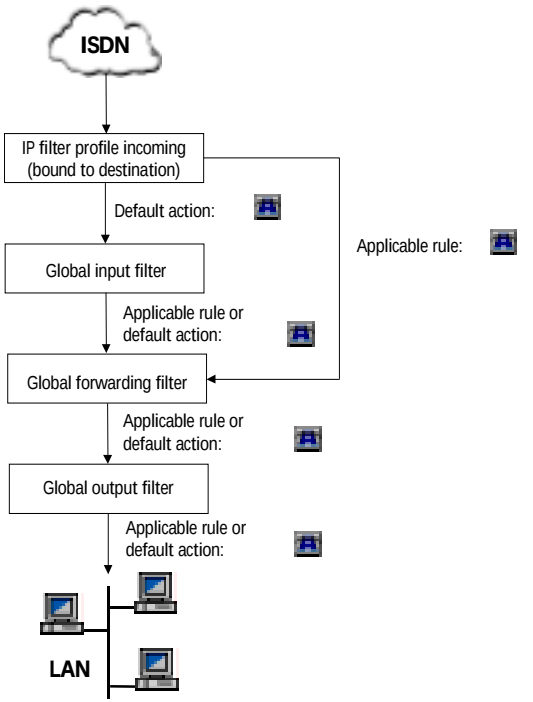
- A filter profile always handles all packets (the rules apply to certain packets and the default action to all others).
- The sequence of the rules is extermely important! It is essential that more general rules be placed toward the bottom of the profile. Otherwise, more specific rules that are located lower down in the hierarchy would never be applied.

The basic principle should be applied when designing a filter profile: handle minority cases first.

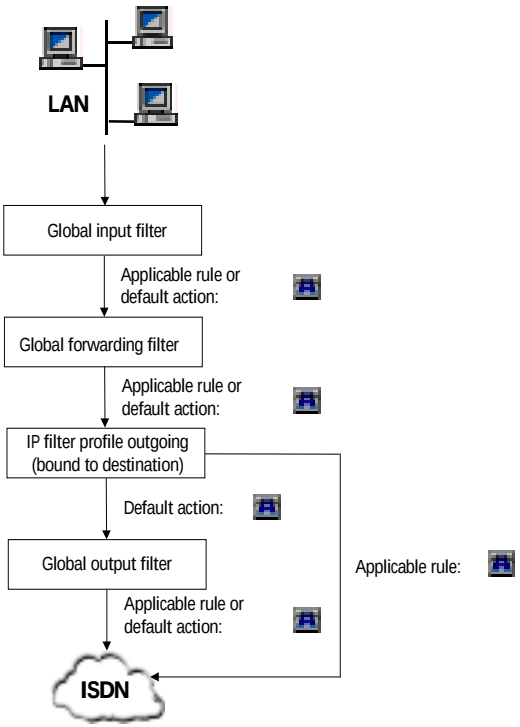
A simple example: Suppose only call destination A is to be granted access to computer B in the LAN. To set this condition, define the following two rules in the global input filter:

1. A is granted access to computer B. Thus the first rule states: accept packets for all services which have the IP range of A as the source and B’s IP address as the destination.
2. No one (i.e., no one else) is permitted access to the computer. Thus the second rule states: deny packets for all services which have any IP address and are addressed to the IP address of B.

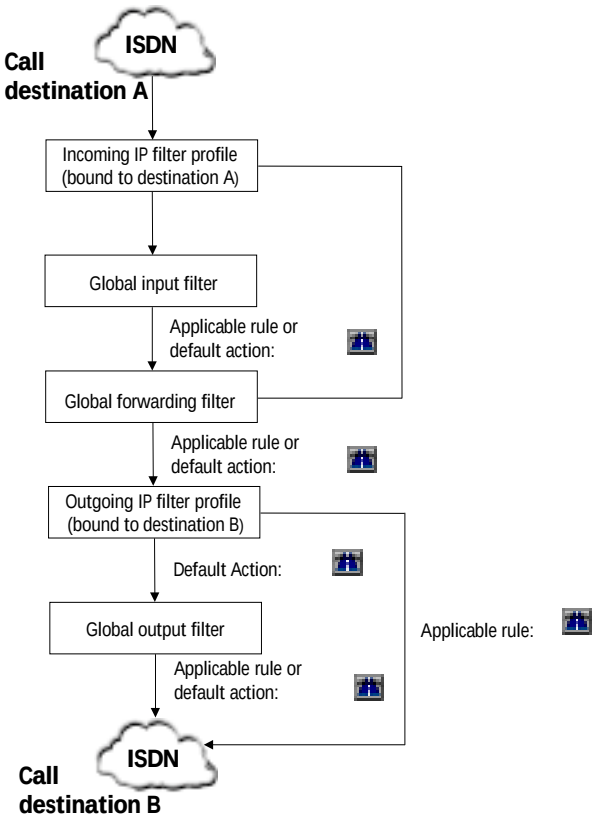
The illustrations below show the order in which the filter instances are applied for incoming and outgoing packets and those forwarded over ISDN to another network. It is assumed that all filter instances are enabled and that the applicable or default rule for the packet in the example is “Accept” so that the longest possible packet path is illustrated:



Example of incoming packets: packet arrives via ISDN from a remote network; destination address is in the LAN



Example of outgoing packets: packet arrives from the local network; destination address is in a remote LAN connected over ISDN



Packet Forwarding Example: a packet arrives via ISDN from a remote network (Call destination A); its destination address is in another remote network connected via ISDN (Call destination B)

Examples for IP Filter Profiles

The pre-defined IP filter profiles “Internet incoming” and “Internet outgoing” can be used for standard Internet access. Profiles can also be adapted to meet your needs, however. To distinguish the direction of the connection request, TCP flags also can be taken into account. Please see the recommended reading in the section “Additional Literature” from page 109.

These profiles can be used without modification for a standard Internet connection. They will protect your network reliably from outside access, while allowing users in the local network to access Internet servers. The two profiles can be used in the scenarios described above, for example.

In the filter profile "Internet incoming", a number of rules have the statuts "disabled" while others are "enabled". All rules which prevent access to your LAN initiated from outside are enabled. Rules that are "disabled" are pre-configured for cases in which such services as the company ftp server, web server or e-mail server are to be made available for access from the Internet. To allow outside access to such additional services, the filter profile must be edited accordingly before it is selected in the configuration of your Internet call destination.

Note the following for both of these lists:

- All the rules in both profiles have been created with the broadest possible criteria for the descriptive categories "Source" and "Call Destination": the source of the packet can be any host (the criterion for the source in each rule is thus: 0.0.0.0 / 0), as can the call destination (destination criterion in each rule is thus: 0.0.0.0 / 0). For the sake of legibility this information was not repeated for each rule in the following list.
- All rules contain the entry "No Log". This information also has been omitted from the list for better legibility.

The rules in both profiles are portrayed and explained below.

IP Filter (Firewall), Destination Filter Profile "Internet incoming"			
Profile enabled Name Action if no rule applies	Yes Internet incoming Deny		
Rules			
Status	**Service/Source/ Destination**	**Action/Log**	**Explanation**
Disabled	WWW Connection Setup	Accept	Enable this rule if you make your own web server available.
Disabled	FTP Connection Setup	Accept	Enable this rule if you make your own ftp server available.
Disabled	SMTP Connection Setup	Accept	Enable this rule if you use SMPT rather than your Internet provider's POP3 service to deliver e-mail to your mail server.
Disabled	DNS (Name Server) Requests	Accept	Enable this rule if you administer your Internet domain via your own name server or have set up a secondary name server.
Disabled	DNS (Name Server) Zone Transfer	Accept	Enable this rule if you administer your Internet domain via your own name server and have set up a primary name server.
Disabled	NNTP Connection Setup	Accept	Enable this rule if you have the news delivered to you by NNTP rather than accessing the ISP's news server.
Disabled	Network Time Protocol	Accept	Enable this rule to synchronize your system time with the time of your ISP using the Network Time Protocol.
Disabled	UUCP Connection Setup	Accept	Enable this rule if your ISP sends you data via UUCP (e.g. news or e-mail).

Status	Service/Source/ Destination	Action/Log	Explanation
Disabled	Telnet Connection Setup	Accept	Enable this rule to allow access to your station via Telnet (for example, if UNIX computers are to be administered remotely).
Disabled	SSH Connection Setup	Accept	Enable this rule to allow access to your station via SSH (Secure SHell) (for example, if UNIX stations are to be administered remotely).
Disabled	TCP/UDP “echo” Port	Accept	This allows the function “traceroute” (UNIX) or “tracert” (Windows XP, Windows 2000, Windows NT, Windows 95, DOS) to be used on your network from outside. These functions trace the route a packet must follow to reach your network from outside. No security risk is entailed. It is common to enable the use of this function for outside use, so that an outside user can establish that a web server addressed is not currently accessible (because the route is missing, the server is deactivated, etc.).
Enabled	RIP Packets	Deny	This ensures that the NT/MPRI only knows the routes that you have set up. RIP information from the Internet is not forwarded. This prevents “man in the middle attacks” on this router: smuggling in routing information to corrupt your routes.
Enabled	NetBIOS Packets	Deny	This ensures that no access to your Windows XP/2000/NT resources (drives, printers, etc.) is possible from the outside.

Status	Service/Source/ Destination	Action/Log	Explanation
Enabled	FTP Data Connection Setup	Accept	This ensures that your users can copy data from the Internet via ftp. Note: this rule can be disabled if all FTP clients in your network use the “ftp-PASV” option.
Enabled	TCP Packets	Accept	This ensures that reply packets from connections you initiated arrive in your network.
Enabled	ICMP Packets	Accept	This ensures that error messages from the Internet are reported back to your station. Such reports are returned with the ICMP service if a station addressed in the Internet is inaccessible.
Enabled	All Packets	Deny	Everything that manages to make it to this point can only be interpreted as an intrusion attempt: for example, tunnel packets packaged in IP or routing packets like OSPF or EGP packets. These packets also are denied access by the default action, however. This rule was set up so that an intrusion attempt can be reproduced if desired. In this case, enable the logging function.

Filter profile “Internet incoming“

IP Filter (Firewall), Destination Filter Profile “Internet outgoing”			
Profile enabled	Yes		
Name	Internet outgoing		
Action if no rule applies	Accept		
Rules			
Status	**Service/Source/ Destination**	**Action/Log**	**Explanation**
Enabled	RIP Packets	Deny	This ensures that no one from the outside knows your network.
Enabled	NetBIOS Packets	Deny	This filter exists in two forms (in the filter profile and as a “Special Filter”). It ensures that your XP/2000/NT resources (drives, printers, etc.) are not advertised to the outside. Packets such as these generally would only make it as far as the ISP, but this rule still should be included in a comprehensive filter set.

Filter profile “Internet outgoing“

IPX RIP/SAP Filters

For the IPX protocol, access to specific routes and network services can be regulated by RIP/SAP filter rules. Both global and destination-specific RIP and SAP filters can be configured. These filters allow your IPX network to be filtered completely, so that it becomes “invisible” either to all outside users or to a specified call destination. It is also possible to filter certain services such as local printer servers.

The RIP protocol (**R**outing **I**nformation **P**rotocol) allows routers to exchange routing table information. By filtering these packets, it is possible to restrict access to particular routes and thus to networks. If some RIP packets arriving at the router from the local network can be discarded (by the RIP input filter), then the information in the router’s RIP table can be reduced to the bare essentials.

The SAP (**S**ervice **A**dvertising **P**rotocol) is used by servers to advertise their services and addresses in a network. Filtering SAP packets can restrict access to certain services such as printers or file servers. If some of the SAP packets arriving at the router from the LAN can be discarded (by the SAP input filter), then the information in the router's SAP table can be reduced to the bare essentials.

Every incoming and outgoing RIP/SAP packet is checked by the RIP/SAP filters for a matching filter rule.

The following filters exist:

- **RIP input filter**: a filter for incoming RIP packets (from the LAN or a call destination to the router).
- **RIP output filter**: a filter for outgoing RIP packets (from the router to the LAN or a remote call destination).
- **SAP input filter**: a filter for incoming SAP packets (from the LAN or a call destination to the router).
- **SAP output filter**: a filter for outgoing SAP packets (from the router to the LAN or to a call destination).

4.2 Leased Lines

Two different kinds of leased lines can be configured to work with the NT/MPRI:

1. Static leased line

   On this kind of leased line, connections are established using a specified number of B channels. It is not possible to add B channels. The number of B channels is defined in the configuration of the leased line.

2. Dynamic leased line

   On this kind of leased line, additional B channels can be added dynamically depending on the load transmitted over the connection. The B channels are added in the form of dial-up connections.

In both cases, the configuration of a leased line requires both settings on the ISDN adapter and a new call destination setup.

The next two sections describe the configuration of both of these types of leased lines.

Configuring a Static Leased Line

The following settings are required for the example configurations described in this section:

- Create a “New Leased Line” as a call destination
- Configure the leased line D64S (1*64 K) for Controller 1 and reserve the first B channel for the newly created call destination.

Controller Settings

1. Make sure that the DSS1 driver for the ISDN-Controller to be used by the leased line is installed.
2. Use the “Configuration / Server Settings / ISDN- and ADSL-Controller” menu command in the NT/MPRI Manager to select the ISDN-Controller intended for the leased line.

   If the line is an ISDN BRI, activate the “Leased line” option and select the desired line type from the adjacent list.

   If the line is an ISDN PRI (primary rate access), activate the “Primary rate interface” option and save the settings.

ISDN-Controller 1 configured for a leased line

Configuring a Call Destination for the Leased Line

1. Select the input mask “Without Profile” from the “Configuration / Call Destinations / New Call Destination”.

2. Activate “Leased line” at the upper right of the input mask to access the mask specific for leased lines. Make the settings listed in the table. Parameters which are not listed in the table keep their default values. If no default setting is entred, no entry is necessary.

Parameter	Action
“Name”	Enter an unambiguous name for the leased line
“Authentication at Remote Site”: “Name”	Enter the name of the local NT/MPRI station (server name)
“Authentication at Local Site”: “Name”	Enter the name of the router station at the remote site
“For Leased Line use”	Enter the ISDN-Controller to be used and configured for the leased line
“IP”	Enable
“Static Route”: “Network address”, “Mask”	Enter the values for the network to be accessed at the remote site (e.g. “192.168.10.0” and “24”)
“NetBIOS Spoofing”	Enable “Negotiate”
“NetBIOS Filter”	Enable “Not active”

3. Save the destination.

Testing and Configuring the Static Leased Line at the Remote Site

1. Restart the NT/MPRI service (“Special / Restart Services”).
2. Start tracing packets by selecting “ISDN/ADSL-Controller / Network Adapter” in the “Monitor / Trace Packets” menu and clicking the “REC” button.
3. As the LQRP packets (**L**ine **Q**uality **R**eport **P**rotocol) are sent constantly, these must be visible in the session recording.

```
1. 28.04.2000 23:09:55.000 Festverbindung PPP >>> 22/22 Normal
   LCP 012#17:ConfReq LQRP(1000) MAGIC(80393BE4)
   0000  FF03C021 01170012 0408C025 00000E68 05068039  ...!.......%.......9
   0014  3BE4                                          ;.

2. 28.04.2000 23:09:57.003 Festverbindung PPP >>> 22/22 Normal
   LCP 012#18:ConfReq LQRP(1000) MAGIC(80397B1D)
   0000  FF03C021 01180012 0408C025 00000E68 05068039  ...!.......%.......9
   0014  7B1D                                          x.

3. 28.04.2000 23:09:59.014 Festverbindung PPP >>> 22/22 Normal
   LCP 012#19:ConfReq LQRP(1000) MAGIC(803A4E77)
   0000  FF03C021 01190012 0408C025 00000E68 0506803A  ...!.......%.......:
   0014  4E77                                          Nw
```

Example for three LQRP packets

4. Configure and test the leased line at the remote site in exactly the same way, but with the ISDN cable disconnected.

5. Re-establish the physical connection by re-connecting the ISDN cable at the remote site. Now the PPP connection should work. If not, even though LQRP packets were sent on both sites (while the ISDN cable was disconnected), contact your ISDN provider for assistance.

Input mask for a static leased line with example data

Configuring a Dynamic Leased Line

The following settings are required for the example configurations described in this section:

- Create a “Dial-up Connection” with an additional static B channel and two additional dynamic B channels
- Configure the leased line D64S2 for one controller and reserve both B channels for the newly created call destination.
- Configure the line type “Primary Rate Access” for a second network adapter.

Configuring the Dial-up Connection

1. Select the input mask “No Profile” from the “Configuration / Call Destinations / New Call Destination”.
2. Make the settings specified in the table. Parameters which are not listed in the table keep their default values. If no default setting is entred, no entry is necessary.

Parameter	Action
“Name”	Enter an unambiguous name for the leased line
“Authentication at Remote Site”: “Name”	Enter the name of the local NT/MPRI station (server name)
“Authentication at Local Site”: “Name”	Enter the name of the router station at the remote site
“IP”	on
“Static Route”: “Network address”, “Mask”	the values for the network to be accessed at the remote site (e.g. “192.168.10.0” and “24”)
“NetBIOS Filter”	Enable “Not active”
“Channel bundling”: “Additional static B channels”	Select the value 1 B channel
“Channel bundling”: “Additional B channels on Demand”	Select the value 2 B channels
“Max. Number of B channels”	Select the value 4 B channels

3. Save the destination.

Controller Settings

1. Make sure that the DSS1 driver for the ISDN-Controller to be used by the leased line is installed.
2. Use the “Configuration / Server Settings / ISDN- and ADSL-Controllers” menu command in the NT/MPRI Manager to select the ISDN-Controller intended for the leased line.
3. Activate the “Leased line” option and select from the list the line type “Digital 64S2 (2*64K)”.
4. Reserve the first and second B channels for the newly created dial-up connection and save your settings.
5. Select an additional ISDN-Controller from the “Configuration / Server Settings / ISDN- and ADSL-Controllers” menu in the NT/MPRI Manager and activate the option “Primary-rate Access”. Save your settings.

Configuring a Dynamic Leased Line at the Remote Site

Now configure the dynamic leased line at the remote site in exactly the same way as you did for the local site.

4.3 Reserving B Channels

The B channels of the ISDN-Controllers used by the NT/MPRI are grouped in a pool and shared among all call destinations. This makes for extreme flexibility and allows optimum utilization of the available channels. The connection setup is also independent of specific ISDN B channels. ISDN leased lines and ADSL connections are exceptions to this, as their call destination settings link them to a certain ISDN-Controller and to a certain B channel/time slot.

At any given time there may be more logical ISDN connections to remote destinations than there are ISDN B channels available. This is possible because the inactivity timeout automatically clears down idle physical ISDN connections, freeing the B channels they occupied in the NT/MPRI for use by other call destinations. The physical connection is restored as soon as packets are requested from or queued for the remote system.

If the majority of the call destinations have been configured to maintain a logical ISDN connection after an inactivity timeout, then the system administrator must make sure that enough B channels are always available (clear logical connection later then physical or never).

For this situation the NT/MPRI also offers the following features to ensure that “important” connections are not obstructed, even when few B channels are available:

- B channels can be reserved for certain call destinations, such as a certain company office, in the ISDN-Controller settings (“Configuration / Server Settings / ISDN-Controller”). These B channels are then removed from the pool of shared channels.
- Call destinations can be assigned a priority level in the call destination settings (high, normal, low). This ensures that high-priority connections will always find a B channel available. If all B channels are busy when a connection is requested, a lower-priority connection is cleared down.

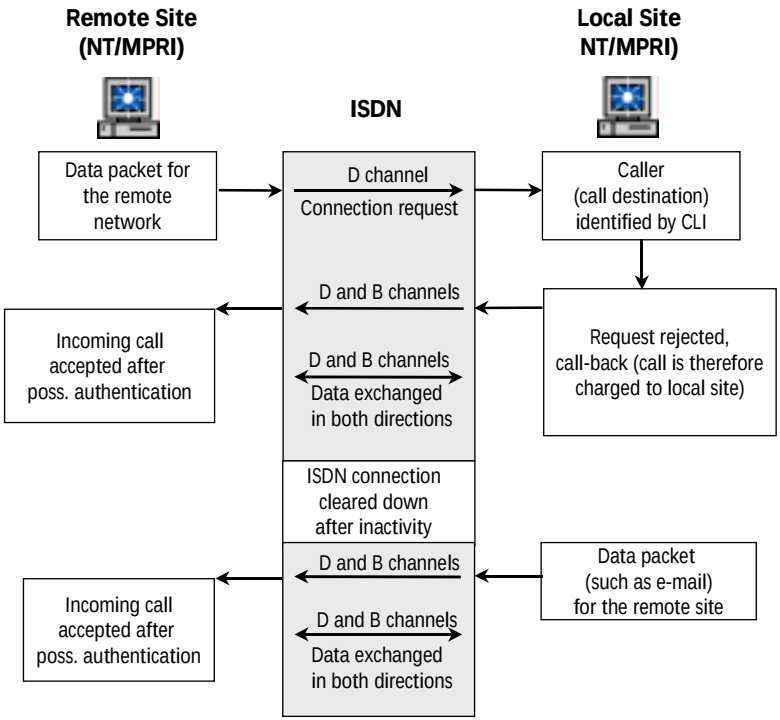
4.4 Cost Assignment (COSO)

The ISDN feature “D-channel Signaling” is provided free of charge by most ISDN providers and is used in the NT/MPRI for cost assignment (COSO = **C**harge **O**ne **S**ite **O**nly).

With this function you can specify which end of the link bears the connection charges. For each call destination this may be the local site, the remote site or whichever site initiates the connection.

Because COSO is a feature for ISDN and not yet incorporated into a PPP standard, the remote router must also support this function. Remote sites equipped with the NetWare® MultiProtocol™ Router for ISDN 3.1 by AVM, for instance, allow COSO.

The following figure illustrates how an incoming call is handled when cost allocation is set to the “Local Site” (NT/MPRI bears the connection charges):



Incoming call handling when cost allocation is set to "Local Site"

4.5 Access Time Restrictions

To regulate LAN access by time of day and day of the week, time profiles can be defined using the menu command "Special". The restrictions defined here then can be assigned to individual call destinations in the call destination settings. For example, a time profile that permits access only on weekdays during business hours can be assigned to all branch offices. Access outside the specified times is then denied.

4.6 Data Encryption

The NT/MPRI allows data encryption to protect data packets from unauthorized access during transmission.

Data are encrypted on the level of the transport protocol (PPP). Encryption on this level is based on the RFC standard, making it interoperable for all transmissions using PPP over ISDN. The advantage of this method is that data compression also takes place on this level, so that data can be compressed first and then encrypted.

Data are encrypted with the Twofish algorithm. The Twofish algorithm encrypts symmetrically in accordance with the Secret Key procedure. Here “symmetrical” means that the same key is used to encode and to decode the data. Only the sender and the recipient know the secret key.

The key has a length of 128-256 bits. Because it is generated when a connection is established, it is known to the sender. Transmission is necessary to make it known to the recipient. Because the key must remain secret on the way from the sender to the recipient, it is encrypted as well. Because the key is encrypted using a separate application which is not a component of the NT/MPRI, it can be adapted to your individual needs. The NT/MPRI can access external routines which encode the key over the Crypt Provider API. An example application illustrating this procedure is included on the NT/MPRI CD.

4.7 IP Masquerading at the Network Adapter

IP filter profiles and masquerading profiles can be activated for each of the network adapters used by the NT/MPRI in the “Configuration / Server Settings / Network Adapters” menu. Using these profiles make sense when the NT/MPRI connects via network adapter to an IP network that offers insufficient security mechanisms, for instance, to the Internet. The NT/MPRI also uses a network adapter to connect to the Internet via ADSL, but in this case a PPPoE channel is established. This means that the only way to activate filter and masquerading profiles is by configuring the settings for the ADSL destination accordingly.

5 Connection Management and Monitoring

For administrators it is especially important to be able to supervise the NT/MPRI in operation. A great number of functions are available for this purpose. Moreover, the NT/MPRI's HTTP management interface allows these functions to be accessed from any PC in the network.

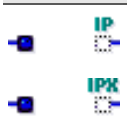
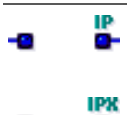
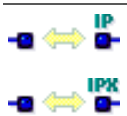
5.1 Connection Management: Setting up and Clearing Down ISDN and ADSL Connections

The "Connection Management" page lists the current ISDN and ADSL connections of the NT/MPRI along with their status. Various commands can be carried out here, depending on the connection status.

Connections to all call destinations with the status "Enabled" are included in the list.

In addition to the call destination's name, number, current connection status and possible actions, this page also displays various configuration and statistical information about the connection.

The following status icons are used:

Icon	Status
	No entry exists for this call destination in the NT/MPRI routing table, i.e., there is no known route to this call destination. The NT/MPRI can not dial up a connection to this destination automatically, but a connection can be set up manually.
	The routing table includes an entry for this call destination, i.e., the route to this call destination is known. The NT/MPRI will dial up the connection automatically whenever data transmission is desired.
	A logical connection exists to this call destination. The physical connection was cleared by the NT/MPRI due to an inactivity timeout.

Icon	Status
 	A logical and physical ISDN connection exists to this call destination. This means that the ISDN B channel or the ADSL channel is in use and connection charges are accumulating. The direction of the arrow indicates the direction of the call (the icons shown here indicate outgoing connections).
 	No more outgoing calls are possible (incl. D-channel signaling) because one of the global thresholds or a call destination budget limit has been reached.

Details
Configuration and statistical information about the connection (such as the IP address assigned, active B channels and charges) are listed under “Details”.

Available Commands
Depending on the connection status, various commands can be activated here: set up/clear down a connection, ping a remote workstation, etc. For information on the available commands, see the Online Help.

Event Log
When connections are set up or interrupted manually, these operations can be monitored here directly.

5.2 Management and Monitoring Functions

The “Monitoring” menu provides detailed information about the server status, current routing tables and services, active physical connections, connection status, cost/connection data and events. The NT/MPRI also features a packet trace function.

In addition to management over HTTP, the NT/MPRI also provides information over SNMP. If you enable SNMP access, authorized computers equipped with network management software can be granted access to the NT/MPRI and download all data defined in the MIB II (Management Information Base) standard.

When using additional SNMP based management products, SNMP access must be activated on the NT/MPRI first (“Configuration / Security / SNMP Access”). By default, SNMP access is disabled for the sake of security. When SNMP access is disabled, all SNMP requests are passed on to the Microsoft TCP/IP stack.

Server Status

This function permits a fast overview of the NT/MPRI's status with regard to the ISDN-Controllers and ADSL-Controllers used, the connection charges and the cost control functions.

This area also displays any configuration changes that have not yet been implemented by restarting the NT/MPRI.

The following information is displayed:

- Information about the service as well as charges and the number of connections since the service was last started.
- ISDN-Controllers and ADSL-Controllers used and their operating status.
- Configured global thresholds and their current values. Use this overview to determine at a glance whether the actual connection costs are approaching the limits defined.

The values shown here are valid only for connections initiated by the NT/MPRI (outgoing connections).

Routes and Services

The "Routes/Services" menu provides an overview of all currently active IP and IPX routes and ARP entries. The number of routes displayed in these windows depends on whether connections are currently established and how many static routes are registered in the NT/MPRI or advertised from the LAN by RIP.

Active IPX SAP information is also displayed. These pages list all SAP services known to the NT/MPRI from static IPX routes or IPX routes advertised by RIP. This information can be used to check what services are available in the network.

Active Physical Connections

The "Active Physical Connections" menu lists all ISDN connections which are **physically active** at the current time.

The following information is displayed:

- Call Destination name
- Call Destination's ISDN number
- Current data throughput in Kbit/s

- Direction of the call (incoming, outgoing) and the cost assignment setting (call destination or LAN)
- CAPI number of the controller through which the connection was established
- Connection charges for the NT/MPRI and calculation method:
  - "AOCD" if charge information is transmitted on your ISDN line or PBX during connections
  - "Charge Profile" if a charge profile for the inactivity timeout or for charge estimation ("ISDN Settings") has been selected in the call destination settings. The NT/MPRI then estimates the charges based on the selected charge profile
- Duration of the physical connections

An excerpt from the NT/MPRI event log is displayed in the lower frame so that events can be monitored as they occur.

Cost/Connection Analysis

The following options are available with the "Cost/Connection Analysis" menu command:

- **Daily Report** of detailed connection information:

  The daily report contains exact details on all connections set up by the NT/MPRI on the given day. The report includes the call destination, number, charges (including the AOCD or charge profile calculation method), data volume and connection duration, as well as the number of outgoing and incoming calls.

  The cost/connection information is summarized by Call Destination.

  Active logical ISDN connections are not included. These can be monitored in the "Connection Management" window.

- **Selection** of a connection and reporting period:

  This command allows you to specify which cost/connection information should be displayed. Information can be requested by Call Destination or Number, and queries may be restricted to any given time period. The "Break down" option determines whether the cost/connection information for each call destination is summarized by day, week or month. The same details are displayed as in the daily report.

- **Budget Overview** (current values of the Call Destination Budget):

  A direct comparison between the budget defined in the call destination settings and the costs incurred so far is presented here. Use this feature to check that no unexpectedly high connection costs have accumulated and to determine whether the budget for a connection should be increased or reduced.

- **Cost Overview**:

  The cost overview presents an overview of the costs accumulated for connections to call destinations. In addition to the NT/MPRI costs, the charges for the remote sites are estimated based on a charge profile. For this reason, make sure to select the correct charge profile for charge estimation in the call destinations' ISDN settings.

Events

Events include all ISDN messages as well as any error messages.

Messages are divided into categories designated by different icons. The following message types occur:

	Error, such as when the remote destination does not respond.
	Warning, such as a call destination budget or global threshold that has been exceeded.
	Information message such as a successful connection setup or clear-down.
	Incoming call
	Outgoing call
	Alarm, such as a detected violation of the filter rules (Firewall)

All ISDN error messages and NT/MPRI messages are listed in this manual in the chapter "Messages" from page 88.

Events can be displayed either as a daily report or as a selection of events.

- **Daily Report** of Events:

  The daily report of events provides a precise overview of all ISDN messages and any error messages. This protocol is arranged chronologically with the most recent messages first.

- **Selection** of Events:

  In this input mask can be defined precisely which ISDN events the NT/MPRI displays. The information can be selected by type of message, call destination or ISDN-Controller and restricted to any time period desired. When searching error messages to locate sources of trouble, for example, it can be useful to view all incoming or outgoing calls or all messages for a given call destination or a certain controller.

Packet Trace

The “Packet Trace” function can be used to identify which protocol packets are being sent in the LAN and over ISDN. In this way it is possible to localize the causes of excessive connection charges, to record the PPP negotiation for connections and to verify the effectiveness of the enabled spoofing functions.

A number of options can be defined for tracing, such as the protocol layer to be traced. Other possibilities include specifying the destination of packets and whether tracing is to be performed on all or just one specific network adapter.

The following section presents two examples of what to do to configure packet tracing.

Paket Trace for Negotiation Problems, Leased Lines

1. Select the “Monitoring / Packet Trace” menu.
2. Define the following parameters:

Parameter	Action
Level	ISDN/ADSL-Controller/Network adapter
Destination	Enable and select destination
Network adapter	Disable

3. Start the packet trace by clicking the “REC.” button.

4. Select a destination in the “Connection Management” menu and establish a connection.
5. Wait until an error occurs and then stop the packet trace by clicking the “STOP” button in the “Monitoring / Packet Trace” menu.
6. Save the trace.

Packet Trace for Polling Problems

1. Select the “Monitor / Packet Trace” menu.
2. Define the following parameters:

Parameter	Action
Level	NT/MPRI
Destination	Enable and select destination
Network Adapter	Disable

3. Start the packet trace by clicking the “REC.” button.
4. Wait until 20-100 packets have been recorded and then stop the packet trace by clicking the “STOP” button in the “Monitoring / Packet Trace” menu.
5. Save the trace.

The Online Help contains detailed information on packet tracing.

5.3 NT/MPRI Database Management

The NT/MPRI provides a solid basis for recording and processing all important configuration, event, connection and cost data for all ISDN connections using standard Microsoft database technology. The NT/MPRI generates the following databases:

NTR.MDB	General configuration information
NTRLOG.MDB	Events, cost/connection data

These databases are located in the NT/MPRI’s installation directory and can be opened with Microsoft Access for individual evaluation.

Over time the NTRLOG.MDB database can grow quite large. It is therefore a good idea to restrict its size (“Configuration / Server Settings / General”) or to save the file periodically under a different name and delete the original.

6 Tips and Troubleshooting

This chapter presents suggestions for resolving problems which arise during operation. A list of **F**requently **A**sked **Q**uestions (FAQs) and their answers are included as a HTML document in the DOCS\FAQ folder on the NT/MPRI CD.

6.1 General Problems

The web browser no longer displays frames on a page.

Close the Microsoft Internet Explorer by exiting the NT/MPRI Manager and then restart it.

Windows NT indicates that there is no more virtual memory available.

Close the Microsoft Internet Explorer by exiting the NT/MPRI Manager and then restart it.

6.2 Problems Connecting

No ISDN connection to a remote system.

If it is not possible to establish an ISDN connection to a remote site, proceed as follows:

- If your ISDN line is a PBX extension, first check whether the ISDN-Controller used has been set up for PBX operation, and whether the correct outside line access was entered (“Server Settings / ISDN-Controllers”).
- Was the NT/MPRI restarted after any changes were made to its configuration?
- Has a configured budget limit been exceeded? In the NT-MPRI Manager, see the following window to check whether a budget limit has been reached: “Monitoring / Cost / Connection Analysis / Cost Overview”.

  Check the corresponding connection to find out whether the limit for the destination has been reached.

- In addition to destination-specific budgets, the configuration of global thresholds also can be checked here. Check the “Monitoring / Server Status” window.

  The thresholds are listed. If the global threshold for the budget, connection duration or the number of outgoing calls has been reached, the corresponding value can be adjusted with the following command: “Configuration / Server Settings / Thresholds”.

- Check whether the NT/MPRI is able to connect to the AVM Data Call Center (ADC). Pre-configured call destinations are provided for the network protocols TCP/IP and IPX. For instructions on setting up these call destinations and adjusting the configuration if necessary, please see the section “Test Connection with the AVM Data Call Center” on page 29.

- If this connection is not successful, install the file transfer program Connect32 on the Windows XP/2000/NT computer and use it to try connecting to the AVM Data Call Center (number: **+49 (0)30 / 39 98 43 00**).

- With dial-up connections, the ISDN error messages 3303 and 3302 indicate a problem with your ISDN line. The ISDN error message 3403 means that the service “data” is not enabled on your ISDN line. In either case, contact your ISDN provider.

- If the problem is not being caused by your ISDN line, use the NT/MPRI’s packet trace function to trace all PPP over ISDN negotiation packets. To do this, set the “Layer” option to “ISDN-Controller / Network Adapter” and select the desired call destination. Then click the “REC.” button.

No ADSL Connection to the Internet.

Check the protocol binding of the second network adapter:

While a network adapter is responsible for connecting the NT/MPRI computer with a local network, the other network adapter is used exclusively for communication with the ADSL modem. The PPPoE (RFC 2516) protocol (included in the Service Wrapper) is used for this communication. Because this protocol transmits the information required for registration with the ADSL provider via the ADSL modem, this protocol must be bound to the network adapter responsible for communication with the ADSL modem. The protocol is bound automatically to this network adapter during the NT/MPRI installation. No other protocol is

required. In order to eliminate conflicts and potential error sources, it is advisable to remove all network protocols from the second network adapter.

6.3 Problems with TCP/IP

Configuration instructions for connecting two Windows NT networks using TCP/IP over ISDN, and for connections to the Internet, can be found in the section “Configuration and Operation of the NT/MPRI: The Basics” from page 31.

Should routing problems arise with TCP/IP, first try to ping the server at the ADC. Then ping the IP address of your own NT/MPRI. If necessary, use the “-w” option to wait longer for a response from the remote host.

In any case, make sure that the IP address configured for the NT/MPRI is the one assigned by the Internet provider. Otherwise reply packets cannot be routed to your network.

Use the NT/MPRI’s packet trace function to test whether the ping request actually goes out over the ISDN line. If so, and yet no answer is received, check the remote router’s routing information.

Windows XP/2000/NT or Windows 98/95 workstations in the LAN cannot access a remote server.

Use WINS for NetBIOS name resolution.

To do so, install a WINS server in each LAN. At each site, enter the remote LAN’s WINS server for replication and set the replication interval to a high value. This saves ISDN costs. Finally, enter the local WINS server in each workstation’s network settings.

No IP connection to a remote system.

- Check whether several default routes inadvertently have been bound to different call destinations and activated.
- Check in the Control Panel whether the IP protocol settings are correct and that they have been implemented in the NT/MPRI configuration. Check the IP settings currently valid in the NT/MPRI Manager at: “Special / Support Information / Compile Data / Configuration / Special / LAN Interfaces (internal)”.

  If the data listed there are not those expected, check the TCP/IP settings in the Control Panel again, this time at:

– for Windows XP:

– for Windows 2000:

– for Windows NT: “Network / Protocols / TCP/IP Protocol”

To implement these settings in the configuration of the NT/MPRI, select the command:

– for Windows XP:

– for Windows 2000:

– for Windows NT: “Network / Protocols / ISDN Services Wrapper / Properties”

Confirm the message window displayed by clicking “OK”. Then restart the computer.

No NetBIOS over IP connection to a remote system.

- Check the name resolution of the NetBIOS names.

  To check name resolution, open a DOS window and enter the command **`PING <NetBIOS name> -n 8 -w 5000`**. Enter the name of the Windows PC at the remote site as the NetBIOS name. Normally the name should be resolved and the corresponding IP address displayed.

  If the NetBIOS names are not resolved correctly, check the following:

  – Were the settings performed correctly in the LMHOSTS file?

  – Is the LMHOSTS inquiry enabled at “Control Panel / Network / Protocols / TCP/IP Protocol / WINS Address”?

- Check network drive connections to a remote Windows computer with drives released to remote users.

  Perform this check by clicking the “Network Neighborhood” icon with the right mouse button and selecting the “Connect Network Drive...” command.

  Regardless of whether or not the requested Windows computer is displayed in the lower section of the window, enter the complete network path of the Windows computer in the form ‹\\computer name\release name› at “Path”. Here, “computer name” stands for the the unambiguous name of the computer in the Microsoft network, which is also used as the NetBIOS name and registered in

the LMHOSTS file. “Release name” stands for the name for the release of any drive on the remote Windows computer. Note that by default, no drives in Windows XP/2000/NT are released for general access. For information about releasing drives, see the manual of your computer.

Network drive connection fails for a NetBIOS over IP connection.

If both networks are connected via the same domain controller, it is possible to browse (search in the network neighborhood) in the remote network.

If neither network has a domain controller, or if each has its own, browsing is not possible. However, connecting network resources (printers or drives) does work in this configuration, given the appropriate releases and user rights.

Check the following:

- Is the path of the remote computer entered correctly?
- Were drives and/or files released correctly on the remote computer?
- Has the user attempting to access the remote system been assigned rights to connect to the released drive?

6.4 Problems with IPX

IPX over ISDN

Make sure that an internal IPX network number has been assigned for the NT/MPRI. The NT/MPRI installation program obtains the network number from the Windows XP/2000/NT Control Panel and registers it in the “General” router settings in the NT/MPRI Manager. If no internal network number was specified in Windows XP/2000/NT before installation, it is sufficient to enter it here in the NT/MPRI configuration.

No IPX connection can be established to a remote router or a server in the remote network disappears after a while.

Make sure that there are no doubled IPX addresses in the WAN. This is one of the most common errors in setting up an IPX WAN. The IPX addresses used in a WAN must be unique.

IPX in the LAN

No connections are possible in the LAN.

This problem can arise if there is no Novell server installed in the LAN, and the frame type is selected automatically on all devices used in the LAN.

Normally the Novell server determines the frame type, and all the other devices in the LAN conform to its setting.

If this is the case, the frame type for the computer on which the NT/MPRI is installed must be selected manually.

6.5 Settings for Incoming Calls

If other CAPI 2.0 applications are installed on the same computer as the NT/MPRI, please note the following instructions about the configuration for incoming calls:

The NT/MPRI uses the ISDN service “data”. If other CAPI applications besides the NT/MPRI are installed on the router computer or on the same S_0 bus, each such application must be assigned a distinct MSN or DDI for incoming calls. This is the only way to unambiguously direct calls with the “data” service indicator, used not only by the NT/MPRI but also by such programs as FRITZ!data. If no distinct numbers are assigned, a program like FRITZ!data may attempt to answer an incoming call actually intended for the NT/MPRI.

If all other terminal equipment on the same S_0 bus uses other ISDN services, such as “voice” in the case of an ISDN telephone, it is not necessary to assign MSNs or DDIs, as the service indicator is sufficient to identify the calls intended for the NT/MPRI.

7 Messages

This chapter lists and explains the error messages which arrive from the ISDN network and the messages displayed by the NT/MPRI.

All messages are recorded in the ISDN event log in the following format:

‹Date› ‹Time› ‹Name of the Destination›
‹Source› ‹Message›

Example:

12.5.2000 14:14:42, ADC-IP
ISDN-Controller 1: B-channel connection to “03039984350” is set up.

7.1 CAPI 2.0 and Euro-ISDN Messages

The following messages are sorted in numerical order.

Number	Messages/Explanations
0x0001	**NCPI not supported by current protocol, NCPI ignored[#0001]** This message indicates protocol conflicts between the sending and receiving stations.
0x0002	**Flags (signals) not supported by current protocol, flags ignored[#0002]** This message indicates that certain control information accompanying the data sent was not supported by the receiving station’s protocol.
0x0003	**Signal already sent by another application[#0003]** This message indicates that another active application has already reacted to the incoming call.
0x1104	**Queue is empty[#1104]** This message indicates internal application errors.
0x1001	**Too many CAPI applications[#1001]** This message indicates that there are too many CAPI applications active. Close any applications currently not required.

Number	Messages/Explanations
0x1002	**Logical block size too small, must be at least 128 bytes[#1002]** This message indicates internal application errors.
0x1003	**Buffer exceeds limit of 64 kBytes[#1003]** This message indicates internal application errors.
0x1004	**Message buffer too small, at least 1024 bytes required[#1004]** This message indicates internal application errors.
0x1005	**Max. number of logical connections not supported[#1005]** This message indicates that the controller has not been configured adequately. Check the configuration of your controller. Change the settings so that it supports more logical connections supported.
0x1007	**The message could not be accepted due to an internal busy condition[#1007]** This message indicates either internal application errors or applications that are not conform to CAPI.
0x1008	**OS resource error (no memory?)[#1008]** This message indicates that the operating system is overloaded. Close all active applications and restart the operating system.
0x1009	**Common-ISDN-API Version 2.0 not installed[#1009]** This message indicates that CAPI 2.0 is not installed. Load CAPI 2.0.
0x100A	**Controller does not support external equipment[#100A]** The ISDN driver does not support the equipment required by the application. This message indicates an internal application error.
0x100B	**Controller only supports external equipment[#100B]** The ISDN driver does not support the equipment required by the application. This message indicates an internal application error.
0x1101	**Illegal application number[#1101]** This message indicates internal application errors. The application has crashed. Contact your software manufacturer and ask about applications that conform to CAPI.

Number	Messages/Explanations
0x1102	**Illegal command or subcommand, or message length less than 12 bytes[#1102]** This message indicates either internal application errors or applications that do not conform to CAPI.
0x1103	**The message could not be accepted due to a full queue condition! The error does not affect messages for other PLCI or NCCI controllers[#1103]** This message indicates either internal application errors or applications that do not conform to CAPI.
0x1105	**Queue overflow; a message was lost! Configuration error, the only recovery method is to perform a CAPI_RELEASE[#1105].** This message indicates internal application errors. Insufficient application capacities require reconfiguration.
0x1106	**Unknown notification parameter[#1106]** This message indicates internal application errors.
0x1107	**The message could not be accepted due to an internal busy condition[#1107]** This message indicates either internal application errors or applications that are not conform to CAPI.
0x1108	**OS resource error (no memory?)[#1108]** This message indicates that the operating system is overloaded. Close all applications and restart the operating system.
0x1109	**Common-ISDN-API Version 2.0 is not installed[#1109]** This message indicates that CAPI 2.0 is no longer available. It was unloaded while an application was active. Reload CAPI 2.0.
0x110A	**Controller does not support external equipment[#110A]** The ISDN driver does not support the equipment required by the application. This message indicates internal application errors.
0x110B	**Controller supports only external equipment[#110B]** The ISDN driver does not support the equipment required by the application. This message indicates internal application errors.
0x2001	**Message not supported in current state[#2001]** This message indicates internal application errors.

Number	Messages/Explanations
0x2002	**Illegal controller / PLCI / NCCI[#2002]** This message indicates internal applications errors.
0x2003	**Out of PLCI[#2003]** This message indicates that the controller is not adequately configured. Please check the controller configuration.
0x2004	**Out of NCCI[#2004]** This message indicates that the controller is not adequately configured. Please check the controller configuration.
0x2005	**Out of LISTEN[#2005]** This message indicates that the controller is not adequately configured. Please check the controller configuration.
0x2006	**Out of fax resources (T.30 protocol)[#2006]** This message indicates that the controller is not adequately configured. Please check the controller configuration. Change the settings so that more resources are available.
0x2007	**Illegal message parameter coding[#2007]** This message indicates internal application errors.
0x3001	**B1 protocol not supported[#3001]** This message indicates that the driver does not provide the protocols the application requires. Install the necessary protocols.
0x3002	**B2 protocol not supported[#3002]** This message indicates that the driver does not provide the protocols the application requires. Install the necessary protocols.
0x3003	**B3 protocol not supported[#3003]** This message indicates that the driver does not provide the protocols the application requires. Install the necessary protocols.
0x3004	**B1 protocol parameter not supported[#3004]** This message indicates that the driver does not provide the protocol options required by the application.
0x3005	**B2 protocol parameter not supported[#3005]** This message indicates that the driver does not provide the protocol options required by the application.

Number	Messages/Explanations
0x3006	**B3 protocol parameter not supported[#3006]** This message indicates that the driver does not provide the protocol options required by the application.
0x3007	**B protocol combination not supported[#3007]** This message indicates internal application errors. Protocol conflicts have occurred, The B protocols used are not compatible and may not be used together.
0x3008	**NCPI not supported[#3008]** The B-channel protocols in use are not compatible.
0x3009	**CIP value unknown[#3009]** The service requested by the application is not implemented in the controller software.
0x300A	**Flags (signals) not supported (reserved bits)[#300A]** This message indicates internal application errors. The signals (flags) requested by the application are not supported by CAPI.
0x300B	**Facility not supported[#300B]** The ISDN driver does not support the requested supplementary service. Please contact your software manufacturer for more information.
0x300C	**Data length not supported by current protocol[#300C]** This message indicates internal application errors.
0x300D	**Reset procedure not supported by current protocol[#300D]** This message indicates internal application errors. Contact your software manufacturer for more information about applications that conform to CAPI.
0x3301	**Protocol error, layer 1 (broken line or B channel removed by signaling protocol)[#3301]** No connection could be established between the terminal equipment and /or the exchange. The call set-up failed at layer 1 of the ISDN protocol. No messages could be exchanged between the terminal equipment and the network terminator or local switch. Possible causes include: cable not correctly connected; cable connectors miswired or wrong sockets used; network termination not correctly enabled or not connected correctly to the line; defective terminal equipment at the bus blocking communication.

Number	Messages/Explanations
0x3302	**Protocol error, layer 2[#3302]** No connection could be established between the terminal equipment and the network terminator or local switch. The call set-up failed at layer 2 of the ISDN protocol: no messages could be exchanged between the terminal equipment and the local switch. Possible causes include: the line is not enabled at the network terminator; an incompatible D-channel protocol used on the line.
0x3303	**Protocol error, layer 3[#3303]** No connection could be established between the terminal equipment and the network terminator or local switch.
0x3304	**Another application got the call[#3304]** This message indicates that another active application received the incoming call.
0x3311	**Connecting not successful (remote station is not a fax G3 machine)[#3311]** The remote station called is not a fax machine.
0x3312	**Connecting not successful (setting error)[#3312]** Due to internal problems (setting errors) the remote station called is not ready to receive.
0x3313	**Disconnected before transfer (remote station does not support transfer mode, e.g. wrong resolution)[#3313]** Due to internal problems the remote station called is not ready to receive.
0x3314	**Disconnected during transfer (remote abort)[#3314]** Due to internal problems the remote station called is not ready to receive.
0x3315	**Disconnected during transfer (remote procedure error, e.g. unsuccessful repetition of T.30 commands[#3315]** Due to internal problems the remote station called is not ready to receive.
0x3316	**Disconnected during transfer (local tx data underrun)[#3316]** This message indicates internal application errors.
0x3317	**Disconnected during transfer (local rx data overflow)[#3317]** Due to internal problems the remote station called is not ready to receive.

Number	Messages/Explanations
0x3318	**Disconnected during transfer (local abort)[#3318]** Due to internal problems the remote station called is not ready to receive.
0x3319	**Illegal parameter coding (e.g. SFF coding error)[#3319]** This message indicates internal application errors.
0x3400	**No ISDN connection. Reason unknown[#3400]** The connection was terminated for unknown reasons.
0x3490	**Normal call clear-down[#3490]** This message indicates that one of the parties involved in the call initiated a call clear-down.
0x349A	**Non-selected user clearing[#349A]** This message indicates that the incoming call was not directed to the user.
0x349F	**No ISDN connection. Reason unknown[#349F]** The connection was terminated for unknown reasons.
0x3481	**Unallocated (unspecified) number[#3481]** This message indicates that the destination requested by the caller could not be reached. The number dialed has not been assigned to terminal equipment.
0x3482	**No route to specified transit network[#3482]** The equipment sending this message has received a request to route the call through a particular transit network that it does not recognize, either because the transit network does not exist or because this particular transit network does not support the equipment sending the message. Support for this message is network-dependent.
0x3483	**No route to destination[#3483]** The user called cannot be reached because the network through which the call has been routed does not serve the destination desired. Support for this message is network-dependent.
0x3486	**Channel unacceptable[#3486]** This message indicates that the sending unit does not accept the channel identified for use in this call.

Number	Messages/Explanations
0x3487	**Call awarded and being delivered in an established channel[#3487]** The user has been awarded the incoming call, which is being connected to a channel already established to that user for similar calls.
0x3491	**User busy[#3491]** This message appears when the user called has indicated the inability to accept another call. The user's equipment is compatible with call, however.
0x3492	**No user responding[#3492]** A user has not responded to a call set-up message with an alert or connect indication within the prescribed time.
0x3493	**No answer from user (user alerted)[#3493]** A user has provided an alert indication, but no connect indication within the prescribed time. This message is not normally generated by ETS 300 102-1 procedures but may be generated by internal network timers.
0x3495	**Call rejected[#3495]** The equipment sending this message does not accept the call, although it is neither busy nor incompatible.
0x3496	**Number changed[#3496]** This message is returned to a caller when the number dialed no longer exists. The new number may optionally be included in the diagnostics field. If a network does not support his feature, message 0x3481 is returned.
0x349B	**Destination out of order[#349B]** The remote system dialed by the user cannot be reached because the interface is not working correctly. The phrase ‚out of order' indicates that a signaling message could not be transmitted to the remote user. Possible causes include: a physical layer or data link failure at the remote station, user equipment offline, etc.
0x349C	**Invalid number format[#349C]** This message indicates that the party dialed cannot be reached because the number dialed is either incomplete or has an invalid format.

Number	Messages/Explanations
0x349D	**Facility rejected[#349D]** This message is returned when a requested service cannot be provided by the network.
0x349E	**Response to status inquiry[#349E]** This message is included in the status report when the status report was generated in response to a status inquiry.
0x34A2	**No circuit/channel available[#34A2]** This message indicates that no suitable circuit or channel is currently available to send or receive data.
0x34A6	**Network out of order[#34A6]** This message indicates that the network is not working correctly and that the condition is likely to last relatively long; immediate redialing is not likely to be successful.
0x34A9	**Temporary failure[#34A9]** This message indicates that the network is not functioning correctly, but that the condition is not likely to last long; the user may try dialing again immediately.
0x34AA	**Switching equipment congestion[#34AA]** The switching equipment generating this message is currently experiencing heavy traffic.
0x34AB	**Access information discarded[#34AB]** The network was unable to supply the access information requested by the user, such as user information and low-layer compatibility.
0x34AC	**Requested circuit/channel not available[#34AC]** The circuit or channel indicated by the requesting unit cannot be provided by the other side of the interface.
0x34AF	**Resource unavailable, unspecified[#34AF]** This message is used to report a resource-unavailable event only if no other message in this class applies.
0x34B1	**Quality of service unavailable[#34B1]** The requested quality of service as defined in CCITT recommendation X.213 cannot be provided (throughput or transit delay is not supported).

Number	Messages/Explanations
0x34B2	**Requested facility not subscribed[#34B2]** This message indicates that the requested supplementary service could not be provided by the network because the user has not made the necessary administrative arrangements.
0x34B9	**Bearer capability not authorized[#34B9]** The user requested a bearer capability which is implemented by the equipment that generated this message, but which the user is not authorized to use.
0x34BA	**Bearer capability not currently availabe[#34BA]** The user requested a bearer capability which is implemented by the equipment that generated this message, but which is not available at this time.
0x34BF	**Service or option not available, unspecified[#34BF]** This message is used to report a “service or option not available” event only when no other message in this class applies.
0x34C1	**Bearer capability not implemented[#34C1]** The equipment sending this message does not support the bearer capability requested.
0x34C2	**Channel type not implemented[#34C2]** The equipment sending this message does not support the channel type requested.
0x34C5	**Requested facility not implemented[#34C5]** The equipment sending this message does not support the requested supplementary service,
0x34C6	**Only restricted digital information bearer capability is available[#34C6]** A device has requested an unrestricted bearer service, but the equipment sending this message supports only the restricted version of the requested bearer capability.
0x34CF	**Service or option not implemented, unspecified[#34CF]** This message is used to report a “service or option not implemented” event only when no other message in this class applies.
0x34D1	**Invalid call reference value[#34D1]** The equipment returning this message has received a message with a call reference which is not currently in use on the user/network interface.

Number	Messages/Explanations
ox34D2	**Identified channel does not exist[#34D2]** The equipment returning this message has received a request to use a channel not activated to accept calls on the interface. This message is generated if, for example a primary interface user has subscribed to channels 1 through 12 and the user's equipment or the network attempts to use channels 13 through 23.
ox34D3	**A suspended call exists, but this call identity does not[#34D3]** This message indicates an attempt to resume a call with a call identity which does not match that of any currently suspended calls.
ox34D4	**Call identity in use[#34D4]** The network received a request to resume a call. The suspend call request contains a call identity which is already in use for another suspended call.
ox34D5	**No call suspended[#34D5]** The network received a request to resume a call. The request contains call identity elements which do not indicate any currently suspended call.
ox34D6	**Call with the requested call identity has been cleared[#34D6]** The network has received a request to resume a call. The request contains call identity elements which once indicated a suspended call; however, that call was cleared down while suspended (either by network time-out or by one of the parties to the call).
ox34D8	**Incompatible destination[#34D8]** The equipment returning this message received a request to establish a connection. However, the call has low-layer, high-layer compatibility or some other attributes which cannot be accommodated.
ox34DB	**Invalid transit network selection[#34DB]** This message indicates that a transit network was identified in an incorrect format.
ox34DF	**Invalid message, unspecified[#34DF]** This message is returned for an invalid message only when no other error message in the "invalid message" class applies.

Number	Messages/Explanations
0x34E0	**Mandatory information element is missing[#34E0]** The equipment returning this message has received a message from which information required for processing was missing.
0x34E1	**Message type nonexistent or not implemented[#34E1]** The equipment returning this message received a message which is defined, but not implemented by the equipment.
0x34E2	**Message type not compatible with call state or message type nonexistent or not implemented[#34E2]** The equipment returning this message has received a message that cannot be received in the current call state, or a status message was received indicating an incompatible call state.
0x34E3	**Information element nonexistent or not implemented[#34E3]** The equipment returning this message received a message which contains information elements that were not recognized, either because the information element identifier is not defined, or because it is defined, but not implemented in the equipment returning the message.
0x34E4	**Invalid information element contents[#34E4]** The equipment returning this message received an information element which is implemented; however, one or more of the fields in the information element are coded in a way which is not implemented in the equipment.
0x34E5	**Message type incompatible with call state[#34E5]** This message indicates that a message was received which is incompatible with the call state.
0x34E6	**Recovery on timer expiration[#34E6]** This message indicates that a procedure was initiated by the expiration of a timer in accordance with ETS 300 120-1 error hanlding procedures.
0x34EF	**Protocol error, unspecified[#34EF]** This message is returned to report a protocol error only when no other message in the protocol error class applies.
0x34FF	**Internetworking, unspecified[#34FF]** This message indicates internetworking with a network that did not provide a reason for the action it performs; for this reason the precise cause of the message sent cannot be ascertained.

7.2 NT/MPRI Messages

The following symbols are used in the message descriptions below:

‹number›	ISDN number or CLI
‹CLI›	CLI number
‹number called›	ISDN number called, for incoming calls
‹call destination›	name of the call destination
‹protocol›	network protocol used (IP or IPX)
‹description›	brief packet description
‹no.›	position of the rule applied within a filter profile
‹profile name›	name of the filter profile

The messages are listed in alphabetical order.

Accepting incoming call from ‹call destination› (‹number›). Setting up B channel.

This message indicates that an incoming call was accepted successfully and that the B-channel connection is being established.

Authentication at remote site ‹call destination› failed.

The local router was not recognized by the remote router. Authentication failed.

Authentication of remote site ‹call destination› at the local site failed.

The remote router was not recognized by the local router. Authentication failed.

B-channel connection to ‹call destination› (‹number›) is cleared.

The physical connection to the specified call destination has been cleared down.

B-channel connection to ‹call destination› (‹number›) is set up.

The physical connection to the specified call destination was successfully established.

Clearing down B-channel connection to ‹call destination› (‹number›).

The physical connection to the specified call destination is being cleared down.

Clearing down B-channel connection to ‹destination› (‹number›). Call destination budget or global thresholds reached.

If the destination-specific budget was reached, the physically active connection is cleared and the call destination in question blocked for all outgoing connections, including call waiting signals over the D channel.

If a global threshold was reached, all physically active connections are cleared down and the computer is locked for all outgoing calls, including call waiting signals over the D channel.

To release the lock, enter a higher budget or threshold value.

Clearing down B-channel connection to ‹call destination› (‹number›). No suitable B channel available.

The incoming call cannot be accepted because all suitable B channels are busy. The B-channel connection is being cleared down.

Clearing down connection because the DSL modem delivers an incomprehensible packet.

The ADSL modem delivers information which cannot be processed by the NT/MPRI. The reason may be a defective ADSL connection. If this message occurs repeatedly, contact the ADSL provider.

Clearing down connection because the DSL modem delivers an incomprehensible packet. The DSL modem returns: %s

The ADSL modem delivers information which cannot be processed by the NT/MPRI. The reason may be a defective ADSL connection. If this message occurs repeatedly, contact the ADSL provider.

Clearing down connection because the DSL modem is not responding.

Check the connection from the NT/MPRI Service PC to the ADSL modem. Use only the original cables supplied with the modem. Make sure that the DSL modem is switched on. Check that the network adapter for communication with the DSL modem is installed in the NT/MPRI Service PC and that a corresponding network adapter is registered in the network settings.

Clearing down connection because the DSL modem reports a general error.

The ADSL modem returns error messages. The reason may be a defective ADSL connection or ADSL modem. If this message occurs repeatedly, contact the ADSL provider.

Clearing down connection because the DSL modem reports a general error. The DSL modem returns: %s

The ADSL modem returns error messages. The reason may be a defective ADSL connection or ADSL modem. If this message occurs repeatedly, contact the ADSL provider.

Clearing down connection because the DSL modem reports a service name error.

The ADSL modem returns error messages. The reason may be a defective ADSL connection. If this message occurs repeatedly, contact the ADSL provider.

Clearing down connection because the DSL modem reports a service name error. The DSL modem reports: %s

The ADSL modem returns error messages. The reason may be a defective ADSL connection or ADSL modem. If this message occurs repeatedly, contact the ADSL provider.

Clearing down connection because the DSL modem reports a system error.

The ADSL modem returns error messages. The reason may be a defective ADSL connection or ADSL modem. If this message occurs repeatedly, contact the ADSL provider.

Clearing down connection because the DSL modem reports a system error. The DSL modem reports: %s

The ADSL modem returns error messages. The reason may be a defective ADSL connection. If this message occurs repeatedly, contact the ADSL provider.

Clearing down connection because the DSL modem reports an unspecified error.

The ADSL modem returns error messages. The reason may be a defective ADSL connection or ADSL modem. If this message occurs repeatedly, contact the ADSL provider.

Clearing down connection because encryption negotiation failed.

The negotiation of encryption fails if the remote site does not support the ECP protocol or if it does not know the encryption algorithm. If this message is returned, contact the network administrator of the remote system.

Clearing down incoming call from ‹call destination› (‹number›). No settings found for remote site.

The incoming call cannot be accepted because no local call destination configuration was found for the remote site. The B channel that was set up is being cleared down again.

Clearing down incoming call from ‹CLI› because cost allocation is set to “Local Site”.

This message indicates that the local router intends to accept the connection charges. The incoming call therefore is rejected, and the local router called back the remote site.

Clearing down ‹protocol› connection.

The logical network connection to the call destination named is now being terminated.

Connection cleared down. The remote site did not call back as expected.

The local NT/MPRI did not receive a security call-back which it requested. The connection was therefore terminated.

Incoming call from ‹call destination› (‹CLI›) rejected. Call collision.

Both sites attempted to set up a connection simultaneously. The incoming call was rejected.

Incoming call from ‹call destination› (‹CLI›) rejected. Several calls for this destination are already being processed.

This message reports that the maximum number of calls which can be processed simultaneously for one call destination has been reached. The incoming call is rejected.

Incoming call from ‹call destination› (‹CLI›) rejected. The maximum number of bundled channels to this call destination is already set up.

This message indicates that no more channels are available for channel bundling. The configured maximum number of B channels is already being used for this connection.

Incoming call from ‹call destination› (‹CLI›) rejected. The maximum number of supported connections has been reached.

This message indicates that no more connections are supported at this time. The incoming call is rejected.

Incoming call from ‹CLI› for ‹number dialed› cannot be accepted. All B channels in use.

The incoming call could not be accepted because all B channels on the ISDN-Controller called are already being used for other physical connections.

Incoming call from ‹CLI› for ‹number dialed› rejected. All B channels in use.

The incoming call could not be accepted because all B channels on the ISDN-Controller called are already being used for other physical connections.

Incoming call from ‹CLI› for ‹number dialed› rejected. The MSN/EAZ/DDI dialed is not configured.

The MSN/EAZ or DDI dialed was not configured for use by the NT/MPRI. The call may have been intended for another application. As a result, the incoming call was not accepted.

Incoming call from ‹CLI› rejected. The local router's own endpoint discriminator was received.

The local router attempted to set up a connection to itself.

Incoming call to ‹number dialed› rejected. This CLI ‹CLI› is not allowed to dial in.

The security settings specify that all incoming calls should be subjected to a CLI number check. The CLI number received was not found in the local CLI number database; therefore the call was rejected.

Incoming logical connection to ‹call destination› (‹CLI›) lost (local).

The local site lost the incoming logical connection to the remote site.

Logical connection cleared after inactivity.

The logical ISDN connection was cleared down due to inactivity.

Logical connection to ‹call destination› lost (local).

The local site lost the outgoing logical connection to the remote site.

Outgoing call to ‹call destination› (‹number›) not possible. Call destination budget or global thresholds reached.

If the destination-specific budget was reached, the call destination is blocked for all outgoing connections, including call waiting signals over the D channel.

If a global threshold was reached, all outgoing connections are locked, including signaling over the D channel.

To release the lock, enter a higher budget or threshold value.

Outgoing call to ‹call destination› accepted by remote site, although cost allocation is set to “Remote Site”.

The outgoing call was accepted by the remote site and charges are being incurred at the local site. The remote site should have refused the call and called back in order to bear the connection charges. Make sure that the CLI transmitted by the local router is registered correctly at the remote site.

Packet ‹description› accepted due to rule ‹no.› from ‹profile name›.

An IP firewall message indicating that the packet described was accepted. The filter profile is indicated along with the position of the applicable rule within the filter.

Packet ‹description› denied due to rule ‹no.› from ‹profile name›.

An IP firewall message indicating that the packet described was discarded. The filter profile is indicated along with the position of the applicable rule within the filter.

Packet ‹description› rejected due to rule ‹no.› from ‹profile name›.

An IP firewall message indicating that the packet described was refused. The filter profile is indicated along with the position of the applicable rule within the filter.

Physical connection cleared after inactivity.

The physical ISDN connection was cleared due to inactivity.

Physical connection cleared after inactivity (charge profile).

The physical ISDN connection was cleared due to inactivity. The value for the inactivity timeout was determined using the specified charge profile.

‹Protocol› connection is cleared.

The logical network connection to the call destination named has been cleared down.

‹Protocol› connection is set up.

The logical network connection to the call destination named has been established.

Remote site ‹call destination› lost logical connection.

The remote site lost the logical connection to the local site.

Remote site does not support security call-back.

This message indicates that the remote site dialed does not support the security call-back requested by the local NT/MPRI.

Self-configuring inactivity timeout for connection to ‹call destination› set to ‹xx› seconds.

The inactivity timeout for the ISDN connection was set to the given value.

Setting up B-channel connection to ‹call destination› (‹number›).

A physical connection to the specified call destination is being established.

Setting up incoming ‹protocol› connection.

This message reports that an incoming connection is being established with the specified network protocol.

Setting up ‹protocol› connection.

A logical network connection to the call destination named is being established.

Unable to set up B channel. All B channels in use.

The physical connection cannot be established. All available B channels currently are being used for other physical connections or are reserved for other connections.

8 Information, Updates and AVM Support

In order to install and configure the NT/MPRI, sound knowledge of LANs and WANs as well as Windows XP/2000/NT is required. Ideally, you should also be familiar with the concept of routing and the implemented network protocols.

AVM provides a number of information resources to assist you in working with the AVM MultiProtocol Router for ISDN/DSL. AVM Support is standing by for those cases when you are unable to solve a problem yourself.

Literature references are provided in the section “Additional Literature” on page 109.

8.1 Information Sources and Updates

Documentation

The NT/MPRI includes comprehensive documentation in a number of different formats:

- The installation directory of the NT/MPRI contains a PDF version of this manual. This manual may be accessed from the start page of the NT/MPRI Manager or from the Online Help.

  The manual includes comprehensive information about the concept behind and potential applications of the NT/MPRI as well as installation requirements and instructions. It presents background information about the way the NT/MPRI functions as well as general information about routing over ISDN and ADSL.

If your computer is not equipped with the Adobe Acrobat Reader for reading PDF documents, this reader can be installed from the \UTILS\ACROBAT directory on the NT/MPRI CD.

- The comprehensive HTML-based Online Help can be accessed from every “page” of the NT/MPRI Manager. It includes detailed descriptions of all settings, monitoring functions and statistics information.

- The Readme file for the NT/MPRI contains important information and installation instructions which were not yet available when the manual was printed. This file can, and should, be viewed in the introduction before proceeding with installation (INTRO.HLP).
- For comprehensive information about Windows XP/2000/NT, see the Windows XP/2000/NT manual.

Additional Literature

Detailed information about Windows 2000/NT is available from the following sources:

- Russel, Charlie and Sharon Crawford: Microsoft® Windows® 2000 Server Administrator's Companion, Microsoft Press, Redmond, Washington, 2000, ISBN 1-57231-819-8

Information about TCP/IP and IP firewalls is presented in the following books:

- D. B. Chapman/E. D. Zwicky: Building Internet Firewalls, O´Reilly & Associates, 1995
- W. R. Cheswick/S. M. Bellovin: Firewalls and Internet Security, Addison-Wessley, Reading, Massachusetts, 1994
- Lee, Thomas and Joseph Davies: Microsoft® Windows® 2000 TCP/IP Protocols and Services Technical Reference, Microsoft Press, Redmond, Washington, 2000, ISBN 0-7356-0556-4

General information on internetworking is available in:

- L. A. Chappell/R.L. Spicer: Novell's Guide to Multiprotocol Internetworking, Novell Press, 1994

For information about IPX, see the various Novell NetWare manuals.

The AVM Data Call Center

With the AVM Data Call Center (ADC) you have access to the latest information and to updates and extensions to AVM products free of charge. The ADC can be reached as follows:

Over the Internet

The URL of the AVM home page is:

`http://www.avm.de/en`

Over the AVM Intranet PPP Server

The ISDN number is:

+49 (0)30 / 39 98 43 20

This call destination is preconfigured in the NT/MPRI (“ADC-IP”) and can be dialed using the “Connection Management” menu.

Over the MPR for ISDN Server

The telephone number is:

+49 (0) 30 / 39 98 43 50

This call destination is preconfigured in the NT/MPRI (“ADC-IPX”) and can be dialed using the “Connection Management” menu.

For more information about these call destinations, see the section “Test Connection with the AVM Data Call Center” on page 29.

The ADC can also be reached with the program Connect or Connect32 included in the ISDN-Controller package. For more information, see the Readme of the ISDN-Controller.

AVM also offers comprehensive information and free updates on the Internet.

- The “Products” section presents detailed information about all AVM products along with announcements of new products and new versions.
- In the “Service” section you have access to the FAQ lists with answers to frequently asked questions. Search for concrete support advice here.
- Through “Download” the current driver software for all AVM ISDN-Controllers may be downloaded.

8.2 Assistance from AVM Support

Please use the information sources listed above before contacting the Support desk!

If you were not able to solve your problem with the tips offered above or using the various information sources listed, contact AVM Support for additional technical assistance. The Support desk can be reached by e-mail or by telefax.

Before Contacting AVM Support

Before contacting AVM Support, please prepare the following information so that we can assist you efficiently:

1. A detailed description of the problem and a sketch of your WAN with the IP addresses and IPX addresses of all integrated components.
2. The exact wording of any error messages returned.
3. The “Compile Data” buton in the “Special / Support Information” menu generates an HTML page with all information about your NT/MPRI that is important for the Support desk. Print out this page or save it as an HTML file. If your system uses the Microsoft Internet Explorer 4.0 or higher, proceed as follows to save the file:
   - In the context menu of the right mouse button, select the command “View Source”. An editor is opened.
   - Save the text as an HTM file using the menu command “File / Save As...”.
4. Should interoperability problems arise with routers from other manufacturers, record a PPP session.

Support by E-mail

Support requests can be sent to AVM by e-mail. Please use our e-mail form at the AVM Internet site.

1. Enter the address of the AVM site:

   http://www.avm.de/en

2. Click “Service”.

3. Select “Support” and click “Other AVM Products Mail Form”, as the NT/MPRI does not have its own English-language support request form.

4. In the first line of the form, at “Product”, select the “Multiprotocol Router for Windows NT” from the drop-down list.

5. Fill out the form and send it to AVM Support by clicking the “Send” button.

Support by Telefax

If you do not have access to the Internet, Support can be reached at the following telefax number:

+49 (0)30 / 39 97 62 66

Please include in this fax the CD Key printed on the CD cover. Also prepare the following information for support staff:

- Which version of the AVM MultiProtocol Router for ISDN/DSL are you using? The version number is listed in the Readme.
- Which Microsoft Service Pack are you using?
- Which operating system is installed on the computer where the NT/MPRI is installed: Windows XP, Windows 2000 or Windows NT?
- Which network protocol are you using?
- Which ISDN-Controller does the NT/MPRI computer use? Which driver version and which build are you using?

  The driver version and the build of any AVM ISDN-Controller is listed in the Readme file in the installation directory of the ISDN-Controller. If FRITZ! is installed on the NT/MPRI computer, the driver version also can be viewed using the “Start / Programs / FRITZ! / FRITZ!version” command. Then click the “System Information” button in the “FRITZ!version” window.

- Is your ISDN-Controller operated on a PBX?

Please try several times, as the AVM Data Call Center often is busy at peak times!

- Is it possible to establish a successful test connection to the AVM Data Call Center with the ISDN-Controller?
- At which step of installation or at what point in the application is an error message returned?
- What is the exact wording of the message?

Glossary

1TR6

1TR6 is the older German national D-channel protocol. No new ISDN line has been installed with this protocol in Germany since December 1993. Only the European D-channel protocol DSS1 is used for new lines.

ADSL (Asymmetric Digital Subscriber Line)

ADSL is a technology which makes high-bandwidth Internet access possible over a normal (analog) telephone line. During downloading data can be transmitted at up to 768 kbit/s; in the opposite direction, up to 128 Kbit/s are possible. Dial-in connections to other ADSL users and service indicators are not possible.

ADSL access is generally supplied along with an ISDN line (if such a line is not yet provided). ADSL access is provided by plugging a cable into a supplementary network adapter or into an AVM ADSL/ISDN-Controller in the computer.

ARP (Address Resolution Protocol)

The Address Resolution Protocol, or ARP, is part of the TCP/IP protocol suite, and provides dynamic mapping of IP addresses to hardware address (MAC addresses) in a LAN. This mapping is maintained automatically and is usually opaque to applications and users.

To exchange data in a TCP/IP network, the sending station must map the destination's IP address to its hardware address. The sending station sends out an "ARP request" packet with the IP address of the destination. All ARP-sensitive systems in the network recognize this packet, and the system with the given IP address returns its hardware address in an ARP reply packet. The sender then stores the combination of IP address and hardware address in its ARP cache.

Authentication

Authentication is the examination of a remote system's log-on information (name and password), for both incoming and outgoing calls. This check secures the NT/MPRI against unauthorized access and identifies the call destination/user if assignment of incoming calls using the D channel number (CLI) is not enabled. The PAP and CHAP authentication

procedures are supported. In the NT/MPRI you may specify the procedure by which each remote site must identify itself (“Authentication at the Local Site”). A name and a password must be configured for each procedure, and these must be communicated to the call destination/user. If the remote site's system also requires authentication information from the NT/MPRI (“Authentication at the Remote Site”), you can enter the correct name and password (received from the remote site) into the call destination/user settings.

B Channel

An ISDN Basic Rate Interface (BRI) consists of two B channels and a D channel. An ISDN Primary Rate Interface (PRI) consists of thirty B channels and one D channel. User data is transmitted on the B channels at 64 kbit/s. The connection speed can be increased by bundling the B channels.

CHAP (Challenge Handshake Authentication Protocol)

One of two authentication protocols. To perform an authentication, the local and remote sites must have the name and password to be used entered in their configuration. Under CHAP, the site requesting the authentication generates a message from the user name and a random value according to a defined encryption algorithm, and sends the message to the remote site. The remote site produces a new value out of the message and the password, also using a preset algorithm, and sends this value back. The first site now checks whether the value it produces from the original message and the password agrees with the value the remote site sent back. If it does, the connection is set up. As the password itself ist not transmitted during this process, CHAP can be considered as safe. CHAP is defined in RFC 1334 and RFC 1994.

Charge Profile

A charge profile contains information on the frequency of charge information as a function of rate periods and calling zones, such as “Local” and “Long distance”. Each profile consists of two lists with the charge rates as they vary over a period of 24 hours: one list is for working days (Monday-Friday), the other for weekends and public holidays (optional). The NT/MPRI can use charge profiles to manage the physical disconnection of idle ISDN connections. If a charge profile is chosen for the inactivity timeout in the call destination/user settings, the connection is terminated 3 seconds before the end of the charge interval, provided no data was transmitted in the preceding 3 seconds. In this way optimum use is made of the charge interval. In addition, the selected charge profile is used to estimate the costs that have accumulated. The charges calculated by the NT/MPRI on this basis are then compared with the call destination/user budget and the global thresholds. Unexpectedly high ISDN costs are thus avoided.

If no AOCD charge information is received on your ISDN line or PBX extension during the connection, you should select a charge profile in the settings of all call destination/users. If the NT/MPRI does not receive charge information, the charge profile is the only means by which the costs incurred can be calculated and compared with the budget. The NT/MPRI also uses the charge profile to estimate remote sites' costs.

CLIP (Calling Line Identification Presentation)

Transmission of the caller's number over the ISDN D channel. CLI is a feature in ISDN which is used by the NT/MPRI to identify incoming calls and to protect against unauthorized access. This feature must be enabled by the ISDN provider for the caller's line. In Germany, for example, this feature can be requested when ordering an ISDN line.

(COMMON-ISDN-API) CAPI

A standardized interface between ISDN PC adapters and ISDN applications, independent of specific manufacturers. Once the AVM ISDN-Controller has been installed, CAPI is available throughout the entire system (current version 2.0). Current CAPI drivers are available free of charge from the \PROGRAMS directory on AVM's FTP server (ftp://ftp.avm.de). The NT/MPRI builds on the application level interface of CAPI 2.0.

D Channel

The D channel transmits management information, such as the type of ISDN service in use or the ISDN number of the communications partner. The bandwidth is 16 kbit/s for the basic rate interface (BRI) and 64 kbit/s for the primary rate interface (PRI). In ISDN, charge information (AOCD, AOCE) and the caller's number can be transmitted over the D channel. In Germany, these features must be specifically requested.

DSS1

A standardized European D channel protocol. All new ISDN lines in Germany use DSS1.

Filters (special)

In practice, certain applications constantly exchange network packets, which in the case of WAN connections over ISDN could lead to connections being set up unnecessarily often. For this reason, the NT/MPRI contains special packet filters to intercept network overhead traffic. In this way, SNMP packets in UDP and TCP can be filtered, for example, as well as NetBIOS broadcasts in IP and IPX, so that they are not transmitted over ISDN. The actual filtering criteria are the source and destination ports. These filter mechanisms are not negotiated with the remote site, but set in the NT/MPRI.

Firewall

The NT/MPRI's firewall filters protect against unauthorized access to the network and select the resources and services to be made available for outside access. Various mechanisms are used to implement firewalls. The NT/MPRI's firewall is implemented as a packet filter. The NT/MPRI checks every incoming and outgoing data packet against the security criteria. These include the packet's source and destination addresses (network address and mask) as well as the service (such as FTP). The security criteria are saved in global IP filters and destination filter profiles. The filter rules specify what measures are to be taken with a packet: send it through, simply discard it, or stop it and send back an error message. See also the section "IP-Masquerading / Network Address Translation (NAT)" on page 118.

FTP (File Transfer Protocol)

FTP is a manufacturer-independent file transfer protocol, not specific to any computer type or operating system. FTP builds directly on TCP, at Layer 4 (Transport Layer) of the OSI reference model. The protocol is described in RFC 959.

ICMP (Internet Control Message Protocol)

ICMP is located at Layer 3 (Network Layer) of the OSI reference model. It is used for error and information messages (such as information on routing and call destination addresses). A widely used function based on ICMP is ping. ICMP builds on the Internet Protocol (IP) as if it were a higher-layer protocol. Before being sent, ICMP data are always supplied with a complete IP header. The data section that follows the header contains the ICMP messages.

IP (Internet Protocol)

Within the TCP/IP protocol family, IP is responsible for relaying data. In general, it has the function of regulating data transmission between different networks. IP's tasks include:

- data packet service
- fragmentation of data packets
- selection of transmission parameters
- addressing function
- routing between networks
- specification of higher protocols

IP does not provide a secure connection (no end-to-end control); it depends on the protocols of the higher levels. This means that lost or rejected data packets cannot be regenerated and re-transmitted. The IP also is not concerned with delivering data packets to the recipient in the correct order. This is the responsibility of the transport layer (Layer 4) of the OSI reference model.

IP builds directly on Layer 3 (Data Link Layer/Security Layer) of the OSI reference model. The protocol is defined in RFC 791.

IP Addresses, see “TCP/IP Addresses” on page 123

IP Mask, see “TCP/IP Addresses” on page 123

IP-Masquerading / Network Address Translation (NAT)

One network, one IP address: With IP Masquerading, one “official” IP address is sufficient for the communication between the private LAN and the public Internet. The NT/MPRI processes the IP addresses in the TCP, UDP and ICMP packets such that, effectively, only one IP address is visible to the Internet. This means that these hosts of a private LAN can use internal (“unofficial”) IP addresses for communication with the Internet. It is considerable more difficult to break into a system protected in this way than it is to surmount a good packet-based firewall.

IPX (Internetworking Packet Exchange Protocol)

A network protocol developed by Novell with which data packets can be exchanged quickly and reliably between two network computers.

IPX Addresses

A hexadecimal number identifying a server in a network. Each server must have a unique internal IPX network number. This number consists of eight hexadecimal digits (1 to FFFFFFFE). If several successive IPX addresses are to be compiled (e.g. when working with the RIP filter in the NT/MPRI), a mask may be defined as well.

For example, to compile the successive IPX addresses 11111111 to 1111111F, enter the address as 11111110 and the mask as FFFFFFF0. To compile the IPX addresses 11111110 to 11111113, enter the address as 11111110 and the mask as FFFFFFFC.

Keep-Alive Packets

Keep-alive packets are broadcast periodically to the entire network to check whether a client is still active, for example. If the sending station does not receive a reply, it discontinues the logical connection.

Logical ISDN Connection

A logical ISDN connection is created when the first physical ISDN connection is set up and connection parameters are negotiated. These connection parameters are valid for the duration of the logical ISDN connection, and include the network protocol to be used, whether authentication is to be carried out, and connection management parame-

ters such as spoofing mechanisms or channel bundling. Depending on the configuration, the logical ISDN connection will either be cleared down along with the physical one, or continue to exist if so agreed with the remote site.

Metric

Metrics are abstract numbers used to evaluate routes. If multiple routes are defined and available to a given destination, the NT/MPRI selects the route with the lowest total metric value, this being classified as the "best route".

MSN (Multiple Subscriber Number)

In Euro-ISDN (the D channel protocol DSS1), Multiple Subscriber Numbers serve to distinguish among several terminals on the same S_0 bus (or between several CAPI applications on the same PC). Deutsche Telekom AG assigns a standard ISDN line three Multiple Subscriber Numbers.

NCP (NetWare Core Protocol)

A protocol for managing communication between the client and the server in a Novell network.

NetBIOS (Network Basic Input/Output System)

A standard for network communication which is independent of specific transport types. NetBIOS is the standard interface in Microsoft networks and can be transported over both IP and IPX. NetBIOS uses numerous broadcasts, which can be intercepted by the NT/MPRI's filters to reduce connection costs.

Network Address Translation (RFC 1631)

With NAT, the NT/MPRI keeps a table that maps external IP addresses and port numbers to internal IP addresses and port numbers. In this way incoming mail (SMTP) connections for example can be directed by the NT/MPRI to specified hosts in the private LAN even if the Internet connection uses a dynamically assigned IP address.

Outside Line Access

The Outside Line Access is the prefix dialed in a Private Branch Exchange (PBX) to obtain an outside line. This is usually "0". Enter the Outside Line Access for each ISDN-Controller into the NT/MPRI

(“Configuration / Server Settings / ISDN-Controllers”). The Outside Line Access is then automatically prefixed to outside numbers on dialing.

PAP (Passwort Authentication Protocol)

One of two protocols for PPP authentication. A name and a password for the remote site must be configured at the site requesting authentication. The remote site must also have this name and password entered in its settings. During PAP authentication, the name and password are transmitted in plain text, and the remote site checks whether they match its own settings. If they do, the connection is set up.

Physical ISDN Connection

With a physical ISDN connection, one or more B channels are actually set up, and charges are incurred. The physical ISDN connection is always set up in accordance with the logical ISDN connection, i.e. the negotiated connection parameters are used.

Ping (Packet InterNet Groper)

A program to test whether a host can be reached. The program sends an ICMP query to an IP host and waits for an appropriate answer. With the aid of the “-w” option after the “ping” command, you can specify how many milliseconds the program should wait for an answer (timeout). Because it can take a few seconds to set up the connection over ISDN and for the remote site to negotiate, a timeout of 5000 ms is recommended for a ping over ISDN.

PPP (Point-to-Point-Protocol)

A data communications protocol for switched networks such as ISDN which provides data transfer independent of specific network protocols. The protocol consists of a number of standards and sub-protocols. These describe the structure of transmitted data for various networks. The objective is to allow communications equipment from different manufacturers to use a uniform procedure for communication. PPP over ISDN is described in RFC 1618.

Proxy ARP

Proxy ARP is not actually a protocol, but an NT/MPRI extension to answer ARP queries using the current routing table, instead of forwarding the queries to remote stations over ISDN. This allows remote users or small networks to use the same IP address range that is valid on the NT/MPRI's LAN segment, thus simplifying configuration.

RIP (Routing Information Protocol)

The Routing Information Protocol (RIP) is used to exchange routing information between networks (IP and IPX). An RIP router is a computer or other hardware component which transmits routing information (such as network addresses) and relays IP frames in connected networks. RIP allows a router to exchange routing information with other routers in the network environment. If a router detects any change in the network (such as an unavailable router), it relays the information to other routers. In addition, routers send regular RIP broadcast packets containing all the routing information they can provide. These transmissions serve to synchronize all routers in the network.

Route

A route describes the path along which a data packet must travel in order to reach its call destination. A return route must be defined at the receiving end so that a reply packet can be sent back to the initial sender of the data packet.

SAP (Service Advertising Protocol)

A protocol in NetWare environments. NetWare servers use SAP to inform all stations in the network what services are available.

Short-Hold Mode

The short-hold mode entails the physical disconnection of idle ISDN links after a specified time. Charges are incurred for physically active ISDN connections, regardless of whether or not data is being transmitted. Because ISDN connection setup is so fast (1 to 2 seconds), it is feasible to clear down the physical ISDN connection if no data has traveled over the line for a certain time. Depending on the configuration, the logical ISDN connection remains. As soon as data is queued for transmission, the physical connection is reestablished. This takes place transparently for the network user.

SMTP (Simple Mail Transfer Protocol)

SMTP is a standard protocol for exchanging electronic mail (E-mail) between different computers. SMTP uses TCP port 25. It has a simple structure and only supports the sending of e-mail over a data network. The protocol is described in RFC 821.

SNMP = Simple Network Management Protocol

In the early 1980s the ISO produced a management model which was documented in the OSI Management Framework (DIS 7498-4). This model's main objective is to allow seamless interoperation between the network management products of different manufacturers. Within the standard, aids are defined for obtaining information about the network's current state and for controlling individual components.

The ISO describes the management area as objects and attributes. The sum of all manageable objects makes up the Management Information Base (MIB). Communication between a Network Management Station (NM Station) and the manageable objects is conducted via Agent Stations. SNMP controls data transmission between the Agent Station and the NM Station over TCP/IP.

In addition to HTML management, the NT/MPRI also offer the option of providing standard information over SNMP. SNMP access can be controlled under the "Configuration / Security" menu.

Spoofing

In practice, certain applications exchange network packets constantly, which in the case of WAN connections over ISDN would lead to connections being set up frequently. Certain types of packets especially in the field of NetWare applications, such as watchdog packets for example, require confirmation from the remote site and as a result cannot be simply filtered out of the data stream and discarded by theNT/MPRI , since the application would then no longer be recognized by the server. Spoofing means that the NT/MPRI simulates the client's answer to such packets locally.

The spoofing mechanisms used are negotiated during the connection set-up with the remote site in accordance with the PSCP Draft. If the remote site does not support spoofing, this function is disabled.

SPX (Sequenced Packet Exchange)

A protocol that enables two workstations or applications to communicate over a network. Like TCP, SPX is located at Layer 4 (Transport Layer) of the OSI reference model and ensures secure end-to-end communication. SPX uses NetWare IPX for data transmission. SPX ensures that the sequence of messages in the packet stream remains the same.

TCP (Transmission Control Protocol)

TCP is designed for the implementation of packet-switched networks. It builds immediately on the Internet Protocol (IP) and provides virtual connection services for correctly sequenced, secure transmission of user data. It ensures a reliable connection between two communications partners. TCP is published as RFC 793.

TCP/IP Addresses

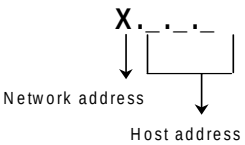
TCP/IP addressing is a permanent part of the Internet Protocol (IP). Internet addresses are written using decimal, octal or hexadecimal representation. The NT/MPRI uses "dotted decimal" notation, in which the decimal values of the individual bytes are separated from one another by periods. The entire set of Internet addresses, the address space, is divided into classes (A, B, C, D and E). Of these five address classes, only the first three are used. These classes are characterized as follows:

Class	Characteristics	Network address, decimal value
Class A address	few networks, many network nodes	0-127
Class B address	medium distribution of networks and network nodes	128-191
Class C address	many networks, few network nodes	192-223

Characteristics of IP address classes

Each IP address consists of two elements: the network address and the host or computer address. The sizes of these two components are variable; they are determined by the first four bits (of the first byte) of an IP address.

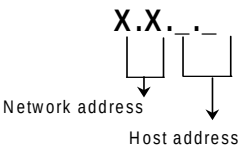
- **Class A addresses** consist of a one-byte network address and a three-byte computer address



Class A Address

Example: 88.120.5.120 (88 defines the network address; 120.5.120 the host address).

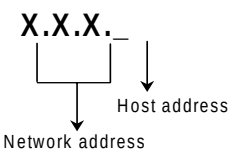
- **Class B addresses** consist of a two-byte network address and a two-byte host address:



Class B address

Example: 130.6.2.130 (130.6 is the network address; 2.130 is the host address).

- **Class C addresses** consist of a three-byte network address and a one-byte host address:



Class C address

Example: 195.15.15.1 (195.15.15 is the network address; 1 is the host address).

RFC 1918 (Address Allocation for Private Internets) designates the following blocks of the IP address range as suitable for private LANs:

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Subnet Masks (Masks)

By using subnet masks, the “host part” of an IP address class can be changed into a subnetwork part. This part then remains unchanged by other computers or routers. The subnet mask indicates which ranges are to be interpreted as subnet addresses and which as computer addresses. The subnet mask is often shown in dotted-decimal notation, but can also be expressed simply as the number of bits to be treated as a network address. For example, a Class A address, which has a standard subnet mask of 8 (i.e. 255.0.0.0, or eight of the 32 bits set), can be treated as a Class B address in combination with the subnet mask 16 (255.255.0.0) or a Class C address with the subnet mask 24 (255.255.255.0).

The following table summarizes this convention:

Range	Number of IP Addresses	Network Bits (of 32)	Subnet Mask
000-255	256	/24	255.255.255.0
000-127 128-255	128	/25	255.255.255.128
000-063 064-127 128-191 192-255	64	/26	255.255.255.192
000-031 032-063 064-095 096-127 128-159 160-191 192-223 224-255	32	/27	255.255.255.224
000-015 016-031 032-047 048-063 064-079 080-095 096-111 112-127 128-143 144-159 160-175 176-191 192-207 208-223 224-239 240-255	16	/28	255.255.255.240

Range	Number of IP Addresses	Network Bits (of 32)	Subnet Mask
000-007	8	/29	255.255.255.248
008-015			
016-023			
024-031			
032-039			
040-047			
048-055			
056-063			
064-071			
072-079			
080-087			
088-095			
096-103			
104-111			
112-119			
120-127			
128-135			
136-143			
144-151			
152-159			
160-167			
168-175			
176-183			
184-191			
192-199			
200-207			
208-215			
216-223			
224-231			
232-239			
240-247			
248-255			

Subnet masks in the NT/MPRI

UDP (User Datagram Protocol)

This protocol is located on Layer 4 (Transport Layer) of the OSI reference model and provides to the higher protocols a defined service for the transaction-oriented dispatch of data packets. UDP is equipped with just the minimum of protocol mechanisms for data transmission between communication partners. Unlike TCP, it does not guarantee end-to-end control; this means that it cannot ensure that data packets

are delivered directly to the recipient, duplicates are recognized, or that data packets are transmitted in the correct order. UDP is defined in RFC 768.

Index

M

N

O

P

R

S

T

U

W