

eicon
technology
corporation

[white paper]

Remote Access

Torsten Schulz

19. April 1999

Contents

INTRODUCTION	3
MARKET.....	3
TECHNICAL BASICS.....	4
WAN INTERFACE	4
PC-BASED RAS SERVER.....	5
NETWORK PROTOCOLS	5
TCP/IP	5
IPX.....	6
NETBEUI	6
REPEATERS, BRIDGES, ROUTERS AND GATEWAYS.....	6
REPEATERS.....	6
BRIDGES	6
ROUTERS	7
GATEWAYS.....	7
COMPATIBILITY THROUGH THE POINT-TO-POINT PROTOCOL (PPP).....	7
VOICE OVER IP.....	8
QUALITY OF SERVICE	8
VOICE COMPRESSION.....	8
VOIP RANGE OF APPLICATION.....	9
FAX OVER IP	9
SECURITY THROUGH AUTHENTICATION	10
CALL NUMBER IDENTIFICATION.....	10
PASSWORD AUTHENTICATION.....	11
Password Authentication Protocol (PAP).....	11
Challenge Handshake Authentication Protocol (CHAP).....	11
RADIUS.....	11
PASSWORD TOKENS	12
GENETIC AUTHENTICATION	12
CHIP CARDS.....	12
DATA ENCRYPTION	13
FIREWALL SECURITY	13
VIRTUAL PRIVATE NETWORK (VPN)	14
POINT-TO-POINT-TUNNELING PROTOCOL.....	15
LAYER 2 FORWARDING.....	15
LAYER 2 TUNNELING PROTOCOL	15
IPSEC	16

MANAGEMENT..... 16

RAS SOLUTIONS WITH DIVA SERVER ISDN ADAPTERS 16

SUMMARY 17

REFERENCES..... 18

Introduction

The purpose of this document is to explain the term “Remote Access” and to describe the potential and the limits of this technology. The primary focus is the discussion of various application scenarios—and the hardware and software technologies that make them possible.

Market

The global market for Remote Access Servers is expanding rapidly, with a yearly growth rate of over 40%. Figure 1 charts the projected sales growth, in millions of dollars, for the years 1996 to 2000.

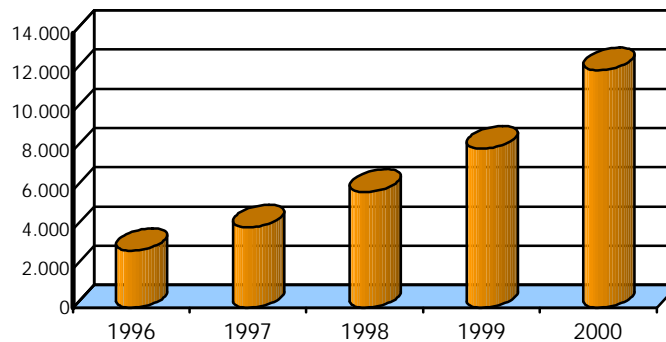


Figure 1: Remote Access Server Market

(Source: The Yankee Group, October '97)

A parallel, equally distinct trend is the growing popularity of NT-based Remote Access solutions. Figure 2 shows that Windows NT already has a clear head start over other operating-system platforms.

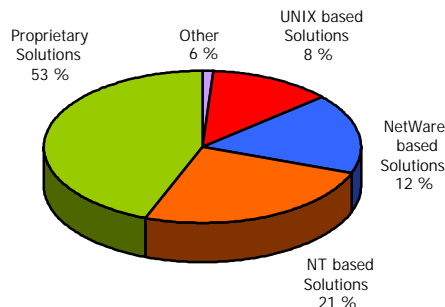


Figure 2: RAS Solutions

(Source: IDC International Data Corporation, 1997)

ISDN-based solutions are particularly relevant to this discussion. Deutsche Telekom activates about 150,000 new ISDN channels each month. By the middle of 1998, there were already 3.7 million BRI connections and 68,000 PRI connections being used by companies and private customers in Germany. And there is no end in sight to the growth of the ISDN market. New and—more importantly—faster transfer technologies have been developed, but because they are not widely available to telecommunications providers, and are hobbled by overall compatibility problems (due to insufficient global standards), their appeal is limited for the majority of users.

After the United States, the European market evidences the fastest-growing demand for Remote Access solutions, as shown in Figure 3. Two target groups make up the bulk of this demand. First are the private customers, who would like to have Internet access at home. Among the growing number of reasons for this is the

increase in services offered on the Web (such as home banking, newsgroups, etc.), which supplement purely consumer sites.

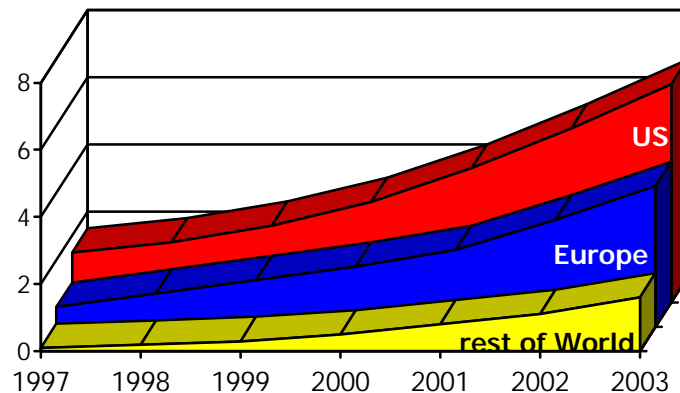


Figure 3: Remote Access Users (in millions)

(Source: Gartner Group)

The second important target group consists of corporations whose outside staff requires access to data from company headquarters while on the road. The increasing popularity of alternative forms of employment (such as telecommuting, or working from a home office) opens up another burgeoning market of potential Remote Access users.

Technical Basics

Conventional routers

Conventional routers are dedicated devices that establish connections between a local network and other networks. They are most often used to couple networks via a WAN connection; specifically, by means of a connection to the local network and a WAN connection to the remote network.

Conventional routers are only partially suited for dial-in connections with several individual workstations. They can, however, be equipped with multiple WAN interfaces for Remote Access. This set-up makes use of only a fraction of their routing capability, and does not provide many important features.

PC Servers

A PC-oriented Remote Access Server allows several individual workstations to be linked simultaneously to an intranet or Internet. The demand for Remote Access Servers continues to grow as the popularity of home employment increases. This new technology will also present Internet providers with many new opportunities.

Windows NT

Windows NT is offered as an operating system with Remote Access Service (RAS). Version 4.0 with Service Pack 3 provides the requisite degree of stability. The hardware required for WAN access is described in the Windows NT Hardware Compatibility List (HCL), and it ensures the successful implementation of tested hardware and minimizes the risk of incompatibility.

The functionality of the Remote Access Server can be extended by installing various “add-on” programs. The ISDN hardware currently available can handle products such as fax servers, online services and voice servers, all on the same server.

WAN Interface

WAN connections for Remote Access are established on various networks, including:

- ISDN

- the analog telephone network (POTS – Plain Old Telephone Service)
- the GSM mobile network
- the X.25 packet-oriented network
- the Internet

WAN connections for Remote Access Servers are established by multiport adapters with modem banks (or one or more ISDN S0 adapters), multiple S0 adapters or S2M adapters. An ISDN network is especially suited to Remote Access, since it provides access to all other networks. This type of network allows the simultaneous use of several channels to various remote stations. The high transfer speed—compared to other media—can be increased even more by bundling channels.

PC-based RAS Server

The trade press is issuing glowing predictions for the future of the “open system”; i.e., PC-based RAS servers. These RAS servers have the following advantages over dedicated hardware solutions:

- They can easily be integrated into existing server architecture—provided it consists of NT-based servers—enabling the combined use of functions such as user administration, access security and domain administration.
- They are readily expandable, making it easy to add ISDN adapters or to increase memory.
- As a component of the simple and familiar NT environment, they significantly reduce the total cost of ownership in regards to education and training—especially when compared to the costs incurred when implementing proprietary solutions.

Network Protocols

The goal of a network is to enable individual workstations—such as computers, servers and printers—to communicate with each other. Data transfer requires the observance of certain rules, which are defined in the form of protocols.

A local network uses network protocols that operate on Layers 3 and 4 of the OSI reference model. The three most common protocols are TCP/IP, IPX and NetBEUI.

TCP/IP

The term TCP/IP is a combination of two essential protocols in the Internet-protocol group: TCP and IP. The Internet Protocol (IP) determines the format of all data sent through the network. By itself, the Internet Protocol is unreliable and must be made secure by the protocol of the transport layer. IP inserts a header before the data to be sent; this header contains the Internet address of both sender and recipient, as well as the identification and length of the datagram.

The User Datagram Protocol (UDP) is a connectionless protocol that is used by higher-layer protocols for exchanging data. UDP provides a simple means for applications to communicate with each other. Like all connectionless protocols, UDP does not guarantee that the recipient actually receives the data. This security must be provided by higher-layer protocols.

Unlike the UDP, the Transmission Control Protocol (TCP) is a connection-oriented protocol, and is used primarily for sending data streams block-by-block. Because it is connection-oriented, TCP provides the higher layers with a reliable protocol that ensures the data reaches the recipient. It thus precludes the possibility of the data being lost, modified, duplicated or mixed up during transfer.

The TCP/IP protocol can be used in both local and wide-area networks. The Internet itself uses the TCP/IP protocol, a fact that has contributed to its prevalence. If a local network is connected to the Internet, it must observe TCP/IP conventions when assigning network addresses. Every country has an institution responsible for allocating these addresses.

IPX

The IPX (Internetwork Packet Exchange) protocol was developed by Novell for the NetWare environment. It is a connectionless transfer protocol on the network layer.

Unavoidable problems arise when using the IPX protocol family for data transfer in a WAN, due to the periodic dispatch of information whose sole purpose is to maintain the network. Protocols that automatically transfer data disable a short-hold mechanism for long-distance data transfer. RIP and SAP broadcasts do not need to be used at all if routing and service information is transferred selectively. These functions can be performed manually in small networks simply by changing the configuration.

Three additional solutions are available for updating this information automatically:

- Timed Update – based on defined timed intervals,
- Triggered Update – occurs after the data has been modified
- Piggy Back – merges information after the transfer of real data

NetBEUI

The NetBEUI (NetBIOS Extended User Interface) protocol was first introduced in 1985 by IBM and Microsoft as the standard protocol for Windows for Workgroups. NetBEUI is a protocol for small networks of up to 200 workstations. It runs exclusively via the NetBIOS interface and offers fast transfer rates and simple network administration.

NetBEUI uses computer names as addresses. Because these addresses do not make network distinctions, this protocol cannot be used with router connections.

Repeaters, Bridges, Routers and Gateways

Since a local network has a limited expanse of network segments—with respect to both the number of connected devices and total length of these segments—solutions are necessary to overcome these limitations. Various technologies may be implemented to connect individual LAN segments to each other. These devices differ primarily in the communication level at which they connect the LAN segments.

Gateway	Layers 4-7
Router	Layer 3
Bridge	Layer 2
Repeater	Layer 1

Figure 4: Network Connection on Varying OSI Layers

Repeaters

Repeaters operate on Layer 1 to connect two LAN segments to each other. Their primary function is signal amplification. Both connected network segments must have the same topology. Data is not evaluated during transfer. Repeaters also do not filter data, and their operation is completely protocol-transparent.

Bridges

Bridges operate on the two lowest layers. They are able to couple segments with divergent topologies. Bridges can also execute Layer 2 functions, such as MAC-address evaluation and error recognition.

MAC-address evaluation enables the bridge to determine which data should be transferred to the other LAN segment, and which data should not. This "intelligent" bridge learns the MAC-addresses of all segment devices and enters them into a table of its own creation. It then decides—based on this table—whether the data packet must be transferred to the other segment. This process prevents any unnecessary burden on system resources and

optimizes network efficiency. Since the bridge operates independently of Layer 3—the network layer—it cannot evaluate network addresses. So it cannot connect more than two segments.

Routers

Routers operate on the transport layer of the OSI reference model. They process the Layer 4 address, selecting the route based on the network address. Routers can therefore transfer only those protocols that employ network addresses, such as TCP/IP and IPX. Protocols that do not use network addresses—like SNA and NetBEUI—can only be transferred via bridges, unless they are embedded in a routing-capable protocol.

Routers also use tables for selecting routes. These tables are defined in part by the network administrator, but can also be learned by the router. Network addresses consisting of multiple ISDN numbers can be neatly arranged in this table. Routers are therefore capable of connecting more than two LAN segments. The bulk of ISDN network connections are achieved with bridges and routers.

Gateways

Communication between devices is most costly when both devices use completely different protocols. These situations are handled by gateways, which work on Layers 4 to 7, and are normally realized via software solutions.

The most important examples are mail gateways, which convert among the formats of various mail systems, and fax gateways, which convert between mail and telefax services. Voice over IP gateways, which convert between voice and data services, are also common.

Compatibility through the Point-to-Point Protocol (PPP)

Individual stations need to conduct extensive mutual communications in order to cope with network requirements. And work in heterogeneous networks that combine divergent solutions requires a comprehensive standard, one that establishes a protocol for WAN connections. The Point-to-Point Protocol (PPP) was developed by the Internet Engineering Task Force (IETF) and has entrenched itself in all corners of the market. This protocol essentially becomes active after a connection is made and before data is exchanged.

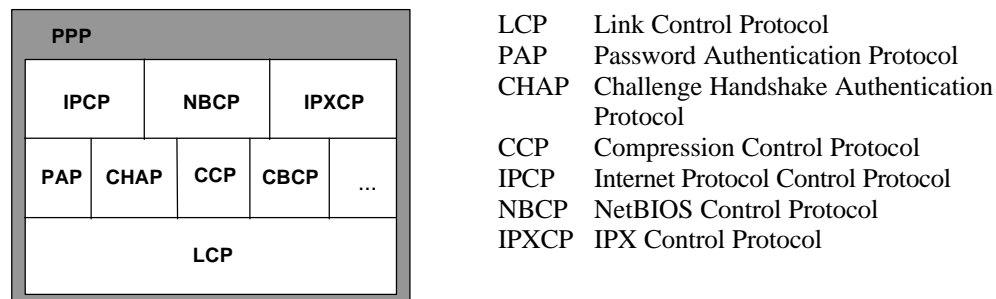


Figure 5: PPP Sub-protocols

PPP, which consists of several sub-protocols, operates on Layer 2 of the OSI reference model. LCP is the first sub-protocol. It negotiates general settings, such as the type of authentication, call-back, and LAN protocol used. This negotiation usually proceeds by the Ping-Pong method: each side states its proposals for the connection, and keeps accepting or refusing the suggestions of the other side, until agreement is reached. Following the LCP negotiation, the mutually acceptable sub-protocols are processed. PAP and CHAP act as access-security measures. CCP negotiates the type of data compression, and a series of other protocols can negotiate additional, connection-specific properties. CBCP comes into play when a call-back has to be negotiated. The connection properties are then negotiated by still more protocols. Finally, protocol-specific settings are negotiated, and the configured protocols are then ready to be used.

The Multilink Point-to-Point Protocol (MLPPP)—developed by the IEFT and published as RFC 1717—increases the rate of data transfer. It supports logical WAN connections over several physical routes

simultaneously (which is known as channel bundling). The MLPPP is ideally suited to ISDN's two data B-channels, but it can also be used for bundling several analog connections—even those of varying speeds.

Voice over IP

Voice over IP (VoIP) owes its existence to the difference in price between long-distance telephone connections and data network connections. Its use requires that a distinction be made between two terms: Internet telephony and IP telephony.

Internet telephony transfers voice transmissions directly from a PC onto the Internet. A telephone conversation is conducted via microphone and loudspeaker connected to the PC. Microsoft NetMeeting is the most common Internet telephony program. Its features also include Internet video communication (image telephony).

IP telephony uses an available data network for transmitting speech by packing voice data into IP packets. VoIP gateways are used to convert the voice data into the IP packets. The advantage of this method is that the subscriber need only use conventional telephone equipment.

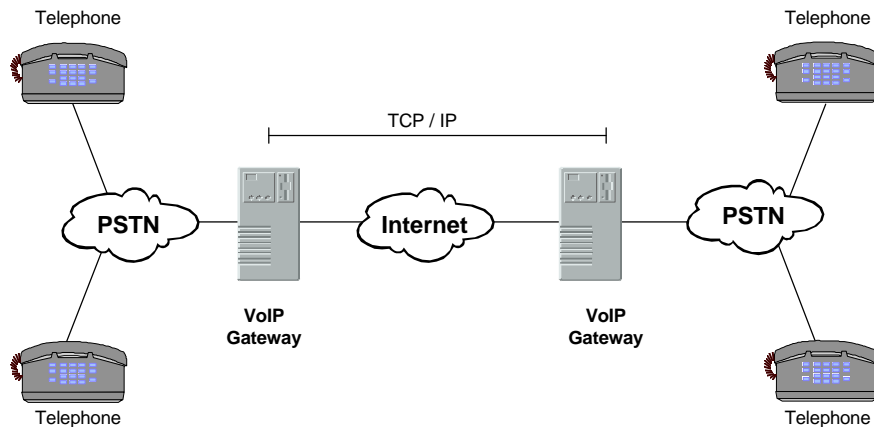


Figure 7: Voice over IP Configuration

Transferring speech over a primarily packet-oriented network entails certain risks. Speech can only be understood when the spoken syllables are played back without interruption. Since accurate syllable-recognition is extremely difficult to realize, a network must guarantee continuous transmission. If voice and data are passed on simultaneously, either the voice transmission must take precedence or the bandwidth necessary for the voice transmission must be guaranteed.

Quality of Service

The Reservation Protocol (RSVP) provides a solution to this problem by reserving a specific network bandwidth for voice communication. RSVP recognizes varying connection classes—such as data and voice—and selects the appropriate bandwidth based on the requirements of the primary connection. To use RSVP, all routers, switches and other network devices must support the RSVP protocol. RSVP does not work with prioritized packets; it only provides signaling for reserving the bandwidth in the network.

Another solution is offered by the Real Time Transport Protocol (RTP), which uses synchronization to prevent delays in voice transmissions and protects against data loss. RTP generates additional fields—including creation time (time stamp) and sequence number—for every packet. RTP was originally developed to guarantee “quality of service,” an increasingly important consideration as Voice over IP becomes more and more popular.

Voice Compression

Voice data can be compressed to take up as little IP-network bandwidth as possible. With ISDN, all 125 voice μ s are scanned and converted into a 12-bit value, which is then compressed into an 8-bit value by a quantization

characteristic (A-law). The quantization characteristic contains the exact frequency ranges of human hearing, neglecting values at the boundaries.

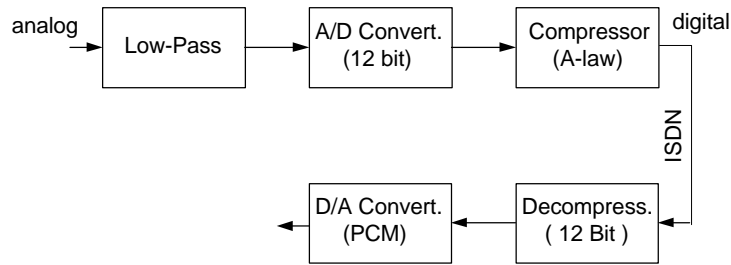


Figure 8: A-law Voice Compression with ISDN

Voice data can be compressed even further. Developments in video conferencing system design have given rise to the primary technology used for IP-based networks: the G.723 voice compression method. Developed from the ITU standard H.323, it runs at a data transfer rate of 5.3 kbps.

Voice transmission may be made even more effective by eliminating the breaks that typically occur in speech. A conventional telephone connection employs the full-duplex method, by which data is always transferred in both directions. Since it is unlikely that both subscribers will speak at the same time, the effectiveness of an IP voice transmission can be doubled simply by using a half-duplex method.

VoIP Range of Application

The VoIP gateway can also convert telephone numbers into IP addresses. Optimum addresses can be generated with the aid of Least-Cost Routers. These determine whether a call should be transported via IP, or whether it can be routed less expensively via the telephone network. Relatively simple VoIP-based telephone systems can be implemented in a home or an office via a data network.

Voice over IP's future viability depends on the price policies of telephone providers as well as the transmission capacity of the Internet. Further expansion of VoIP is possible only if enough total bandwidth can be reserved for it. The too-narrow bandwidth set aside for the Internet may hamper the development and acceptance of this technology.

However, VoIP does offer advantages beyond cost savings:

- It enables systems to be expanded simply and in a variety of ways, either by expanding the network or by adding additional ports to the VoIP gateway
- Voice data—in data format—can be processed by a computer. Calls can be chopped up, and messages from answering machines or voice mail can be saved or forwarded
- VoIP-based PBX features are realized in the software, so additional features—such as conferencing, forwarding and answering machine capabilities—can be implemented easily
- PC-based PBX can be designed and implemented with standard PC components, resulting in enormous price advantages
- The configuration of the system via the network is simple. Existing resources—such as graphical user interfaces or Simple Network Management Protocol (SNMP)—can readily be applied to the task at hand.

VoIP is proving to be a very popular method of connecting local exchanges and telephone systems (cascading) via IP networks. It is also being used for multiplexing several voice channels over a dedicated network with a fixed bandwidth.

Voice over IP with the H.323 standard can also be used for IP-based video conferencing. Although images cannot be transferred, voices are transmitted without any problems.

Fax over IP

Fax documents are currently transmitted via the public telephone network. Calls are metered by the second, and telephone companies charge the highest rates during business hours. However, the same faxes can be

transmitted over the Internet at considerably lower cost. When sent via the Internet, documents incur only local call rates, plus Internet costs.

Fax over IP can be achieved in one of two ways. A fax can either be sent in real time via IP, or it can be sent according to a “store and forward” principle. The ITU and IETF are trying to equivalently standardize both methods in Standards T.38 and T.39.

In many cases, fax servers are already available in local networks. They receive documents via the local network and then establish a long-distance telephone connection for sending them to a remote station. A document may also simply be transmitted via the Internet without the cost of a long-distance connection. On the receiving end, documents are also accepted and distributed by a fax server. Even free-standing fax machines can be reached in this manner, by calling fax gateways that distribute documents to a fax machine via a local connection.

Fax over IP in real-time is actually a by-product of Voice over IP (VoIP). VoIP transmits normal telephone calls via Internet connections. A fax can be transferred via the Internet in the same way. Document receipt is confirmed immediately.

Another Fax over IP option is to send a fax document as an attachment to an Internet e-mail message (depending on the SMTP service). This process is based on the store-and-forward principle. Almost all fax-server solutions already distribute faxes via the local network's e-mail system. Special prioritization or extra Internet services are thus not really necessary, as long as both sides are operating a computer-based system using SMTP.

Fax gateways are particularly interesting in this regard. They establish the connection between the Internet and the telephone or fax network, and they offer Internet Service Providers a wide range of potential activities.

Fax over IP has many advantages. Documents created on a workstation can be transferred digitally by a data service. This process precludes the loss of data, which can occur over analog telephone lines. In addition, digitally-received documents readily lend themselves to further processing. And transfer speed is not restricted to the current maximum data rate of 14.4 kbps.

Security through Authentication

Controlling user access is the first priority of a network security system. Before a data connection can be established, the guest at the Remote Access Server must be unambiguously identified as an authorized user. A number of methods are available to make the process as secure as possible:

- Call number identification
- Password query
- Call-back
- Automatically changing passwords (token)
- Genetic identification

Microsoft's RAS service checks only whether the user has dialing and call-back entitlements. However, other software is available for verifying other types of entitlements:

- Access time
- Access duration
- Duration of a session
- Special IP address, and more

After dialing in, the user has the same entitlements in the domain as he does in the local network.

Call Number Identification

The user's own call number—transmitted automatically over ISDN's control channel—can provide the first stage of Remote Access security. This is only possible, however, if the remote ISDN connection has activated the “Calling Line Identification” (CLID) feature. The advantage of this solution is that access is already controlled before the ISDN data channel is opened. It does, however, rely on the capabilities of the remote connection. The user also cannot make use of this protected access while on the road.

Password Authentication

Entering a pre-defined password is a much more flexible means of authentication. Various types of password authentication—such as the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP)—can be executed as early as the PPP negotiation phase.

Password Authentication Protocol (PAP)

PAP is a simple protocol that transfers the username and password. This data is checked and confirmed on the server side, where a pre-defined password is stored.

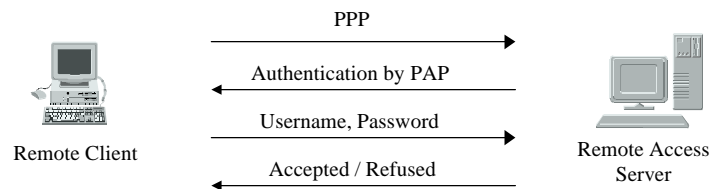


Figure 9: Authentication by PAP

PAP authentication is a threshold requirement in PPP. However, since third parties can read the values for username and password from the data stream, this process cannot be considered especially secure.

Challenge Handshake Authentication Protocol (CHAP)

CHAP eliminates this disadvantage. With CHAP, the server generates a key and passes it on to the client. The client uses the key to encrypt his password and transfers the result back to the server. The server also encrypts the expected password, and compares the result against the encrypted password from the user in order to determine whether the client has access authorization. Since the key itself is continually changing, interception of the authentication data poses no significant danger.

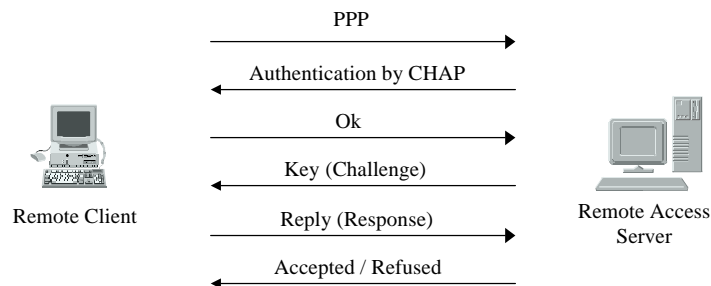


Figure 10: Authentication by CHAP

Unfortunately, CHAP encryption mechanisms vary, so not all CHAP implementations are mutually compatible. Windows NT RAS, for example, uses MS CHAP, and Cisco uses CHAP MD5, so these systems can communicate only via PAP.

RADIUS

Even the CHAP option has security gaps. Passwords can be read off a monitor screen, or the transfer of keys can be manipulated. A series of more sophisticated authentication options have therefore been developed, along with a special protocol that can be used for all kinds of authentication. The Remote Access Dial-In User Service (RADIUS) is an open standard that is gradually replacing proprietary TACACS-based solutions.

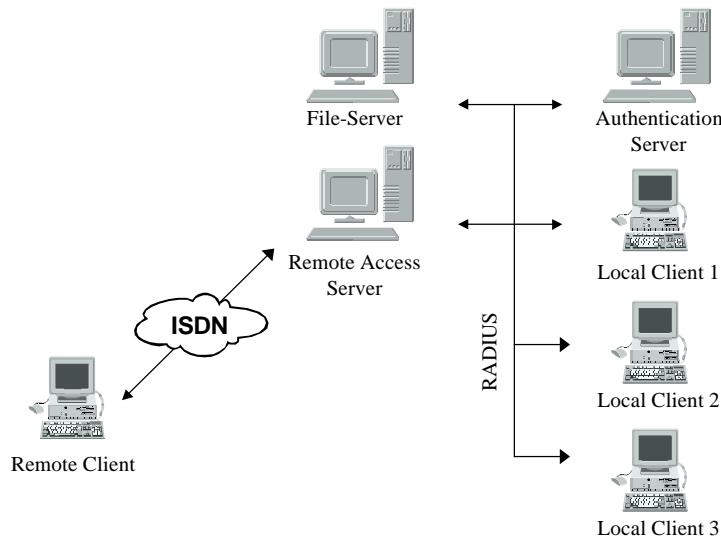


Figure 11: RADIUS Protocol for Authentication

The RADIUS protocol, which is based on TCP/IP, establishes the connection between the client in the local network and the Remote Access Server, taking the place of the remote client with respect to the authentication server.

Password Tokens

Password tokens are widely used to provide an even higher degree of access security. These tokens are small cards or key rings that generate new passwords and show them on a small display. A one-way procedure ensures that the passwords are generated simultaneously on card and server. For authentication, the password is transferred along with an identification number (PIN). Each password has a life span of one minute. The token itself is protected by the PIN. If lost, the token cannot be used without the PIN. PIN-pad cards, on which the PIN and password can be encrypted, protect the PIN from being read by unauthorized persons.

Password tokens are an expensive solution, since every user has to have his own card. And, in spite of the expense, they can only safeguard authentication—not data transfer.

Genetic Authentication

A very personal type of authentication can be achieved through the transmission of genetic values. These may include facial features, lip movements and speech. The hardware required for this authentication—such as microphone and camera—is already installed in many workplaces. Unfortunately, speech variables and changes in appearance can create difficulties for authentication equipment. Only high-grade programs can successfully deal with these problems.

Chip Cards

Chip cards (Smartcards) are one of the most secure methods available for authentication and data encryption. A Smartcard is a plastic, bank-style card with an integrated microchip. Reading devices can be connected to client computers as external components, built into the PCMCIA (PC card) structure, or integrated into a keyboard. The Smartcard itself is protected by a PIN.

The Remote Access Server uses a Challenge Response method for authentication. Personal identification (PID) is first sent to the server, which sends a request (challenge) back to the Smartcard, which in turn calculates the response to send back to the server based on a user-specific personal value (personal key – PK). After the server confirms the response, additional settings—which are stored on the card—are entered for the new user. All transferred data is then encrypted. The keys are stored in a safeguarded area of the card memory. The encryption process, however, is so computationally demanding that it must be performed by a computer. High-end Smartcards handle their own encryption by means of a crypto-coprocessor.

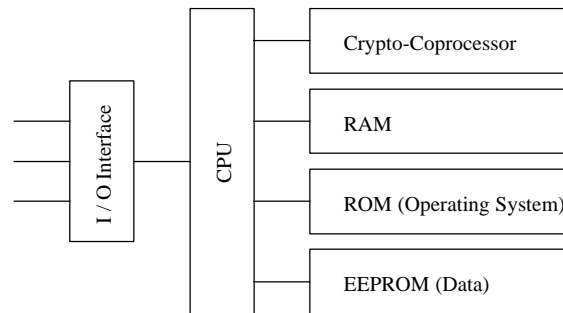


Figure 12: Internal Structure of an Authentication Chip Card

Data Encryption

After authentication, data traffic can begin to flow. But even at this stage there is a constant threat of data being intercepted. To protect against this, data must be transferred in an encrypted state. Encryption takes on two forms: synchronous and asynchronous.

The RSA method—named after Rivest, Shamir and Adleman—is based on factorizing large numbers in a short time. Encryption and decryption require the calculation of modular exponents, a very time-consuming process. RSA thus cannot be used for data encryption in real time, but remains a viable option for seldom performed operations, such as authentication of the remote site, or the exchange of keys or the digital signature.

DES is the abbreviation for Data Encryption Standard. The block ciphers used most often in data encryption operate according to this standard. The size of a block is 64 bits (the same as the key length), eight of which are required for error protection. The disadvantage of a key that is only 56 bits long is compensated for by triple encryption (Triple DES). DES is considered a symmetrical method because both sender and recipient need to possess the same key.

Firewall Security

A Firewall performs two primary functions: it prevents unauthorized access in a local network, and it controls the access that local stations have to the Internet. It works by identifying the user and verifying his network entitlements.

Firewalls are usually dedicated devices having access to a known system (trusted network) and an unknown network (untrusted network). Firewall functions are often offered in proxy servers, software routers and Remote Access Servers.

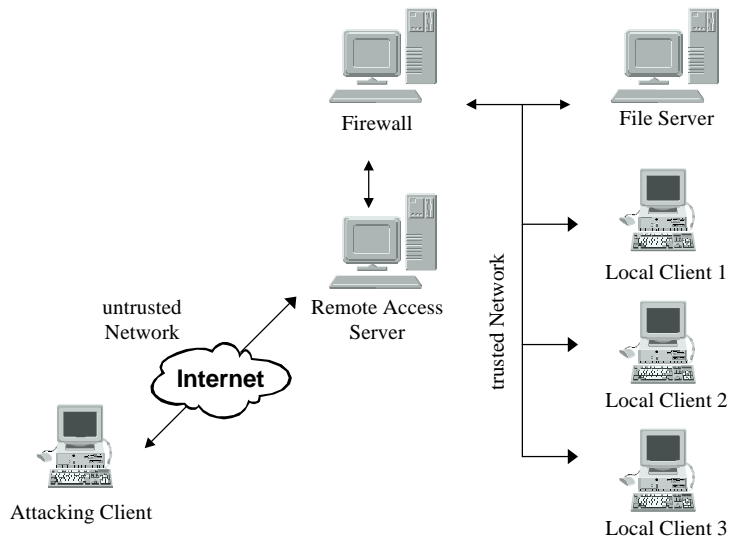


Figure 13: Firewall Protection for Remote Access

Firewalls operate at various levels in a network (OSI reference model). A network-layer Firewall works on Layer 3—the level at which the TCP/IP protocol operates. The other part of the Firewall works at the application level, which is the next layer above. A range of restrictions can be defined on the network layer, including:

- Source addresses
- Target addresses
- Port numbers
- Protocols
- User ID
- Time of day
- Domain / Subnet

Restrictions on accessing Internet services (HTTP, SMTP, FTP, Telnet, etc.) are defined primarily at the application level. Information on attacks fended off is especially useful to the operator. Logging and alarm functions should also be taken into consideration when selecting a Firewall.

Virtual Private Network (VPN)

The Internet is ready to replace public telecommunication networks (ISDN, telephone network, GSM, etc.) as a medium for transferring data. Using the Internet saves money otherwise spent on long-distance calls and allows access from sites having any kind of Internet connection. Private networks that exist on the Internet are called Virtual Private Networks (VPN).

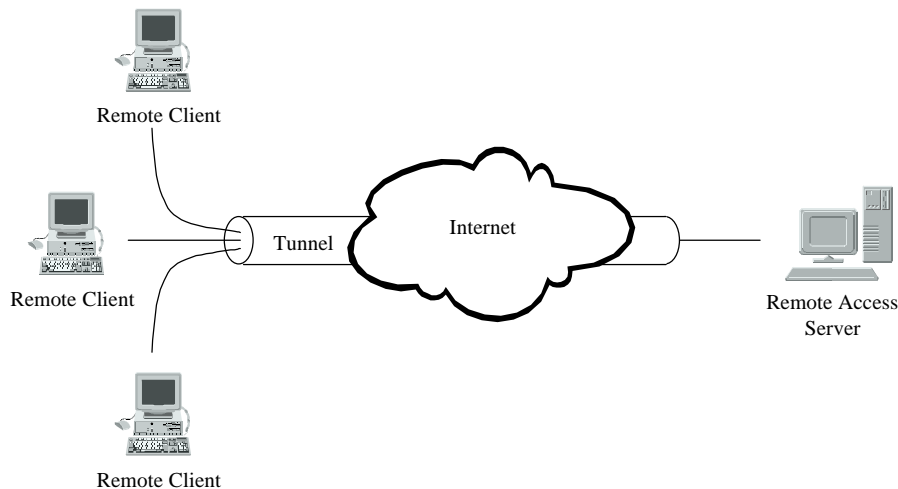


Figure 14: Virtual Private Networking (VPN)

Tunneling is the name given to the form of data security employed for the special transfer of private data via the Internet. Tunneling takes data and protocols from one protocol stack and encapsulates them in a second protocol stack. This second protocol deals with routing and encryption. The protocols for various tunneling procedures include:

- Point-to-Point-Tunneling Protocol (PPTP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- IPSec Tunneling

Tunneling is also useful for packing protocols not normally transferable via the Internet into the Internet protocol. The SNA protocol, for example, can be transferred over the Internet using the tunneling method.

Point-to-Point-Tunneling Protocol

The Point-to-Point Tunneling protocol encapsulates IP, IPX or NetBEUI packets into IP packets. It uses TCP to manage the tunnel and PPP to encapsulate the data. PPTP must be installed only on the client system and the server. The intermediate network infrastructure knows nothing of this process, and treats PPTP as a normal TCP/IP datagram.

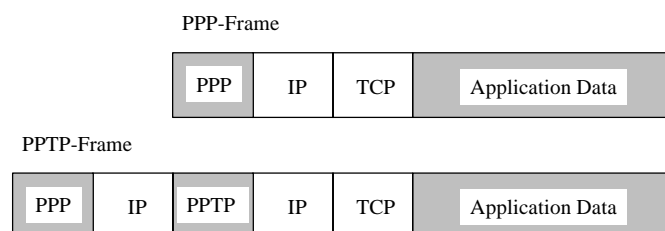


Figure 15: PPTP Frame Structure

Layer 2 Forwarding

Layer 2 Forwarding is a Tunneling protocol developed by Cisco for ATM and Frame Relay. It requires that all participating routers and servers support the L2F data stream.

Layer 2 Tunneling Protocol

The Layer 2 Tunneling Protocol, a compromise between PPTP and L2F, has been proposed as a standard by the IETF. It uses UDP to manage the tunnel and UDP/PPP to transfer data within the tunnel. Data is encrypted on the basis of the methods defined for PPP.

IPSec

IPSec is a type of Network Layer Tunneling (on OSI Layer 3). IPSec defines how a complete IP packet is encrypted and passed on as data to another IP packet. It enables the creation of Virtual Private Networks without having to consider the attributes of the network structure used.

Management

One of the advantages of the Windows NT-based Remote Access Server is the flexibility of the graphical user interface. Special RAS applications increase the manageability of users and resources via the RAS API. The following features are standard:

- Access based on time
- Access based on usage duration over a certain time period
- Access based on transfer volume in a certain time period
- Access limited to connection fees (ISDN call-back)
- Saving of the connection data for accounting and statistics

This software expansion is, in some cases, an absolute necessity. The RAS Management Function alone does not enable Internet Service Providers to perform customer accounting.

Larger systems are usually monitored and configured from a central site. Complex management solutions are, in many cases, already being employed for this purpose. These solutions use SNMP to control the various network devices from a single management interface. Devices for remote access should therefore also support SNMP.

The following standard MIBs are defined as RFC for RAS equipment:

- RFC 2127 (ISDN)
- RFC 2128 (Dial MIB)
- RFC (Modem MIB)
- RFC (T1 MIB)

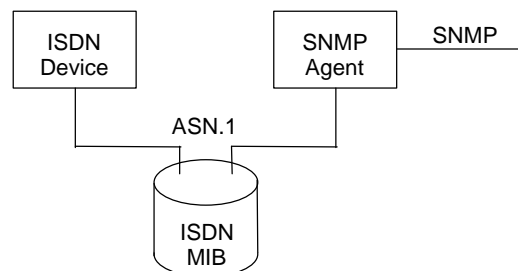


Figure 16: SNMP Component Connections

The Management Information Base (MIB) stores the latest data for each device. The MIB for ISDN is defined in the RFC 1213. The objects of the MIB are defined in the Abstract Syntax Notation One (ASN.1) and have a unique name by which they are addressed. The SNMP Agent is a small program that has access to the database and can itself be addressed via the SNMP protocol. The SNMP protocol supports only three operations: Set, Get and Trap. Get and Set enable MIB information to be read and set. The Trap operation contains warnings and error messages for the management interface.

RAS Solutions with DIVA Server ISDN Adapters

Eicon Technology's DIVA Server product line is ideally suited for connecting Remote Access Servers to ISDN networks. The product line offers a wide range of hardware, including the active, 2 channel adapter DIVA Server BRI, the 8 channel adapter DIVA Server 4BRI, and the DIVA Server PRI, which supports 23 (North America and Japan) and 30 (Europe) simultaneous channels. Additional adapters can be installed in the same computer, allowing configurations of up to 120 channels.

Existing driver software improves RAS performance considerably. It automatically recognizes all supported types of calls—whether they originate from an analog telephone network (modem), ISDN or GSM—and handles them accordingly. For the administrator, this means that all remote users—regardless of the service they are using—can call the same dial-in number. DIVA Server adapters also support features such as callback and channel bundling.

The Eicon Remote Access Manager—provided as an option—further increases system manageability. It offers expanded access control (including access at certain times, and limits on data, time and ISDN call numbers), and supports a comprehensive set of information for statistical analysis of RAS use.

There are also numerous interfaces available for expanding the functionality of the RAS server. CAPI 2.0 gives all CAPI applications access to the ISDN gateway, enabling implementation of solutions such as central fax communication, speech processing (voice messaging) and software multi-protocol routers. Modem emulation is also available for all modem-based programs, such as CompuServe software, various terminal programs and numerous fax programs.

Not to be forgotten are the more than 100 different fax-support solutions on the market, most of which can be implemented on the CAPI interface. Non-European fax servers still use modem technology. Eicon's DIVA Server solutions, however, support almost all fax server solutions.

Summary

The rapidly-increasing popularity of communications solutions using PC-based Remote Access Servers can be attributed to a number of key factors. They are reasonably priced, adaptable to a wide variety of tasks, relatively simple to implement, and can be custom configured to address an organization's specific requirements.

Eicon Technology's extensive product line of DIVA Server adapters supports a complete range of communication types and protocols, so it offers an almost limitless flexibility. Additionally, the DIVA Server adapters are fully scalable, so organizations seeking to implement an open system remote access solution can easily install additional adapters in their servers at any time to accommodate their growing needs. In short, Eicon's DIVA Server adapters provide an efficient, cost-effective, and versatile remote access solution for corporations of any size.

References

- [1] Eicon Technology's Entry into the Fax Market, Peter Hum, June 26, 1998
[2] ISDN am Computer, Torsten Schulz, Springer Verlag Berlin, 1998

Eicon Technology Corporation

Tel.: (514) 745-5500
Fax: (514) 745-5588

**In the United States, Canada,
Latin America:**

Tel.: 1-800-80-EICON
(214) 239-3270
Fax: (214) 239-3304

In Europe, Middle East, Africa:

Tel.: (44) 181 967-8000
Fax: (44) 181 967-8050

In Australia, New Zealand, Asia:

Tel.: (61) 2 9919-7200
Fax: (61) 2 9929-6300

Internet:

North America: sales@eicon.com
Europe: sales.europe@eicon.com
Asia Pacific: sales.asiapac@eicon.com
Worldwide Web: <http://www.eicon.com/>

