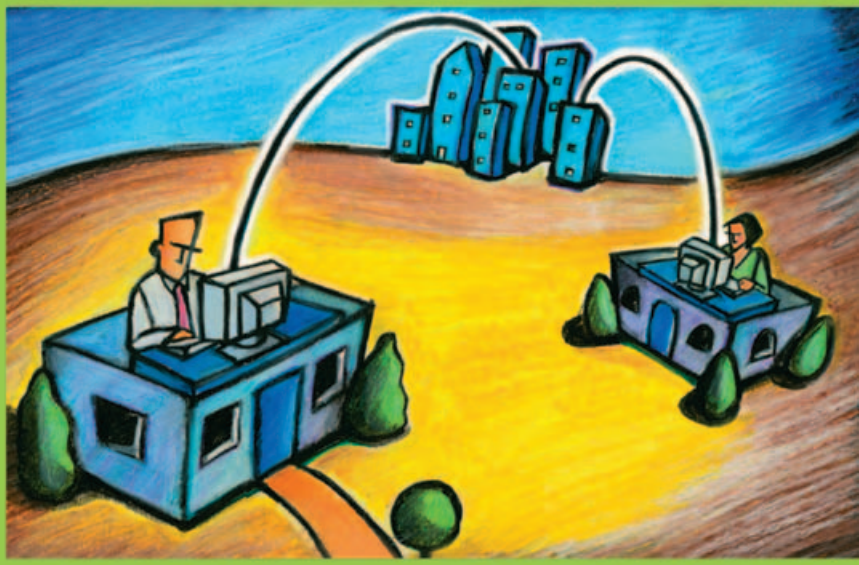
NETWAYS ISDN

- ISDN
- DSL
- Firewall
- VPN



AVM NetWAYS/ISDN

Remote Access for PCs and Notebooks

- Internet Access
- Remote Access

HIGH-PERFORMANCE COMMUNICATION BY ... AVM

NetWAYS/ISDN

Documentation release 11/2003

AVM Audiovisuelles Marketing
und Computersysteme
Alt-Moabit 95

10559 Berlin

AVM Computersysteme
Vertriebs GmbH
Alt-Moabit 95

10559 Berlin

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

Contents

1 Welcome to NetWAYS/ISDN 5

1.1 Why NetWAYS/ISDN? 5

1.2 Package Contents 11

2 Installation and First Steps 12

2.1 System Requirements 12

2.2 Installing NetWAYS/ISDN 13

2.3 Default Configuration 14

2.4 Getting Started 15

2.5 Removing NetWAYS/ISDN 19

3 Remote Access with NetWAYS/ISDN 20

3.1 Throughput Optimization 20

3.2 Cost Management 21

3.3 Security 31

3.4 Internet Connections 34

3.5 VPN Connections 36

4 NetWAYS/ISDN for Administrators 46

4.1 Automated Installation of NetWAYS/ISDN 46

4.2 Locking the Settings 49

4.3 The NetWAYS/ISDN Service 49

4.4 The NetWAYS/ISDN API 51

4.5 Supported Standards 52

5 Information, Updates and Support 54

5.1 Information Sources 54

5.2 Updates 55

5.3 Getting Assistance from AVM Support 55

Glossary 58

Index 74

Typographical Conventions

The following typographic conventions and symbols are used in this manual to make reading easier and to emphasize important information.

Highlighting

The table below explains the highlighting conventions used in this manual.

Highlighting	Function	Example:
Quotation marks	Keys, buttons, icons, tabs, menus, comands	“Start / Programs” or “Enter”
Capital letters	Path and file names in running text	DOKU\NETWAYS.PDF or CAPIPORT.HLP
Pointed brackets	Variables	‹CD-ROM drive›
Typewriter font	Information to be typed in using the keyboard	`a:\setup`
Gray italics	Hints, instructions and warnings, always accompanied by a symbol in the margin	*... For more information see ...*

Symbols

The following graphic symbols in the manual always appear in connection with text printed in gray italics:

This symbol indicates useful tips and supplementary information.

The exclamation mark designates sections which contain important information.

This symbol indicates important instructions that must be observed to avoid malfunctions.

1 Welcome to NetWAYS/ISDN

NetWAYS/ISDN integrates remote workstations and mobile computers in the company network. In this way all classic LAN applications can be used over ISDN: client/server applications, Internet applications, e-mail, database applications, and terminal emulation programs.

The digital telecommunications network ISDN offers ideal features for remote access: widespread availability, high bandwidth, secure and robust connections, and cost efficiency.

ADSL is a communication technology that permits Internet access with high bandwidth over ordinary telephone cables.

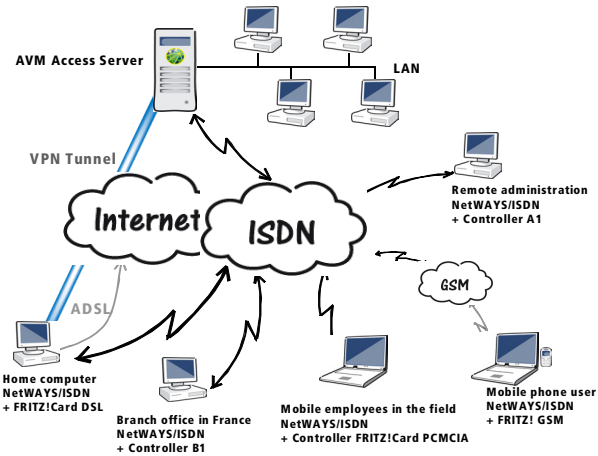
As demands for mobile remote network access increase, the digital cellular network GSM (Global Systems for Mobile Communication) and HSCSD (High-Speed Circuit-Switched Data) are used alongside ISDN.

1.1 Why NetWAYS/ISDN?

NetWAYS/ISDN is a software product that provides transparent access to LANs and the Internet for stand-alone PCs and mobile computers equipped with AVM ISDN-Controllers. Employees in branch locations or telecommuters can work with the company LAN using NetWAYS/ISDN just as if they were on site, and access all of the company network's resources.

Field sales employees, for example, can query databases on the company's servers or in the Internet. Telecommuters can use network file and print servers from their home offices, and technicians can perform remote administration using large-scale applications in the company network.

The following diagram illustrates the versatile uses of NetWAYS/ISDN.

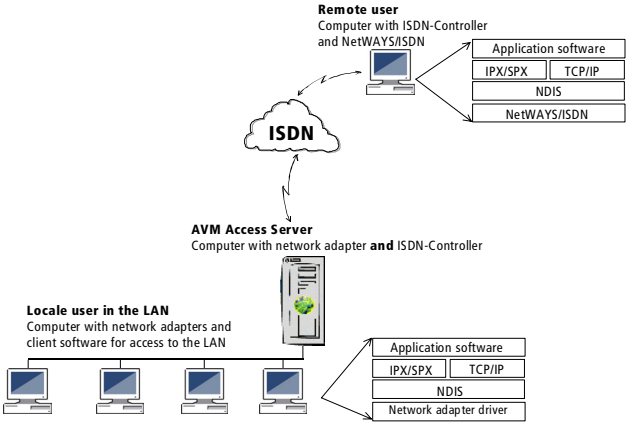


Applications of NetWAYS/ISDN

Technology

NetWAYS/ISDN on the remote computer communicates with the LAN transparently over ISDN or GSM. The network protocols are bound to NetWAYS/ISDN acting as a network adapter. The networking interface conforms to the NDIS standard. NDIS stands for Network Device Interface Specification, a standard for communication between network adapters (hardware) and network protocols (software). Thanks to NDIS support, any TCP/IP or IPX/SPX-based networking application can be used over ISDN. The network settings of remote NetWAYS/ISDN computers are only marginally different from those of directly connected LAN computers.

The following diagram compares how two computer are connected to a LAN. One is a NetWAYS/ISDN computer with RAS (Remote Access Service) over ISDN; the other is a conventional LAN workstation.



Comparison between a conventional LAN workstation and a remote computer connected over ISDN

The dial-in server for NetWAYS/ISDN at the LAN or Internet end may be one of AVM's market-leading remote access servers, or any other manufacturer's RAS product that supports the "PPP over ISDN" standard.

All classic LAN applications can be used on the remote computer. Such applications may include client software for Microsoft or NetWare networks, web browsers, e-mail clients, and terminal emulation programs.

Yet NetWAYS/ISDN, in cooperation with the remote system, does much more than an ordinary network adapter driver. The software provides many advanced functions that define the state of the art in remote access:

- reduced connection costs
- increased throughput
- greater security

Cost Management

One of the primary objectives in designing NetWAYS/ISDN was to minimize the ISDN connection costs. NetWAYS/ISDN uses proven techniques optimized for ISDN to cut connection costs to the bare minimum. This means that remote access is as economical as possible. In “Short-Hold Mode”, the ISDN connection is cleared down whenever idle. When it is needed again—that is, when data needs to be transferred—the ISDN connection is automatically dialed up again. Connection charges thus accrue only for the amount of data transmitted, not for the duration of a session.

NetWAYS/ISDN automatically detects the billing rate for the current time of day and can adjust the inactivity timer accordingly. This feature is especially significant in reducing costs, given the complex rate structure of ISDN network operators. Moreover, NetWAYS/ISDN and AVM’s remote access servers suppress the network operating system's redundant overhead data traffic on the ISDN link. This is done using proven and sophisticated protocol filtering and spoofing techniques.

NetWAYS/ISDN supports cost allocation. This feature ensures that the ISDN connection costs are charged to a specific end of the connection. For example, the central LAN may be configured to bear the charges for all connections, regardless of which site initiates them.

NetWAYS/ISDN gives users control of the connection costs through monthly use accounting and connection cost budgets.

Speed

With 64 kbit/s per channel, ISDN provides sufficient native bandwidth for today's client/server applications. Thanks to on-the-fly data compression and header compression, NetWAYS/ISDN achieves a further performance boost. These techniques permit speeds of up to 240 kbit/s, depending on the type of data transported. Moreover, two B channels can also be bundled to increase bandwidth still further.

ADSL permits fast Internet access over the same cable as a telephone line. Data communication takes place at up to 6 Mbit/s downstream (that is, from the Internet to the user) and up to 640 kbit/s upstream.

Security

Security too has been a top priority in the development of NetWAYS/ISDN. Authentication between the remote client and the LAN server takes place even before data packets can be exchanged at the network protocol level. NetWAYS/ISDN supports two types of authentication: PAP (the Password Authentication Protocol) and CHAP (the Challenge Handshake Authentication Protocol). NetWAYS/ISDN uses "Caller ID" as an additional security check. At the LAN end, AVM products permit the use of access controls and packet filters. Furthermore, the network operating system's user-level security mechanisms are also applied.

VPN

Remote access to a LAN can also be implemented with NetWAYS/ISDN over a VPN link. IPsec is used as the network protocol to meet the following security requirements:

- Authenticity: when a connection is opened, the communicating parties identify each other to ensure that all data comes from the authentic source.
- Privacy: data communication is encrypted, so that no third party can eavesdrop.
- Integrity: a digital signature on each packet ensures that the data is not manipulated in transmission.

Interoperability

At the LAN end, the AVM Access Server is an especially advantageous dial-in point for remote access with NetWAYS/ISDN.

In addition, NetWAYS/ISDN guarantees interoperability with remote access servers that support the PPP over ISDN standard. NetWAYS/ISDN users will find this standard ensures convenient connections to Internet Service Providers. NetWAYS/ISDN not only processes the IP protocols, but also transmits IPX protocol packets directly over PPP. PPP authentication is fully supported in accordance with PAP and CHAP.

The interoperability standard PPP over ISDN is defined in the Internet standards documents, or RFCs (Requests for Comments). The RFCs supported by NetWAYS/ISDN are listed in the chapter "NetWAYS/ISDN for Administrators" from page 46. These techniques are integrated both in NetWAYS/ISDN and in the AVM Access Server.

Logs and Use Statistics

Comprehensive logs and use statistics provides detailed information about current and past connections at any time, permitting precise analysis of all NetWAYS/ISDN activities.

Easy to Install and Configure

NetWAYS/ISDN is easy to install with the help of a Setup Wizard. Furthermore, administrators can prepare an automatic installation process to integrate pre-defined locations and call destinations in the program without configuration by the user.

NetWAYS/ISDN can also be configured to activate a network connection automatically when the computer starts, with no user interaction. The graphic user interface of NetWAYS/ISDN makes operation intuitive. Furthermore, custom applications are also possible thanks to a documented application programming interface (API). For details about the API integrated in NetWAYS/ISDN, see the chapter "NetWAYS/ISDN for Administrators" from page 46.

1.2 Package Contents

The NetWAYS/ISDN package contains:

- 1 NetWAYS/ISDN v6.0 CD-ROM
- 1 NetWAYS/ISDN v6.0 manual

If either of these components is missing, please contact your supplier.

If the computer for which you have purchased the NetWAYS/ISDN license does not have a CD ROM drive for installation, you may copy the necessary software from the NetWAYS/ISDN CD to floppy disks for this non-commercial purpose. AVM does not ship the NetWAYS/ISDN software on floppy disks.

2 Installation and First Steps

This chapter describes how to install and remove and how to start and stop NetWAYS/ISDN. Furthermore, the section “Getting Started” on page 15 explains how you can set up a test connection to the AVM Data Call Center, and what to do to set up an Internet connection.

2.1 System Requirements

Before you can install NetWAYS/ISDN, the following prerequisites must be met:

NetWAYS/ISDN Computer Hardware and Software

- Industry standard PC with at least 32 MB of RAM
- Intel Pentium or compatible CPU at 90 MHz or above
- Windows XP, 2000, or NT, or Windows Me or 98. For Windows XP, 2000 and NT, the current Microsoft Service Pack must be installed.
- AVM ISDN-Controller or AVM FRITZ!Card GSM
- for ADSL connections: an AVM FRITZ!Card DSL, or an external ADSL modem and an Ethernet adapter (PPPoE)

The AVM ISDN-Controller must be installed before you install NetWAYS/ISDN. Its driver software must be loaded automatically when Windows starts. See your ISDN-Controller manual for further information.

Before installing NetWAYS/ISDN in Windows XP, 2000 and NT, you must install the current service pack from Microsoft on your computer. The latest service pack must be reinstalled after each software installation or configuration change that requires the Windows NT CD-ROM.

Remote Access Server Hardware and Software

- Windows XP, 2000, or NT server with the AVM Access Server and an AVM ISDN-Controller B1, T1, T1-B, C2 or C4
- any remote access server that supports PPP over ISDN

2.2 Installing NetWAYS/ISDN

To install NetWAYS/ISDN, proceed as follows:

1. Insert the NetWAYS/ISDN CD in your CD-ROM drive.

   The CD introduction starts automatically.

2. Start by selecting the language in which you want to install NetWAYS/ISDN.

3. Select the operating system you are using.

4. In the sign-on window, select “Install NetWAYS/ISDN” to start the Setup program.

5. Click “Next” in the NetWAYS/ISDN Setup program’s sign-on dialog to proceed with the installation.

6. In the dialog that follows, enter your NetWAYS/ISDN Product Identification Code. The Product Identification Code is printed on the back of the NetWAYS/ISDN CD case.

7. In the “Choose Destination Location” dialog, specify the folder in which you want to install NetWAYS/ISDN’s program files.

   The Setup program suggests the default path C:\ PROGRAM FILES\AVM\NETWAYS. Click “Browse...” if you would like to specify a different folder.

8. The Setup options you have selected are summarized in the “Start Copying Files” dialog. If you want to change any of these settings, click “Back” to return to the previous dialog.

   When all the settings are correct, click “Next” to install NetWAYS/ISDN.

The NetWAYS/ISDN program files are then copied to your hard disk.

In Windows XP, the installation process may be interrupted by an operating system warning that refers to the Windows logo test. Ignore this warning and continue the installation.

9. When the installation has been completed, restart your computer.

When the computer has been restarted, NetWAYS/ISDN is ready to use. The Programs folder in the Start menu contains the new program group “NetWAYS/ISDN”. This group contains a shortcut named “NetWAYS/ISDN”, which opens the NetWAYS/ISDN window, and a shortcut to the “Readme” file containing the latest information about NetWAYS/ISDN.

For instructions on starting and stopping NetWAYS/ISDN, see the section “The NetWAYS/ISDN Service” on page 49.

2.3 Default Configuration

NetWAYS/ISDN is integrated in Windows as a network adapter driver. This driver is automatically configured during installation. The Windows network settings are modified as follows:

- The network protocol TCP/IP is automatically bound to NetWAYS/ISDN.
- The network protocol IPX/SPX is also bound to NetWAYS/ISDN, if IPX/SPX was installed before the NetWAYS/ISDN installation.

After the NetWAYS/ISDN installation, the pre-configured call destination “Fast Internet over ISDN” is available in the NetWAYS/ISDN window. The following settings are configured for this call destination:

- The filtering and spoofing mechanisms for IP are activated.
- Data compression is set to “Negotiate automatically”.
- Header compression is activated.

- Idle physical connections are dropped after 50 seconds.
- The logical connection is terminated at the same time.
- Channel bundling is set to “Manual”.
- Cost allocation is set to “Caller”.
- The CLI number (Caller ID) is not used for authentication.
- NetWAYS authenticates itself with the ADC using the user name “Gast”, and without a password.

2.4 Getting Started

When you have installed and started NetWAYS/ISDN, you can set up a test connection to a dial-in server in the AVM Data Call Center (ADC) using the pre-configured call destination.

Before you can activate a test connection to the ADC or to AVM’s web site, you must configure a location in NetWAYS/ISDN. For detailed instructions, see the Online Help.

If you want to monitor the progress of an existing connection, NetWAYS/ISDN offers two ways to do so.

- Select the “Statistics...” command in the “Monitoring” menu. The Statistics dialog appears. This dialog provides complete information about the current connection.

  Or

- Select the “Cockpit” command in the “Monitoring” menu. The “Cockpit” display appears. The Cockpit indicates whether a connection is currently active, when the physical connection will be cleared down (if it remains idle), and how many B channels are in use.

First Connection: Testing TCP/IP

To set up a connection to the ADC using the network protocol TCP/IP, perform the following steps:

1. Open the NetWAYS/ISDN window.
2. Select the call destination “Fast Internet over ISDN”.
3. Select the “Connect” command in the “File” menu.

   If the connection is successfully dialed up, the status information “Physically connected” appears in the status bar of the NetWAYS/ISDN window.
4. Open a Web browser and enter the address of AVM’s WWW or FTP server in the “Address” bar:

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

   `ftp://ftp.avm.de`

From the AVM home page or the root directory of the FTP server you can browse to other documents.

Going Online with NetWAYS/ISDN

Before you can connect to the Internet, certain conditions must be met in your NetWAYS/ISDN settings and by your Internet Service Provider.

Internet Service Provider Prerequisites

- The provider must offer access over ISDN and/or ADSL.
- The dial-in server should support “synchronous PPP” in accordance with RFC 1618.
- Authentication with the Internet Service Provider can take place using Caller ID or a user name and password.
- The connection to your Internet Service Provider may use either a static or a dynamic IP address. IP masquerading is recommended on the connection to the Internet.

Local System Prerequisites

When creating a call destination for your Internet Service Provider, please observe the following instructions:

- Deactivate the network protocol IPX/SPX in the NetWAYS/ISDN call destination settings.
- Set the delay before an idle physical connection is dropped to more than 10 seconds. At peak use times, dialing up the connection to an Internet Service Provider can take a while. By setting the idle timeout to a longer delay, you can ensure that the connection set-up is not aborted due to a timeout.
- Certain Internet Service Providers require you to enter specific proxy server and port settings. For details, consult your system administrator or your Internet Service Provider.
- Make sure you enter the dial-in number, the user name and the password correctly.

Configuring an Internet Call Destination

1. In the “Settings” menu, select “Call Destinations / New call destination...”. The NetWAYS/ISDN wizard starts and assists you in configuring an Internet connection.
2. In the “Type of network” dialog, select the option “Internet”.
3. In the dialog that follows, select the type of Internet service provider used.
4. Select the desired Internet Service Provider.

   The Internet Provider Selection dialog appears only if you have selected the option “Internet Providers with Registration” or “Internet Providers without Registration” in the pre-selection dialog.
5. The name of the Internet Service Provider is entered for you as the call destination name. You may use this suggestion or edit the name as desired.

6. Enter the authentication information for your Internet access account.

7. Click “Next”, then “Finish” to complete the configuration.

   An icon representing the Internet connection now appears in the NetWAYS/ISDN window.

Importing a VPN Connection Configuration Created with the AVM Access Server

The AVM Access Server allows you to export the configuration data for a VPN user to a file. This file can then be given to the VPN user by e-mail or floppy disk, and imported on the NetWAYS/ISDN computer. The VPN call destination can be automatically configured simply by importing the file.

1. Insert the floppy disk containing the export file created by the AVM Access Server.

2. In the “File” menu, select “VPN import”. The Windows file selection dialog opens.

3. Select the file with the file name extension .EFF on the floppy disk, and confirm your selection by clicking “Open”.

4. Enter the password that was assigned when the export file was created on the AVM Access Server.

Activating an Internet Connection

To dial up the connection to the Internet, proceed as follows:

1. Start NetWAYS/ISDN.

2. In the main NetWAYS/ISDN window, select the call destination icon for your Internet Service Provider.

3. Select the “Connect” command in the “File” menu.

4. When the connection has been successfully dialed up, the status information “Physically connected” appears in the status bar of the NetWAYS/ISDN window.

5. Open a Web browser.

You can now visit any page in the World Wide Web.

2.5 Removing NetWAYS/ISDN

To save all the settings you have configured in NetWAYS/ISDN, make a backup copy of all files in the program installation folder with the file name extensions .DAT and .IDX. After you have reinstalled the same version of NetWAYS/ISDN, simply copy these files back to the NetWAYS/ISDN installation folder. Your settings are then available once more.

To remove the software, proceed as follows:

Removing NetWAYS/ISDN in Windows XP and 2000

1. Open the “Control Panel” icon in Windows XP in the “start” menu, or under “Start / Settings” in Windows 2000. Open the “Add or remove Programs” icon.
2. Make sure that the “Change or Remove Programs” button is selected in the column at left. In the list of currently installed programs, select “AVM NetWAYS/ISDN” and click the “Change/Remove” button.
3. Confirm that you want to remove the selected component by clicking “Yes” at the safety prompt.
4. Follow the instructions displayed on the screen. When a message box informs you that the software has been successfully removed, close the “Change/Remove Programs” dialog by clicking “OK”.

Removing Software in Me, 98, NT

1. Select “Settings / Control Panel / Software” in the Windows Start menu.
2. On the “Install/Uninstall” dialog page, select the entry “AVM NetWAYS/ISDN” and then click the “Add/Remove” button.
3. Click “OK” to complete the removal of NetWAYS/ISDN.

3 Remote Access with NetWAYS/ISDN

This chapter explains the basic principles of NetWAYS/ISDN, and provides detailed information about the features, functions and configuration options.

For complete information about individual commands and parameters, see the Online Help.

3.1 Throughput Optimization

Each ISDN B channel permits data throughput of 64 kilobits per second. Because many applications today demand higher throughput, NetWAYS/ISDN incorporates two efficient compression techniques to make optimum use of the available bandwidth: header compression and payload data compression. In ADSL Internet access, data communication takes place at up to 6 Mbit/s downstream (that is, from the Internet to the user) and up to 640 kbit/s upstream.

Header Compression

Every data packet in network communication has a header which contains the source and destination addresses. By compressing this header NetWAYS/ISDN increases the throughput rate enormously, especially when packet sizes are small. IPX headers can be compressed from 36 bytes to as little as 2 bytes. TCP/IP headers can be compressed from 40 bytes to three.

Data Compression

The payload data of the packet can also be compressed for transmission. NetWAYS/ISDN uses the data compression standards V.42bis, Stac LZS (RFC 1974) and MPPC (RFC 2118). These techniques achieve compression ratios of up to 8 to 1, depending on the data content.

Channel Bundling

In addition to compression, NetWAYS/ISDN can also optimize throughput by using both ISDN B channels for the data connection. Channel bundling attains a bandwidth of 128 kbit/s (2 x 64 kbit/s). The following channel bundling options can be configured:

Channel bundling setting	Description
None	The connection is set up using only one B channel.
Static	The connection always uses two B channels.
Dynamic	The second B channel is automatically added as required for the data traffic load. When the data traffic load decreases, the second B channel is automatically cleared down.
Manual	The second B channel can be added to the existing connection as needed by clicking a button.

Please note that using both B channels doubles the connection costs. You should therefore consider carefully whether the data to be transferred justifies the use of channel bundling.

3.2 Cost Management

ISDN connections, unlike local network media, cost money to use. ISDN operators charge by the duration of the dial-up connection, not by the volume of data transferred. NetWAYS/ISDN uses a number of intelligent techniques to reduce ISDN connection costs.

Physical Inactivity Timeout

To reduce connection charges, the inactivity timeout (Short-Hold Mode) clears down an ISDN connection automatically if no data has been transferred for a certain period of time. When data needs to be transferred again, NetWAYS/ISDN

automatically dials up the connection. Thanks to the fast dial-up times in ISDN (1 to 2 seconds), this operation is hardly noticeable.

The time before the idle physical connection is cleared down (the inactivity timeout) can be controlled either as a fixed delay setting, or by charge profiles.

Inactivity Timeout

If no data communication takes place during a specified delay, the ISDN connection between the NetWAYS/ISDN computer and the remote network is cleared down. This delay can be determined in two ways:

- Statically

  You can specify a fixed delay before an idle connection is cleared down.

- Using the self-configuring timer

  NetWAYS/ISDN can adjust the timeout delay itself. In this case the delay before the idle physical connection is cleared down is not fixed. Instead, NetWAYS/ISDN sets the inactivity timeout based on the charge information received from the ISDN line. The inactivity timeout is then closely aligned to current charge interval. This feature in NetWAYS/ISDN is called the “self-configuring timer”.

Please note that, in order to use the “self-configuring timer” feature, your ISDN line must provide charge information during the connection. Have your ISDN provider enable this service on your line. If your ISDN line is a PBX extension, the PBX must also forward the charge information.

Inactivity Timeout Using a Charge Profile

NetWAYS/ISDN can use charge profiles to control how long it waits before clearing down an idle physical connection. A charge profile contains information about the length and cost of connection charge intervals. These charge rates are dependent on geographic dialing areas, and change with the time of day.

Predefined charge profiles are supplied with NetWAYS/ISDN for German rates. These profiles reflect the usual rates applied to Deutsche Telekom's standard ISDN line offering.

NetWAYS/ISDN also allows you to create your own charge profiles or edit an existing one to suit your requirements, by adding your national holidays for example.

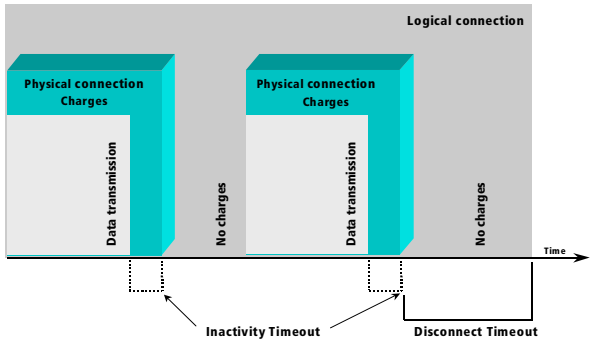
Logical Connection Timeout

A logical network connection can be maintained after the physical connection has been cleared down due to an inactivity timeout. The logical connection ensures that the physical connection can be automatically dialed up again, with the connection parameters already negotiated, when data needs to be transferred.

You can specify how long a logical connection is maintained if idle. As long as this delay is not exceeded, certain connection parameters negotiated with the remote system remain in effect, and the remote access server keeps a dial-in port and network resources reserved for the NetWAYS/ISDN client computer. The remote access server must also support logical connections, of course.

If the specified time limit for the logical connection has elapsed without any further physical connections, then the port is released for other applications or connections.

The following diagram illustrates the relationship between data communication, the physical inactivity timeout, and the logical connection timeout.



Physical and logical connection timeouts, with fixed inactivity timeout delay

Filters and Spoofing

Network clients, servers and applications exchange not only user data, but also network control information. This kind of communication allows a server to test whether the connections to its clients are active, for example.

In such cases, messages that are broadcast throughout the network would normally be transported to remote computers as well.

Ordinarily this results in the physical connection remaining permanently dialed up, with costs accruing continuously. In order to prevent that, NetWAYS/ISDN uses filters and “spoofing” mechanisms to minimize the redundant network traffic over the ISDN link.

Many network overhead packets and control messages are not absolutely necessary in order for the remote computer to operate in the LAN, and can be filtered out of the traffic over the ISDN line.

Which packets and network protocols are affected by filters and spoofing mechanisms depends on the remote access server’s features. The AVM Access Server supports all of the features described here.

NetWAYS/ISDN provides the following filters for the IPX and IP protocols:

- SNMP

  SNMP (Simple Network Management Protocol) is a common protocol used to transport network management information. SNMP packets are used for centralized monitoring of network resources. These packets transport status and alarm messages from network components such as workstations, servers and routers. SNMP can be transported by IP and IPX packets. When this filter is activated, SNMP packets over IP or IPX are filtered out and not transported over ISDN.

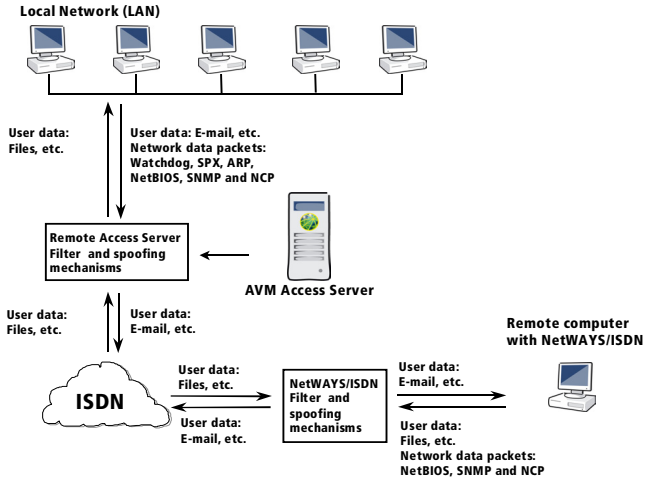
- NetBIOS

  NetBIOS is a command set used by certain applications for network communication. NetBIOS can be transported both over IPX and over IP, and is the protocol used by Windows file and printer sharing. To prevent these packets from being transmitted over ISDN, activate the NetBIOS over IPX or the NetBIOS over IP filter.

If there are Windows XP, Me, 2000, 98 or NT computers acting as servers in the LAN, then you must allow NetBIOS packets to be transported over ISDN in order for these servers to be accessible. Although communication in Microsoft networks is independent of the transport protocol, it depends on NetBIOS.

Spoofing

Some types of packets exchanged between clients and servers must be acknowledged by the remote system, and cannot be simply filtered out of the data stream. Otherwise, communication between the server and the remote client would no longer function correctly. Spoofing mechanisms can be used by the NetWAYS/ISDN computer and the remote access server to intercept such packets and acknowledge them locally, simulating a reply from the system at the other end of the ISDN line. In this way such overhead packets can be kept out of the ISDN traffic without interrupting an existing logical connection.



Filters and spoofing mechanisms in data communication

The following spoofing mechanisms are available to reply to LAN overhead packets, depending on the network protocol used (IPX or IP):

- Watchdog spoofing

  NetWare servers send out watchdog packets at regular intervals to verify that the clients logged in on the server are still active. These watchdog packets are intercepted in the LAN by the AVM Access Server. The Access Server simulates an acknowledgment by the remote computer, without activating the connection to it.

- SPX spoofing

  Many LAN applications use IPX/SPX. SPX servers and clients exchange “keep-alive” packets at regular intervals to verify that a given application is still active. SPX packets must be acknowledged at both ends in order for the logical SPX connection to be maintained.

  If SPX spoofing is activated, SPX packets are acknowledged locally by the remote access server in the LAN, and not forwarded over ISDN to the remote client. Keep-alive packets generated by an application on the client

PC are likewise acknowledged locally by NetWAYS/ISDN, and not sent over ISDN to the remote network.

- NCP spoofing

  NCP (NetWare Core Protocol) spoofing prevents NCP requests such as “Get Directory Path” or “End of Job” from being sent over ISDN. Such NCP requests are frequently generated by Windows applications opening a dialog to browse the file system, as when the command “File / Open” is selected in Microsoft Word for example. When NCP spoofing is activated, the remote computer prevents unnecessary NCP request (such as update requests) from being transmitted to all servers on which the client has mapped a network drive. Instead, the replies to the requests are simulated locally.

- ARP spoofing

  ARP (Address Resolution Protocol) is used to obtain the Ethernet hardware address (or “MAC address”) of the interface that corresponds to a given IP address.

  Normally, ARP transmits a message in the IP network every six minutes to ascertain IP and MAC address mapping. The response to a ARP request contains the IP address with the corresponding hardware address. When clients are connected over ISDN, ARP could cause high connection costs, since the ISDN line would be dialed up for each ARP request. To prevent this, the AVM Access Server provides ARP spoofing to supply the requested hardware address locally. ARP spoofing is activated automatically in NetWAYS/ISDN and in the AVM Access Server.

Call-back Options and Cost Allocation

A classic use of NetWAYS/ISDN is to integrate telecommuters in a company LAN. Typically, the telecommuters' ISDN costs for connections to the LAN are always borne by the same site—usually the company's main office. For this purpose NetWAYS/ISDN provides the "Call-back request" and "COSO" (Charge One Site Only) features for ISDN-optimized cost allocation and call-back.

Call-back Request

The "Call-back request" option allows the NetWAYS/ISDN computer to signal the remote access server that it expects to be called back so that the costs for the ISDN connection are charged to the remote access server.

The type of dial-up connection is negotiated, including the call-back request option, each time NetWAYS/ISDN activates the connection to the remote access server. The NetWAYS/ISDN computer dials the remote access server to carry out the negotiation. If the call-back request is successfully negotiated, then the remote access server hangs up the connection and dials a return call to the NetWAYS/ISDN computer. The same procedure takes place when data is once again queued for transmission to the remote site after an inactivity timeout.

The first physical connection must be dialed (and the charges borne) by the NetWAYS/ISDN computer in order to negotiate the connection parameters, including the call-back option.

Charge Assignment with COSO (Charge One Site Only)

NetWAYS/ISDN provides the feature "COSO" (Charge One Site Only) to allow you to specify which end of the network link bears the connection charges. The NetWAYS/ISDN computer and the remote access server can be configured so that the same site bears the charges for all connections, regardless of which system initiates the connection set-up.

The cost assignment feature must be supported and enabled on both systems. COSO uses PPP over ISDN features to assign costs.

The COSO feature in NetWAYS/ISDN works as follows:

When charge assignment is set to the default option “Caller”, the connection costs are borne by whichever site dials up the connection. Use this setting if the remote system does not support charge assignment.

When charge assignment is set to “Local system”, all connections are charged to the local site. In this case, NetWAYS/ISDN does not answer incoming calls. Instead, NetWAYS/ISDN calls back, dialing up the connection to the call destination itself.

When charge assignment is set to “Remote system”, all connections are charged to the destination site. When data needs to be transmitted to the remote network, NetWAYS/ISDN signals a connection request over the ISDN D channel. The remote access server rejects the incoming call and calls the client computer back.

For both of these options, “Local system” and “Remote system”, the number of the site calling is transmitted over the D channel. For this reason the ISDN provider must support the CLIP feature (calling line identification) on the ISDN lines.

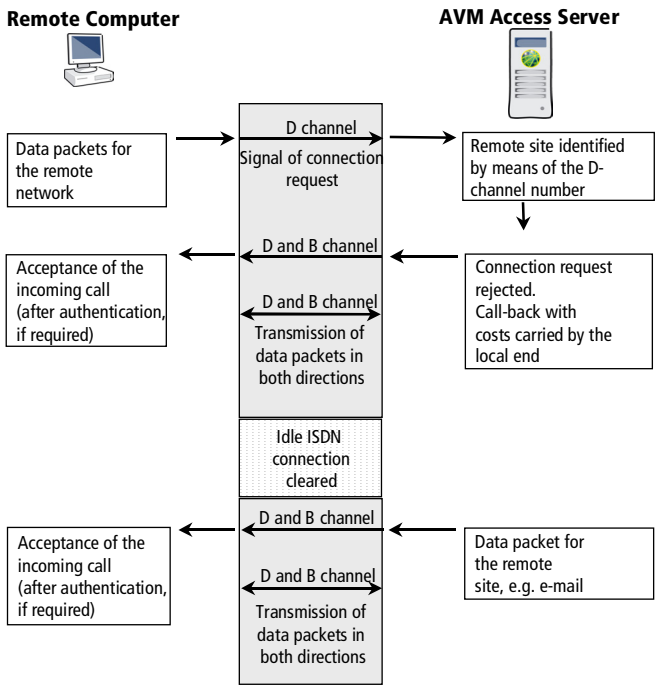
In most countries, the call-back request over the D channel is toll-free. Ask your ISDN provider if this is the case for your line.

If the cost allocation settings in NetWAYS/ISDN and the remote system do not match, a requested call-back may not be carried out correctly.

In this case a message is displayed in the Event Log and no further outgoing calls are then permitted to this call destination. Only the remote system can activate the connection.

For example, the main office may bear all the charges during working hours, while the NetWAYS/ISDN computer is charged for connections after hours.

The following diagram illustrates the cost allocation function using the “remote system” setting.



Call-back and cost allocation to the remote system by COSO (Charge One Site Only)

Leased Lines

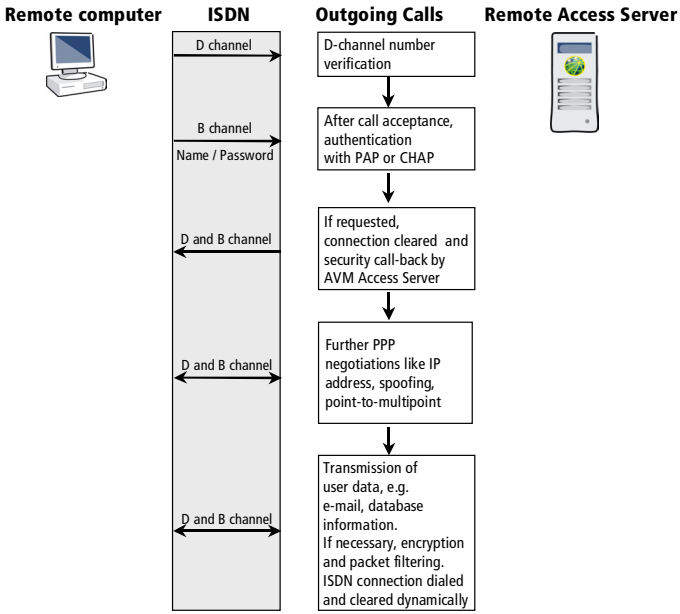
In addition to dial-up connections, ISDN is also used to provide leased lines. If the data traffic to the remote network is so high that a leased line is more economical than dial-up operation, NetWAYS/ISDN also supports ISDN leased lines. No additional hardware is necessary.

NetWAYS/ISDN supports leased lines with one B channel (Deutsche Telekom’s Digital 64S). Furthermore, NetWAYS/ISDN also supports BRI lines which use one B channel as a leased line and the other for dial-up connections.

3.3 Security

In remote network access, it is very important to protect both the remote access server and the NetWAYS/ISDN computer against unauthorized access. NetWAYS/ISDN provides several security mechanisms for this purpose, which must also be supported by the remote access server.

The following diagram illustrates the security checks that can be applied on a connection to a remote access server.



Security in remote network access

Caller ID

When a remote computer dials in to a network, the remote access server must decide whether or not to accept the connection. The remote computer is first identified by the number of its ISDN line, signaled with the incoming call on the D channel. The remote access server compares this number with those registered in its database. The connection is accepted only if the number is matched.

Transmission of the caller's number over the ISDN D channel (Calling Line Identification, or CLI) is an ISDN feature used by NetWAYS/ISDN for protection against unauthorized access and for charge assignment.

In order for the "CLI" number check to function in NetWAYS/ISDN, the CLI feature must be activated for the ISDN line by the ISDN provider.

User Name and Password

As a further security mechanism, NetWAYS/ISDN provides authentication by user name and password. The authentication process tests whether the remote system possesses a user name and password that match the information registered locally. If so, the remote systems is authentic and the connection can be set up.

Password authentication ensures that only authorized users can access a system. The user name and password for authentication with the remote site can be obtained from the network administrator.

Authentication by user name and password is performed under the PPP over ISDN protocol.

The PPP protocol provides two authentication techniques:

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

PAP and CHAP can be used for authentication on both outgoing and incoming calls.

Security Call-back

For still greater security, the remote access server can disconnect and call the remote computer back after authenticating it by user name and password. The number dialed for the return call is the CLI number. If the CLI number received is not the complete number, the security call-back can also take place using a number specified explicitly in the remote access server's configuration.

Data Encryption

Data packets can be sent in encrypted form to protect them against unauthorized access during transmission.

Encryption is performed at the PPP level in accordance with the RFC standards. Because data compression is also performed at this level, the data can be first compressed and then encrypted.

Encryption is performed using the Twofish algorithm, a symmetrical or "secret key" encryption technique. Symmetrical encryption means that the same key is used to encrypt and to decrypt the data. Only the sender and the receiver know the key.

This random key, with a key length between 128 and 256 bits, is generated on connection set-up by the sender. The key must then be sent to the receiver. Because it must remain secret, the key itself is encrypted for transmission to the receiver. Encryption of the key is performed by the crypt provider service. The crypt provider "AVM Crypt Services for NetWAYS/ISDN" is installed by NetWAYS/ISDN Setup. Certain preparatory steps must be carried out before this service can be started. Detailed instructions can be found in the NetWAYS/ISDN Online Help.

The default crypt provider can be replaced by another service, such as a smart card, PIN, biometric or other system. The Crypt Provider API is the interface between such services and NetWAYS/ISDN. New encryption keys are generated and sent to the remote site each time a connection is established for data communication.

A detailed description of the Crypt Provider API is available from the AVM Data Call Center (ADC): \NETWORKS\NETWAYS\UTIL\API\AVMNWAPI\CRYPTAPI.DOC.

3.4 Internet Connections

For connections to the Internet, NetWAYS/ISDN also supports the economical AO/DI service and high-speed ADSL access. AO/DI allows you to maintain a permanent, economical connection to the Internet over the ISDN D channel. ADSL permits Internet access at significantly higher data speeds.

IP masquerading and Short-Hold Mode provide additional security on connections to the Internet.

AO/DI

The AO/DI (Always On/Dynamic ISDN) technique uses the ISDN D channel for a permanent connection to the Internet. Data packets are transmitted over the D channel using the X.25 protocol. In this way the NetWAYS/ISDN computer is constantly connected to the Internet (Always On). The capacity of the D channel is sufficient for the transmission of smaller amounts of data, and no connection costs are incurred. When the amount of data to be transmitted requires more bandwidth, one or more B channels are automatically connected as well (Dynamic ISDN).

AO/DI saves connection charges in Internet communication involving lower volumes of data, since no connection costs are incurred as long as no B channel is used.

AO/DI can only be used if it is supported by both the Internet Service Provider and the ISDN provider.

ADSL

ADSL (Asymmetric Digital Subscriber Line) is a communication technology that permits Internet access with high bandwidth over ordinary telephone cables. ISDN and ADSL use different frequency bands for simultaneous operation over the same wire.

Data communication takes place at up to 6 Mbit/s downstream (that is, from the Internet to the user) and up to 640 kbit/s upstream. Dial-up connections to other subscribers are not possible over ADSL.

NetWAYS/ISDN supports the ADSL protocols PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA). If FRITZ!Card DSL is used for the connection to the ADSL line, either of these protocols can be used. If the computer is connected to ADSL using an Ethernet adapter and an external ADSL modem, then only PPPoE can be used. NetWAYS/ISDN comes with two pre-configured locations for ADSL: “FRITZ!Card DSL” and “ADSL Modem PPPoE”.

IP Masquerading

The IP masquerading module in NetWAYS/ISDN replaces the source IP addresses in TCP, UDP and ICMP packets with the official IP address assigned to NetWAYS/ISDN by the remote system. NetWAYS/ISDN’s use of IP masquerading provides the following advantages:

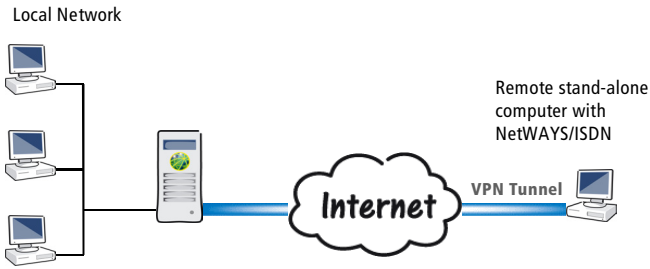
- Each time the connection to the Internet Service Provider is re-established after an inactivity timeout, NetWAYS/ISDN is assigned a new IP address. Thanks to IP masquerading, the computer’s routing table does not need to be updated each time the official IP address changes. The IP masquerading function always substitutes the current official IP address for the source address of packets traveling from the LAN to the Internet, throughout the logical connection.
- By default, IP masquerading prohibits all incoming TCP connections. Incoming packets that have not been requested by an application in the LAN are discarded. This makes the local network more secure.

3.5 VPN Connections

NetWAYS/ISDN allows you to set up Virtual Private Network (VPN) connections. VPN connections are an economical way to connect remote PCs to the company LAN. Until recently, remote systems were usually interconnected using direct dial-up or leased line connections over public telecommunication networks, such as ISDN or GSM. However, the costs for direct dial-in increase with the distance to be bridged. International connections in particular can be very expensive. Today, systems separated by long distances can be economically linked by VPN connections.

VPNs in General

A remote stand-alone computer is connected to the company LAN by a VPN link transported over the Internet.



Example: a VPN connection over the Internet

The private connection carried over the public Internet between the two communicating parties is called a tunnel. The two networks exchange data through this tunnel. The remote stand-alone computer and the company LAN do not share a physical network connection: the shared network is a virtual one. This virtual network is a higher-order data structure that uses the existing public infrastructure of the Internet for data transport. The other interfaces and applications of the two connected systems are not affected by the VPN link. The connection is economical because both sites only incur charges for a connection to an Internet Service Provider.

VPNs in NetWAYS/ISDN

The term VPN refers simply to a private link carried over a public infrastructure. Which techniques are used to accomplish this is not specified.

NetWAYS/ISDN sets up its VPN links over existing Internet connections, taking advantage of the Internet Service Provider's infrastructure. The Internet Service Provider has nothing to do with the actual VPN connections, however, nor with the network communication between the systems involved. NetWAYS/ISDN contains the software needed to operate VPN connections. The remote system must also be equipped with appropriate software (such as the AVM Access Server) to establish VPN connections. Because the VPN connection is independent of specific Internet Service Providers, practically any Internet access can be used for VPN communication.

The VPN link acts as a tunnel through the public Internet, through which data can be transported. The VPN software in the NetWAYS/ISDN and the remote system provides a transparent connection to the network, authentication of the communicating parties, and encryption of all data transported over the public network.

Once the VPN tunnel has been set up, neither the tunnel nor the Internet as the underlying medium is visible at the application level.

Security

Because the VPN connection is carried over the public Internet, there is a certain risk of eavesdropping or manipulation by unauthorized third parties. Appropriate security mechanisms must therefore guarantee the following three kinds of security:

- **Privacy**
  The data interchange must be encrypted to prevent eavesdropping.

- **Authenticity**
  When a connection is opened, the communicating parties must be identified to ensure that all data comes from the authentic source, and is not simply being replayed by an interceptor, for example.
- **Integrity**
  The VPN must ensure that data cannot be modified by third parties (as in "man-in-the-middle" attacks) on its way through Internet.

The VPN Protocol IPsec

A protocol used to set up VPN connections must bring with it the following characteristics:

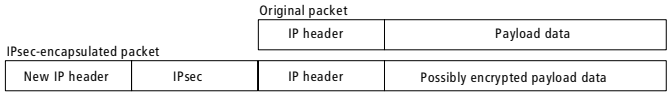
- Support for security mechanisms that guarantee privacy, authenticity and integrity as described above.
- The ability to connect through a tunnel.

The IPsec suite provides these characteristics, and is therefore used by NetWAYS/ISDN as the standard VPN protocol.

IPsec is a network-layer (ISO OSI Layer 3) protocol, and hence independent of the underlying infrastructures. However, IPsec is limited to the IP network protocol. In other words, only IP data can be transported over an IPsec-based VPN.

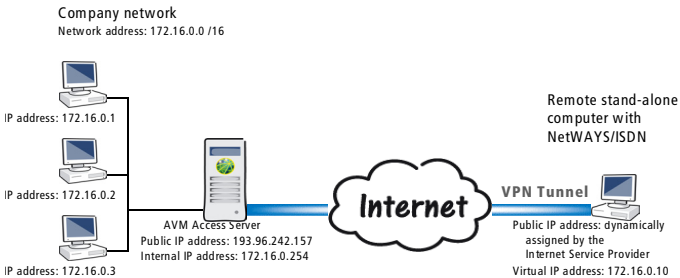
IPsec permits two different operating modes: Tunnel Mode and Transport Mode. Transport Mode does not create a tunnel, and strictly speaking does not provide a virtual private network. Only Tunnel Mode is used in VPN connections.

In Tunnel Mode, a tunnel is set up through a public network. In other words, the IP packets are encapsulated before transmission. Each IP packet, with its complete IP header, is transmitted as the payload of a new IPsec packet. The new packet also has its own IP header. In this way both single computers and whole networks using private IP addresses can communicate over the public Internet.



Original packet and IPsec encapsulated packet with new IP header

The illustration below shows a sample VPN connection in Tunnel Mode. Here a remote stand-alone computer is connected to the local company network.



Example: VPN Connection in Tunnel Mode

The IP addresses in the example above are used in different ways:

- Company network

  The company LAN has the network address 172.16.0.0/16. Each computer in the company network has an IP address in the address range defined by this network address. These are all private IP addresses which must never appear in the public Internet. They are reserved under RFC 1918 for communication within private LANs.

- AVM Access Server

  The AVM Access Server computer has two network interfaces: one in the LAN and one with an external IP address, i.e., a valid public Internet address which is dynamically assigned by the Internet Service Provider. The Access Server communicates with the other computers

in the LAN using an internal IP address. The AVM Access Server also provides the LAN with its gateway to the Internet.

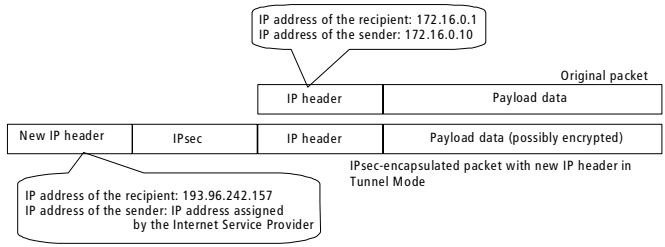
- Remote Computer with NetWAYS/ISDN

  When the VPN connection is active, the remote standalone computer also has two IP addresses: its official IP address that is valid in the Internet, and its IP address in the virtual private network. The official IP address is usually assigned dynamically by the Internet Service Provider each time the Internet connection is dialed up. This means the address can change with each new connection. The IP address of the computer in the virtual network is a private IP address in the company network. This address is assigned by NetWAYS/ISDN before the VPN connection is activated.

In the encapsulated packets transported over the IPsec tunnel between the NetWAYS/ISDN computer and the AVM Access Server, different IP addresses appear in the original packet's IP header and in the encapsulating packet header:

IP addresses in the original packet	
Destination	The private IP address of the computer in the company network that is the intended recipient of the communication.
Source	The remote computer's IP address in the virtual network.
IP addresses in the tunnel packet	
Destination	The AVM Access Server's official IP address in the Internet.
Source	The official, public IP address of the remote computer in the Internet.

The diagram below shows sample IP addresses for source and destination in the two packet headers:



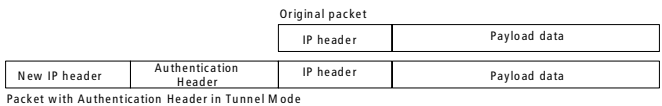
IP addresses in the original and encapsulating packet headers

The IPsec Transport Protocols

IPsec uses two different transport protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). These two protocols can be combined, and can be used in both Tunnel and Transport Modes.

Properties of the Authentication Header (AH)

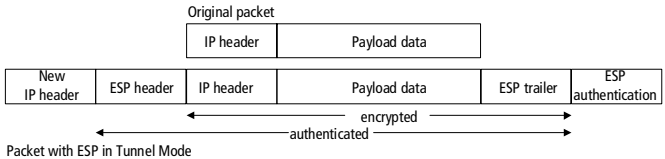
- Authenticates the source of the payload data: AH includes a mechanism that allows the recipient to verify whether the source of the data is authentic.
- Ensures the integrity of the payload data: The same mechanism that provides authentication also allows the recipient to detect any manipulation of the payload data.
- Prevents replay and detects man-in-the-middle attacks: AH contains a unique serial number that can be used to identify packets replayed by a third party.
- AH does **not** provide encryption of the data payload.



Packet in its original state and with Authentication Header

Properties of the Encapsulating Security Payload (ESP)

- Encrypts the user data payload. In Tunnel Mode, the IP header is also encrypted. The symmetrical encryption methods available include DES, 3DES, AES and others.
- Authenticates the source of the payload data: ESP includes a mechanism that allows the recipient to verify whether the source of the data is authentic.
- Prevents replay and detects man-in-the-middle attacks: ESP contains a unique serial number that can be used to identify packets replayed by a third party.



Packet in its original state and encapsulated with ESP

Negotiation

IPsec provides many options. Many combinations of encryption and authentication parameters are possible in VPN connections. When establishing a secure VPN connection, the communicating parties must agree on the parameters they want to use.

Every VPN party has a security policy database containing the authentication algorithms, the encryption algorithms, authentication data and other information about its own IPsec capabilities. This information forms the basis for negotiation with remote IPsec systems.

Negotiation of the connection parameters to be used is performed under another protocol, called Internet Key Exchange (IKE). The parameters agreed upon in IKE negotiation are stored in a Security Association (SA). The SA defines:

- the type of authentication used (certificates, a pre-shared key or another method)
- the encryption algorithm used
- the hash algorithm used

- the duration of validity, or “lifetime”, of the SA

SAs have a limited period of validity. When the lifetime of an SA has elapsed, a new SA must be negotiated. A separate SA is negotiated for each direction of communication. The SAs are stored in the security association database.

IKE negotiation takes place in two phases.

IKE Phase 1

The purpose of IKE Phase 1 is to negotiate an SA to provide secure communication during IKE Phase 2. In IKE Phase 1, the two peer systems perform the following steps:

- They authenticate themselves.
- They negotiate an encryption algorithm to be used in IKE Phase 2.
- They negotiate a Diffie-Hellman group.
- Each system generates a private key, and generates a corresponding public key using the negotiated Diffie-Hellman group. The public keys are exchanged. Each system generates the secret key to be used for the encryption of IKE Phase 2 communication based on its own private key, the peer's public key and the negotiated Diffie-Hellman group. The resulting key is identical in both systems.
- The two systems negotiate the lifetime of the SA.

There are two protocol modes to choose from in IKE Phase 1: “main mode” and “aggressive mode”. Main mode requires more messages to be exchanged than aggressive mode. If the NetWAYS/ISDN computer’s public IP address is dynamically assigned by the Internet Service Provider and hence not known, then IKE Phase 1 must be conducted in aggressive mode.

IKE Phase 2

The goal of IKE Phase 2 is to negotiate the SAs for the encryption of actual user data. This negotiation is itself encrypted based on the SA that was negotiated in Phase 1. The following parameters are negotiated:

- the IPsec transport protocol (AH and/or ESP)
- the encryption algorithm for user data transmitted over the VPN connection (DES, AES, or 3DES, for example)
- the hash algorithm used to ensure the integrity of the user data
- the IPsec operating mode (Tunnel or Transport Mode)
- the lifetime of the SA
- the random key material for the encryption and authentication algorithms

Once IKE negotiation has been completed, secure IPsec communication begins.

Asymmetrical Encryption Techniques

Asymmetric encryption methods use a key pair rather than a single key. A key pair consists of one public and one private key. Data encrypted with one of these keys can only be decrypted with the other. The advantage over symmetrical encryption methods is that no secret key needs to be exchanged between the communicating parties.

A popular application using asymmetric encryption is PGP (Pretty Good Privacy), which is frequently used for e-mail encryption. The recipient's public key is accessible to anyone, and so can be used by the sender to encrypt an e-mail message. The result is an encrypted message that can only be decrypted using the recipient's secret key.

It is also possible to use the secret key for encryption, so that only the corresponding public key can be used for decryption. This is the method used to create digital signatures. A hash digest of the original message is encrypted by the author using the secret key, and attached to the message. The signature can then be decrypted by anyone using

the author's public key, and the resulting hash value compared with a locally calculated hash of the message as received. If the values match, then the signer must have possessed the corresponding secret key, and message can hence be considered authentic.

Asymmetric encryption techniques are less suitable for high-volume data communication, however, since the keys used are very large (typically 1024 bits at present) and the amount of computation required is great. Furthermore, the input value cannot be longer than the key used. Familiar asymmetrical encryption techniques include RSA and Diffie-Hellman.

NetWAYS/ISDN uses the asymmetric Diffie-Hellman technique for key exchange in IKE Phase 1.

Compression Techniques (IPComp)

Encrypted data cannot be compressed. This is because compression techniques generally take advantage of repetition within a data string. When a repetition is found, the encryption algorithm substitutes a symbolic reference to the first occurrence. A good encryption algorithm produces a seemingly random string, however—that is, one containing few repetitions. (Otherwise it would be relatively easy to decrypt a message using statistical methods, such as letter frequencies if the language used is known.) For this reason, if compression is desired, it must be applied before encryption is performed. This is done by the IPComp protocol. Three compression methods are possible in IPComp:

- Deflate (RFC 2394)
- LZS (RFC 3051), also used in Stac compression (RFC 1974)
- LZJH (RFC 2395), which corresponds to V.44, used in the modem protocol V.92

NetWAYS/ISDN implements all three compression methods.

4 NetWAYS/ISDN for Administrators

This section provides the network administrator with additional information about the functions used to install, configure and manage NetWAYS/ISDN according to your individual requirements.

4.1 Automated Installation of NetWAYS/ISDN

NetWAYS/ISDN allows administrators to customize and automate the NetWAYS/ISDN installation so that general settings are configured without user interaction.

To make multiple installations still easier, NetWAYS/ISDN can be automatically installed with pre-configured locations, call destinations, profiles, and a list of holidays.

For complete information on creating locations, call destinations, charge profiles and the list of holidays, please see the Online Help.

Configuring NetWAYS/ISDN

Administrators can configure the NetWAYS/ISDN installation routine to complete the installation without user input. This is especially practical when NetWAYS/ISDN needs to be installed quickly on a number of stand-alone computers.

In order to take advantage of this feature, you must create a file named SETUP.CFG and place it in the folder containing the NetWAYS/ISDN setup files. SETUP.CFG is an ASCII file which contains all the information that would otherwise be entered by the user during the NetWAYS/ISDN installation. The NetWAYS/ISDN installation program checks on starting whether the file NetWAYS/ISDN is present. If it is, then the installation is performed as defined in that file without user interaction.

Please note that the configuration values in the following description are merely examples.

The SETUP.CFG file should contain the following information:

CDKey_NETWAYS=XXXXXXXXXXXXXXX

This is the Product Identification Code (PIC). All letters are uppercase; dots, hyphens and slashes are omitted.

InstallDirectory=c:\netways

The folder in which the program is to be installed

Node=000000000908

The 12-digit IPX node number: 000000000002 = automatic node address assignment, 2 = fixed node address

AutoInstall=1

0 = manual installation, 1 = automatic installation (1)

InstallMode=1

1 = the NetWAYS/ISDN service starts automatically; 0 = NetWAYS/ISDN does not start automatically when Windows starts

KeepDatabase=1

0 = delete existing databases in the installation folder; 1 = continue using existing databases

Installing Pre-configured Call Destinations and Locations

NetWAYS/ISDN allows administrators to automate the installation of pre-configured call destinations and locations.

The call destinations and locations to be used in the custom installation must first be configured once in an installed copy of NetWAYS/ISDN. NetWAYS/ISDN stores the call destinations and locations in the following files in the NetWAYS/ISDN folder:

Call destination files:

- TARGET.DAT
- TARGETI.IDX
- TARGETN.IDX

- TARGETU.IDX

Charge profile assignments to call destinations and locations:

- TTIMER.DAT
- TTIMERCE.IDX
- TTIMERID.IDX
- TTIMERL.IDX

Location files:

- LOCATION.DAT
- LOCATIONI.IDX
- LOCATION.IDX

In order for your call destinations and locations to be copied in new installations, these files must be placed in the NetWAYS/ISDN installation folder. The Setup program then installs them automatically with the program, so that the pre-configured call destinations and locations do not have to be created by the user, but are immediately available when NetWAYS/ISDN is started.

To install pre-configured call destinations and locations, the files named above must always be copied together.

Installing Pre-configured Profiles

NetWAYS/ISDN also allows the administrator to customize the installation by including pre-configured profiles and a list of holidays.

In order to use this feature, you must first configure the profiles and the list of holidays in an installed NetWAYS/ISDN program. NetWAYS/ISDN stores the charge profiles and the list of holidays in the following files in the NetWAYS/ISDN folder:

Files containing holidays:

- HOLIDAY.DAT
- HOLIDAY.IDX

Files containing the charge profiles:

- CPROFILE.DAT
- CPROFILE.IDX

4.2 Locking the Settings

The administrator can set a password to protect the preconfigured locations, call destinations, profiles and holiday list against changes by the NetWAYS/ISDN user. Once locked, the settings can only be changed by entering a password. A user who enters the password can unlock the settings either until the program is restarted, or permanently.

4.3 The NetWAYS/ISDN Service

NetWAYS/ISDN is installed as an operating system service. This has the following advantages:

- NetWAYS/ISDN is automatically started when Windows starts. When NetWAYS/ISDN is stopped, any existing connections are cleared down.
- The ISDN connection to a remote system can be established before any Windows user logs in. In this way clients connected over ISDN behave to a large extent the same as locally connected LAN clients.
- Execution as a system service makes it easier to use NetWAYS/ISDN to log in to Windows NT domains and Novell NetWare Directory Services (NDS).

Starting the NetWAYS/ISDN Service

NetWAYS/ISDN runs as a Windows service. This means that the program starts automatically when Windows starts, and stops when Windows is shut down.

When NetWAYS/ISDN is stopped, any existing connections are cleared down.

The NetWAYS/ISDN user interface is separate from the service. If you want the NetWAYS/ISDN window to be opened when Windows starts, copy a shortcut to NetWAYS/ISDN to the "Startup" folder.

Starting and Ending NetWAYS/ISDN Manually

- To start NetWAYS/ISDN manually, select the command "Programs / NetWAYS/ISDN / NetWAYS/ISDN" in the Windows Start menu. The NetWAYS/ISDN window appears.
- To stop NetWAYS/ISDN manually, select the "Stop" command in the "File" menu.

Before you exit NetWAYS/ISDN, you should clear down any existing connections.

Selecting a Call Destination to Connect Automatically

If you want to activate the connection to a certain remote network every time Windows starts up, select the desired call destination with the mouse, then select the command "Connect automatically on NetWAYS/ISDN startup" in the "File" menu.

If you want this call destination to be placed on stand-by when Windows starts, select the call destination with the mouse, then select the command "Stand-by on startup" in the "File" menu.

NetWAYS/ISDN then connects to the call destination automatically either when Windows starts, or as soon as data is queued for transfer to the remote network.

4.4 The NetWAYS/ISDN API

NetWAYS/ISDN provides a number of programming interfaces to allow custom applications to control routing, remote access and data encryption.

Routing and Remote Access API

AVM's routing and remote access API is a program interface which allows NetWAYS/ISDN to be controlled by external software. This API permits other tasks and routines to use NetWAYS/ISDN commands for automatic operation. For example, dial-around routines can be defined to perform automatic database updates among branch offices during cheaper rate periods, or to integrate additional security mechanisms such as smart cards in the PPP authentication procedure.

For detailed information about the use of the Routing and Remote Access API, see the directory \NETWORKS\NETWAYS\UTIL\API\AVMNWAPI on the ADC.

Crypt Provider API

The Crypt Provider API is a programming interface designed to allow users to customize the data encryption service. New encryption keys are generated and sent to the remote site each time a connection is established for data communication. Because these keys must also be sent in encrypted form, they are encrypted by the crypt provider, which can be programmed to use custom security techniques (smart cards, PINs, biometrics, etc.). The Crypt Provider API is the interface through which NetWAYS/ISDN accesses the crypt provider's algorithms.

For detailed information about the use of the Crypt Provider API, see the directory \NETWORKS\NETWAYS\UTIL\API\AVMNWAPI on the ADC.

4.5 Supported Standards

The protocols PPP over ISDN and IPsec are based on internationally recognized, open internetworking standards. These standards are defined and described in RFCs (Requests for Comments), the Internet standardization documents. To be compatible with NetWAYS/ISDN's features, remote systems must provide support for the corresponding RFCs. The following two tables list the RFCs implemented in NetWAYS/ISDN.

PPP over ISDN

RFC 1144	Compressing TCP/IP Headers for Low-Speed Serial Links
RFC 1332	The PPP Internet Protocol Control Protocol (IPCP): dynamic IP address assignment
RFC 1334	PPP Authentication Protocols (PAP)
RFC 1552	PPP Internetwork Packet Exchange Control Protocol (IPXCP): dynamic IPX node address assignment
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	Point-to-Point Protocol (PPP)
RFC 1662	PPP in HDLC-like Framing
RFC 1962	The PPP Compression Control Protocol (CCP)
RFC 1968	PPP Encryption Control Protocol (ECP)
RFC 1974	PPP Stac LZS Compression Protocol
RFC 1989	PPP Link Quality Monitoring
RFC 1990	The PPP Multilink Protocol (MP)
RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2118	Microsoft Point-to-Point Compression (MPPC) Protocol
RFC 2125	The PPP Bandwidth Allocation Protocol (BAP) / The PPP Bandwidth Allocation Control Protocol (BACP)

RFC 2131	Dynamic Host Configuration Protocol (DHCP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)

IPsec

RFC 1829	The ESP DES-CBC Transform
RFC 1851	The ESP Triple DES Transform
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 2394	IP Payload Compression Using DEFLATE
RFC 2395	IP Payload Compression Using LZS
RFC 2401	Security Architecture for the Internet Protocol
RFC 2402	IP Authentication Header (AH)
RFC 2403	The Use of HMAC-MD5-96 within ESP and AH
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2405	The ESP DES-CBC Cipher Algorithm with Explicit IV
RFC 2406	IP Encapsulating Security Payload (ESP)
RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409	The Internet Key Exchange (IKE)
RFC 2410	The NULL Encryption Algorithm and Its Use with IPsec
RFC 2412	The OAKLEY Key Determination Protocol
RFC 2451	The ESP CBC-Mode Cipher Algorithms
RFC 3051	IP Payload Compression Using ITU-T V.44 Packet Method
RFC 3173	IP Payload Compression Protocol (IPComp)
RFC 3268	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
Draft	Extended Authentication Within ISAKMP/Oakley (XAuth)
Draft	The ISAKMP Configuration Method (“mode-config”)

5 Information, Updates and Support

AVM provides numerous sources of information to assist you in your day-to-day work with NetWAYS/ISDN. If you need help in solving problems that may occur, you can also get in touch with AVM Support.

5.1 Information Sources

Further information about NetWAYS/ISDN is available from the following sources:

Documentation

NetWAYS/ISDN comes with comprehensive documentation in various formats:

- The present manual is included in PDF format on the NetWAYS/ISDN CD-ROM. The PDF file can be opened either by clicking the link in the introductory Help file that starts automatically when you insert the CD, or by browsing the folder NETWAYS\INSTALL in the Windows Explorer and double-clicking the file.

  The manual contains detailed information about the concepts and applications of NetWAYS/ISDN, the prerequisites for its installation, and instructions for installing and using NetWAYS/ISDN. The manual also provides a comprehensive glossary in an appendix.

If you do not have a program to display PDF documents, you can install the Adobe Acrobat Reader for this purpose using the link in the introductory Help file that starts automatically when you insert the CD, or by running the installation program in the folder UTILS\ACROBAT\ENGLISH.

- The complete, context-sensitive Online Help provides details on all NetWAYS/ISDN configuration settings.

5.2 Updates

The latest software updates for NetWAYS/ISDN are available free of charge from AVM's web site, or from the AVM Data Call Center.

Internet

To download updates over the Internet, please visit:

www.avm.de/en/download

You can also download software updates from AVM's FTP server. Click the "FTP Server" link in the download area, or see:

www.avm.de/ftp

The AVM Data Call Center (ADC)

The AVM Data Call Center and AVM's web site provide current information about all AVM products, the latest drivers for AVM ISDN-Controllers, and free enhancements for AVM products.

AVM Data Call Center (ADC)

+49-(0)30-39 98 43 30

(Fast Internet over ISDN)

5.3 Getting Assistance from AVM Support

Please use the information sources described above before getting in touch with Support.

If these instructions and the various information sources have not helped to solve your problem, contact AVM Support for additional technical assistance. You can send your request to AVM Support by e-mail or telefax.

Support by E-mail

You may send your support request to AVM by e-mail. To do so, please use the Support form on the AVM web site.

1. Enter AVM's Internet addresses:

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

2. On this page, select "NetWAYS/ISDN" in the list of "Software" products.

3. Then select the area in which you encountered the problem. An e-mail form appears.

4. Fill out the form and send it to AVM support by clicking the "Send" button.

Support by Fax

If you do not have Internet access, you can also contact Support by telefax at the following number:

+49-(0)30-39 97 62 66

Please prepare the following information to give to the Support technician:

- TheNetWAYS/ISDN version you are using. The version number can be found in the Readme file in the NetWAYS/ISDN installation folder.
- The operating system used on the computer on which you have installed NetWAYS/ISDN (Windows XP, Me, 2000, 98, or NT).
- The number of the Microsoft Service Pack installed.
- The network protocols you are using.
- The ISDN-Controller model installed in the NetWAYS/ISDN computer. The version and build numbers of the ISDN-Controller drivers.

  The driver version and build numbers can be found in the "Readme" file in the driver installation directory of the AVM ISDN-Controller. If you have installed FRITZ! on the NetWAYS/ISDN computer, then the driver version can also be found in the FRITZ!version window: select "Start / Programs (or All Programs) / FRITZ! / FRITZ!version". In the "FRITZ!version" window, click the "System Information" button.

- Is your ISDN-Controller connected to a PBX extension?
- Are you able to dial up a test connection to the AVM Data Call Center (ADC) using the pre-configured call destination “Fast Internet over ISDN”?
- At what point in the installation procedure or in the program does the error occur?
- What is the exact wording of the message?

Once you have gathered this information, you are ready to contact AVM Support. We are confident that the support team will be able to assist you in solving the problem.

Glossary

ADSL (Asymmetric Digital Subscriber Line)

ADSL is a communication technology that permits Internet access with high bandwidth over ordinary telephone cables. Data communication takes place at up to 6 Mbit/s downstream (that is, from the Internet to the user) and up to 640 kbit/s upstream. Other telecommunication services and dial-up connections to other subscribers are not possible over ADSL. This technology is marketed by telecom providers under various brand names, such as Deutsche Telekom AG's "T-DSL".

ISDN and ADSL can be carried over the same telephone cable using different frequency bands.

AH (Authentication Header)

A security protocol in the IPsec suite. AH ensures the authenticity of a packet's source and the integrity of its contents. AH does not provide encryption of the data payload, however.

AOCD

AOCD, or Advice of Charge During Call, is an ISDN feature. When this feature has been activated for the ISDN line, charge information is transmitted over the D channel as charges are incurred during a connection according to the European standard AOCD. For more information about AOCD, consult your ISDN provider.

AO/DI

AO/DI stands for Always On/Dynamic ISDN. This procedure uses the ISDN D channel for connections with the Internet. Data packets are communicated in the D channel using the X.25 protocol. The connection is permanently active. The capacity of the D channel is sufficient for the transmission of smaller amounts of data and no connection costs are

incurred. AO/DI dynamically enables one or more B channels (Dynamic ISDN) depending on the amount of data to be transmitted.

ARP (Address Resolution Protocol)

The Address Resolution Protocol, or ARP, is part of the TCP/IP protocol suite. ARP is used dynamically to obtain the Ethernet hardware address (called the MAC address) of the interface that corresponds to a given IP address. This takes place automatically, and is normally transparent to applications and users.

In order for TCP/IP network communication to take place, the transmitting station must obtain the hardware address corresponding to the IP destination address. To obtain the hardware address, the transmitting station sends an ARP request packet containing the IP address of the desired destination. This packet is broadcast to all ARP-capable stations on the network, and the one with the IP address requested responds to it with an ARP reply packet. The sender then stores the IP address—hardware address association in its ARP cache.

Authentication

Authentication refers to identifying a remote system by verifying its login information (name and password) on establishing incoming and outgoing connections. NetWAYS/ISDN uses authentication not only to prevent unauthorized access, but also to ascertain which remote user settings to apply if incoming call assignment by CLI number is not activated. For PPP connections PAP and CHAP are available as authentication protocols.

In NetWAYS/ISDN, authentication of the remote system can be activated or deactivated for each call destination, and the authentication protocol used can be specified for each destination separately. For each authentication protocol, a name and password must be configured and communicated to the remote site. If the remote server also demands

authentication, the name and password assigned by the remote administrator must be entered as well. Obtain this information from the administrator of the remote site.

B channel

An ISDN basic access consists of two B channels and one D channel. The B channels are used to transport user data. They allow transmission at a rate of 64 kbit/s. B channels can be bundled to accelerate transmission.

CAPI

See “COMMON-ISDN-API (CAPI)” on page 61

CHAP (Challenge Handshake Authentication Protocol)

One of the two authentication protocols in the PPP suite. To perform an authentication, the local and remote sites must have the assigned name and password entered in their configuration for the connection. The remote system must be configured to present the same name and password. 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 system produces a new message out of the first message and the password, also using a preset algorithm, and sends this value back. The first site performs the same operation and compares its results with the message received from the remote system. If they match, the remote system is authentic and the connection can be set up. The advantage of this method is that the password itself is never transmitted between the two systems. For this reason CHAP is considered a secure protocol. CHAP is described in RFC 1334 and RFC 994.

CLI (Calling Line Identification)

ISDN terminal devices can transmit their line number over the D channel with outgoing calls. CLI is an ISDN feature used by NetWAYS/ISDN to identify incoming calls.

Client

A client is a computer in a network that requests services from another system, such as access to files or information from databases.

COMMON-ISDN-API (CAPI)

CAPI is a standardized, manufacturer-independent interface between PC ISDN adapters and ISDN applications. The driver software for AVM ISDN-Controllers provides the CAPI interface throughout the system. Current CAPI drivers can be downloaded free of charge from AVM's FTP server (ftp://ftp.avm.de/). NetWAYS/ISDN builds on the CAPI 2.0 applications interface.

D channel

The D channel is used to carry control information in ISDN, such as the type of communication service requested and the numbers of the parties communicating. The D-channel throughput is 16 kbit/s for BRI lines and 64 kbit/s for PRI (primary rate) lines. D channel information is used for ISDN features such as charge information (AOCD) and caller ID (CLIP). In Germany, the CLIP and AOCD services must be specially requested on ordering an ISDN line.

DSS1

Standard European ISDN D-channel protocol. All newer ISDN lines use DSS1.

ESP (Encapsulating Security Payload)

A security protocol in the IPsec suite. ESP provides authentication of the source of a data packet, as well as encryption to ensure the privacy.

Hash algorithm

A hash algorithm is a function that yields a short value that is practically unique for a given input. The value of the hash is also called a "digest" of the input. One-way hash algorithms are used in cryptography to create digital signatures for authentication.

- Characteristics of one-way hash algorithms:
  - The input data can be of any length.
  - The output is generally of a fixed length.
  - The input data cannot be reconstituted from the output.
  - The algorithm must be sufficiently free of collision: in other words, the probability of two different input values yielding the same output must be very small.
- Keyed hash functions:

  Keyed hash functions are one-way hash algorithms that use a key in addition to the variable input data. Keyed hash functions are used to generate message authentication codes (MACs). Only those who hold the same key can generate the same MAC from a given message. This makes the hash algorithm still safer against collisions.

HDLC (High-Level Data Link Control)

A communications protocol standardized by ISO for data packets over serial lines. HDLC is actually a structured set of standards which define the means by which dissimilar devices can communicate over data networks. HDLC is a bit-oriented and hence code-independent data link protocol for point-to-point and point-to-multipoint connections. HDLC is also standardized by ITU-T (ITU = International Telecommunication Union; ITU-T = ITU Telecommunication Standardization Sector). One version of this protocol, called LAP B, is used in the data link layer of all X.25 networks. HDLC defines frames in which the data blocks from the network layer are encapsulated for transport over the physical link. According to DIN 66221, an HDLC frame consists of the start-of-frame flag, the address field, the control field, the data field, the

frame check sequence (FCS), and the end-of-frame flag. HDLC is used in full-duplex mode, and provides for the acknowledgment of several frames at a time (usually eight). The number of frames transmitted before acknowledgment is called the window size.

Header

Data packets are generally transmitted beginning with a header which contains the source and destination addresses and identifies the protocol used to interpret the packet. Header information is often repetitive and thus can be compressed over some links, such as ISDN lines, to increase the speed of data communication and so save time and costs.

HMAC (Keyed-Hash Message Authentication Code)

Message Authentication Code (MAC) generated using a keyed hash function. Any hash algorithm can be used. HMAC signatures are used in all IPsec authentication functions.

ICMP (Internet Control Message Protocol)

ICMP is part of the IP (Internet Protocol) suite. It is situated at Layer 3 (the Network Layer) of the OSI reference model, alongside IP itself. ICMP uses the IP packet structure in a similar way to higher-layer protocols, however.

ICMP is a component of every IP implementation, and transports only error and diagnostic information for IP. A well-known service based on ICMP is the program “ping”.

IKE (Internet Key Exchange)

A protocol in the IPsec suite used to negotiate secure connection parameters. IKE is described in RFC 2490.

IP (Internet Protocol)

IP is the Network Layer protocol responsible for addressing and routing in the TCP/IP protocol family. In general terms, its purpose is to provide data communication between various networks.

IP address

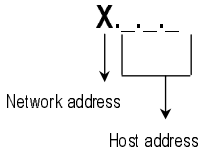
Addressing is one of the main functions of the Internet Protocol (IP). Addresses in IP version 4 are 32-bit numbers, which can be written as four bytes in decimal, octal or hexadecimal notation. In the NetWAYS/ISDN configuration, "dotted-decimal" notation is used: The four bytes of an address are represented by decimal numbers separated by dots. The sizes of the network address and the host address are variable, and determined by the first four bits (of the first byte) of the IP address. The full set of IP addresses, called the address space, is grouped into address classes designated as A, B, C, D and E. Only the first three of these five address classes are actually used. These classes can be described as follows:

Class	Characteristics	First byte of network address (decimal)
Class A addresses:	Few networks with many nodes	0-127
Class B addresses:	Medium number of networks and medium number of nodes	128-191
Class C addresses:	Many networks with few nodes	192-223

IP address classes

Every IP address contains two components: the network address and the host address. The sizes of the network address and the host address are variable, and determined by the first four bits (of the first byte) of the IP address.

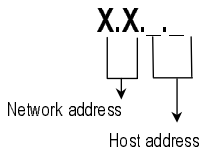
- **Class A addresses** consist of a one-byte network address and a three-byte host address:



Class A addresses

Example: 88.120.5.120 (88 is the network address, 120.5.120 is the host address).

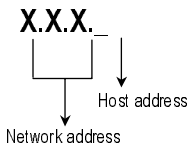
- **Class B addresses** consist of a two-byte network address and a two-byte host address:



Class B addresses

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 addresses

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

RFC 1918 (Address Allocation for Private Internets) reserves the following parts of the IP address space for use in private networks:

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)

IP masquerading

Also known as Network Address Translation, or NAT. A whole network can communicate with the Internet using just one IP address: A computer situated between the private LAN and the public Internet, with just one public, "official" Internet address, can forward all LAN computers' communications to computers in the Internet using its own IP number as the source address, as if all the connections came from it. NetWAYS/ISDN translates the IP addresses of TCP, UDP and ICMP packets so that only one source IP address is visible in the Internet. This means that the actual, internal LAN IP addresses never appear in the Internet, and so do not have to be "official" addresses. This also protects the local network against unauthorized access from the Internet: the IP Masquerading/Network Address Translation (NAT) gateway is significantly more difficult to break through than a good packet filter firewall.

IPsec (Internet Protocol Security)

A network-layer security standard for Internet communication. IPsec is well suited for VPN connections and remote LAN access over public telecommunication networks. IPsec uses the two security protocols Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides source authentication; ESP provides both authentication and encryption. Information specific to the security protocols is transported in a packet header appended to the IP header.

IPX (Internetworking Packet Exchange Protocol)

A network protocol developed by Novell used to exchange data packets quickly and reliably between two computers in a network.

Keep-alive packets

Keep-alive packets are sent periodically throughout the network to verify whether a client is still active. If the sending station receives no response, it clears down the logical connection.

LAN (Local Area Network)

A computer network limited to a given location, such as a company site or a government agency's office building. Remote computers can use appropriate software (such as NetWAYS/ISDN) to join a LAN over ISDN, ADSL, GSM or VPN connections.

Logical ISDN connection

A logical ISDN connection refers to the situation in which two computers consider an ISDN connection between them, which can be dialed up in one or two seconds, to be virtually continuous. An actual B-channel connection need not be continuously active during the logical ISDN connection. Throughout the entire duration of the logical ISDN connection, NetWAYS/ISDN maintains all the connection parameters that were negotiated when the physical connection was first dialed up. These parameters include the network protocols used, the authentication requirements, spoofing mechanisms and channel bundling. If data is queued for transmission when no B-channel connection is active, the B channel can be dialed up immediately.

Logical ISDN connections to the Internet are not supported by Internet Service Providers.

Logical network connection

A logical network connection refers to a network-layer connection between two LANs, or between a LAN and a remote client. The connecting router recognizes the remote system as long as the logical network connection persists.

A logical ISDN connection constitutes a record of all the connection information negotiated at the initial connection setup between the systems at either end of an ISDN WAN link.

These connection parameters are valid for the duration of a logical ISDN connection. These parameters include the network protocols used, the authentication requirements, spoofing mechanisms and channel bundling. Depending on the configuration, the logical ISDN connection will be cleared together with the physical connection or, if so negotiated with the remote site, remain valid even after the physical connection is no longer active.

MSN (Multiple Subscriber Number)

In Euro-ISDN (the D-channel protocol DSS1), point-to-multipoint ISDN lines are assigned multiple subscriber numbers, which can be used to distinguish between several end systems on the same S_0 bus, or between several CAPI applications on the same computer.

In Germany, Deutsche Telekom AG assigns standard ISDN lines three MSNs.

NAT (Network Address Translation)

See “IP masquerading” on page 66

NCP (NetWare Core Protocol)

A protocol to control communication between client and server in a NetWare network.

NetBIOS (Network Basic Input/Output System)

A standard for network communication that is independent of underlying transport protocols. NetBIOS is the standard network interface in Microsoft networks, and can be transported over IP as well as IPX.

Network address

See “IP address” on page 64

Outside line access

The Outside Dialing Prefix is the digit dialed at an extension line to obtain an outside line. Generally this is “0”.

PAP (Password Authentication Protocol)

One of the two authentication protocols in the PPP suite. A name and password for the remote system must be configured on the system that requests authentication. The remote system must be configured to present the same name and password. In PAP authentication, the name and password are sent unencrypted, and the authenticating system simply compares them with its settings. If they match, the remote system is authentic and the connection can be set up. Because PAP transmits the password in the clear, PAP should only be used on media that are safe from eavesdropping, and only if the more secure CHAP is not supported by the remote site.

Physical ISDN connection

The physical ISDN connection exists when one or more B channels are connected to the remote site and connection charges are accumulating. The physical ISDN connection is always based on a logical ISDN connection: the connection is controlled by the negotiated connection parameters.

Ping (Packet InterNet Groper)

A program that tests whether an IP host is reachable. The program sends an ICMP echo request packet to an IP host and waits for a reply. The command line option "-w" causes the Windows implementation of "ping" to wait a specified number of milliseconds for a reply. To allow a few seconds for ISDN dial-up and PPP negotiation, you should use the command "ping -w 5000" to specify a timeout of five seconds when testing an ISDN connection.

PPP

See "PPP over ISDN (Point-to-Point-Protocol)" on page 69

PPP over ISDN (Point-to-Point-Protocol)

A communication protocol for circuit-switched networks such as ISDN that provide protocol-independent communication on ISO OSI Layer 2. PPP over ISDN incorporates a collection of subordinate standards and protocols. These describe the

structure of data transport for a variety of networks. These standards are primarily intended to provide interoperability, ensuring that different manufacturers' devices with different sets of features can communicate by a uniform method. PPP over ISDN is specified in RFC 1618.

Ports

TCP and UDP packet headers provide port numbers for source and destination, in addition to the IP addresses. Because computers run many networking applications with many simultaneous connections, the IP address is not sufficient to address data to a specific application and a specific communication process. For outgoing requests and replies, the operating system assigns an application a unique TCP or UDP port number, choosing one sequentially or randomly. In NetWAYS/ISDN's IP masquerading module, source port numbers are mapped to connections.

"Well-known ports" are destination port numbers that are reserved for common network services and applications by IANA, the Internet Assigned Numbers Authority. Well-known ports are in the range from 0 to 1023.

Short-Hold Mode

Short-Hold Mode refers to the physical interruption of idle ISDN connections after a specified delay. Connection charges accrue for physically active ISDN connections (an occupied B channel), regardless of whether or not data are actually being transferred. Because an ISDN connection can be dialed up very quickly (in 1 to 2 seconds), it makes sense to clear down the physical ISDN connection temporarily when no data is sent for a certain time. The logical ISDN connection is maintained in accordance with the configuration settings. As soon as new data is queued for transmission, the physical connection is dialed up again in the background. This mechanism is transparent to the network user.

SMTP (Simple Mail Transfer Protocol)

SMTP is a standard protocol for exchanging e-mail between computers. SMTP implementations listen on TCP port 25. The protocol structure is simple, supporting only e-mail transmission over a data network. SMTP is defined in RFC 821.

Spoofing

“Spoofing” in data communication means to send data with a false source address, pretending to be from a different system.

Several network applications are known to exchange data packets that can cause frequent, unnecessary physical connections when operated over ISDN WAN links. Some packet types, in particular those used by Windows file and printer sharing, require acknowledgement from the remote system. They cannot simply filter such packets out of the data stream going over the ISDN link, since without the response the server would consider the client application to be inactive.

The responses are therefore “spoofed”, or generated at the local end using the remote client's source address. If the ISDN connection is physically active, the packets can be sent over the ISDN line. As soon as the physical connection is interrupted by the inactivity timeout, and as long as the logical ISDN connection persists, the remote access software answers the packets locally, simulating the existence of a physical connection to the remote site. Once the physical ISDN connection has been dialed up again due to user data, spoofing stops and the overhead packets are transported over ISDN again.

The spoofing mechanisms to be used are negotiated with the remote client on connection set-up in accordance with the PSCP Draft. If the remote client does not support spoofing, the function is not activated.

SPX (Sequenced Packet Exchange)

A protocol that enables two workstations or applications to communicate over a network. SPX uses the NetWare protocol IPX for addressing. SPX uses NetWare IPX to transmit data, but controls the receipt and the order of messages in the packet stream.

TCP (Transmission Control Protocol)

TCP is a connection-oriented protocol for use over packet-oriented networks. TCP builds directly on the Internet Protocol (IP) and provides virtual connection services for assured, sequenced transport of user data. TCP provides a reliable connection between two systems. TCP is specified in RFC 793.

Tunneling

Tunneling is a technique in which the packets of a given protocol are transparently transported in those of another protocol. The resulting transparent connection between the endpoints of the transport is called a tunnel. The data packets of the transported protocol are encapsulated for transport in those of the second protocol. At the other end of the tunnel, the encapsulated packets are extracted again.

(VPN) Virtual Private Network

International name for secure logical networks based on virtual connections.

A virtual private network is a wide-area network accessible only to members of a given company or organization, but transported over the existing infrastructure of a publicly available network.

Virtual private networks use tunneling, a technique in which the packets of a given protocol are transparently transported in those of another protocol.

X.75

X.75 is a transfer protocol with a transfer speed of 64 kbits/s.

Remote networks

“Destination/Remote networks” is used as a collective concept designating Internet connections and connections to remote networks.

Index

A

ADC see AVM Data Call Center
ADSL 34
AO/DI (Always On/Dynamic ISDN) 34
ARP spoofing 27
AVM Data Call Center (ADC) 15, 55

C

call-back request 28
caller ID 31
channel bundling 21
CHAP (Challenge Handshake Authentication Protocol) 32
charge profiles 22
compression techniques 45
configuration 14, 46
connecting automatically on start-up 50
connection to the ADC
  testing TCP/IP 16
COSO (Charge One Site Only): see cost assignment
cost assignment (COSO) 28
cost management 8, 21
  AO/DI 34
  call-back options 28
  charge profiles 22
  cost assignment 28
  filters and spoofing 24
  inactivity timeout 21
  logical connection timeout 23
Crypt Provider API 51

D

data compression 20
data encryption 33
default configuration 14

E

encryption techniques 44

F

filters
  NetBIOS 25
  SNMP 25
filters and spoofing 24
first connection
  testing TCP/IP 16

H

header compression 20
HSCSD 5

I

importing a VPN configuration 18
inactivity timeout 21
information sources 54
installation
  automatic 46
  NetWAYS/ISDN 13
  requirements 12
Internet access configuration 17
Internet connections 16
interoperability 10
IP masquerading 35
IPsec 38
  transport protocols 38, 41

L

leased lines 30
locking the settings 49
logical connection timeout 23

N

NAT: see IP masquerading
NCP spoofing 27
NetBIOS filter 25
NetWAYS/ISDN
- configuring 46
- for administrators 46
- removing 19
- service 49

P

package contents 11
PAP (Password Authentication Protocol) 32
pre-configured installation
- call destinations 47
- profiles 48

R

remote access server
- hardware and software 13

remote access with NetWAYS/ISDN 20
removing 19
requirements
- NetWAYS/ISDN computer 12
- remote access server 13

RFCs 52
routing and remote access API (RAPI) 51

S

security 9, 31
- caller ID 31
- data encryption 33
- IP masquerading
- security call-back 32
- user name and password 31, 32

SNMP filter 25
speed 9
spoofing 25
- ARP spoofing 27
- NCP spoofing 27
- SPX spoofing 26
- watchdog spoofing 26

SPX spoofing 26
standards 52
system requirements 12

T

technology 6
test connection 15
throughput 20
timeout
- logical 23
- physical connection 21

tunnel 36, 37, 38

U

user name and password 31, 32

V

VPN
- compression techniques 45
- connections 36
- encryption techniques 44
- import configuration 18
- IPsec 38
- protocol 38
- security 37
- transport protocols 38, 41
- tunnel 36, 37, 38

W

watchdog spoofing 26