SIEMENS

Remote Maintenance with WinCC flexible
Communication via a Wide Area Network (WAN)

Basic Knowledge **Issue 12/04**

Foreword

This document contains an introduction to the following Sm@rt options in WinCC flexible:

- Sm@rtAccess
  - Distributed operator panels with Sm@rtClients
    Operation on a remote machine
  - System-wide access to tags via HTTP
    Read and write access to tags
  - Interface between panels and Office applications
    Read and write access to tags
- Sm@rtService:
  - E-mail support
    Sending e-mails based on signals and events
  - Maintenance functions via the Interface
    Standard HTML pages with service and maintenance functions, as well as diagnostic information
  - Remote control via the Internet
    Complete remote control of an HMI system with the aid of the Internet Explorer

Disclaimer / Liability

Siemens AG accepts no liability, regardless of the legal grounds, for damages arising from the use of this entry, apart from the statutory liability accepted, for example, for damage to items used for personal purposes, personal accidents or due to malicious intent or gross negligence.

Warranty

The entries relate to selected suggested solutions for queries with complex tasks which have been dealt with in Customer Support. We also wish to point out that current technology not does permit us to exclude the possibility of errors in software programs taking all application conditions into account. The entries have been compiled to the best of our knowledge. We cannot agree to accept any liability over and beyond the standard warranty for class C software in accordance with our "General Terms and Conditions for the Transfer of Software Products for Automation and Drive Technology". The programs are available on the Internet under individual licenses. They are non-transferable.

Contents

1 Introduction

WinCC flexible and the Sm@rtService option enable you to connect directly to an operator panel via the Internet from your service / maintenance station.

This gives the service technician remote access to the operator panel, enabling him to call up its operator interface directly at his service / maintenance station and monitor developments in-process. Updated WinCC flexible projects can be transferred more quickly this way.

You can use the remote access for the following applications:

- Remote administration
  You can transfer a project from the station to an operator panel. This allows you to update WinCC flexible projects from a central location.
- Remote diagnostics
  Each panel provides HTML pages from which you can access the likes of the installed software, version or system messages using a web browser.
- Remote operation and monitoring
  You can control an operator panel from your station and monitor developments in-process.

Two HMI systems can communicate with one another with the Sm@rtAccess option.

- Distributed operator panels with Sm@rtClients
  Operation on a remote machine
- System-wide access to tags via HTTP
  Read and write access to tags
- Interface between panels and Office applications
  Read and write access to tags

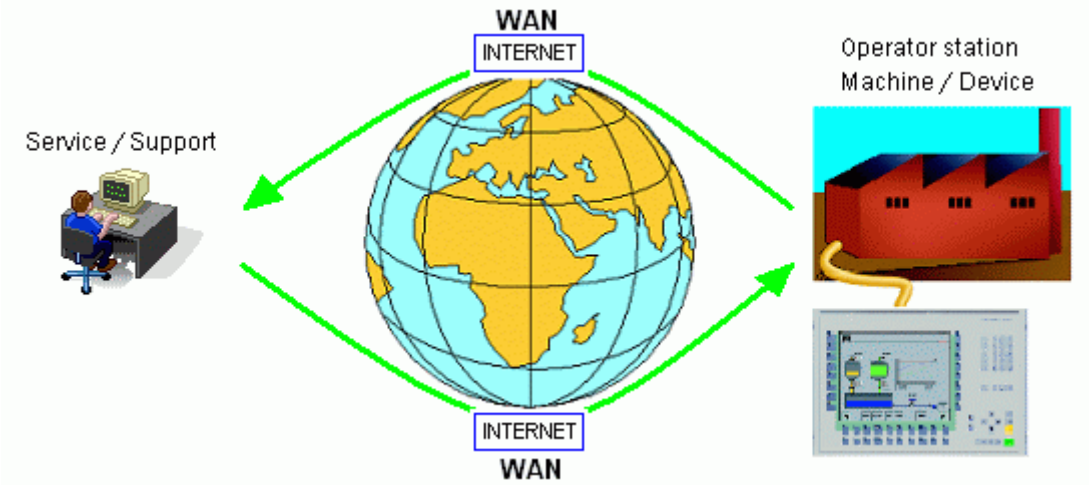
You can find detailed information about Sm@rtService and Sm@rtAccess, as well as a sample application relating to this topic in the following manual:

WinCC flexible 2004, Getting Started Options

Entry ID: 18657078

2 Automation task

Fig. 2-1



2.1 Typical examples

Case 1:

You are providing support for a customer's system abroad. In your company you are developing new process flows for your customers. Consequently, the recipe data has to be changed "on site" at the customer's facility, and the operator interface has to be adapted to the new process flows. This change should be made in-process at the customer's facility without causing a major interruption.

Case 2:

You are providing support for a customer's system. The customer is having difficulties with this system. The problem cannot be resolved by telephone. You need to view the system values online.

Case 3:

There needs to be a facility for remote operation and monitoring of other SIMATIC HMI systems from a central location (control room), as well as for system-wide information retrieval and archiving of process data.

2.2 Possible solution

You can now perform the following in cases 1 and 2 described in section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

- You can connect to your customer and implement the changes "on site".
- You can connect directly from your service / maintenance station to the customer's HMI operator panel via an Internet connection. (Sm@rt Service)

You can now perform the following in case 3 described in section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

- Sm@rtAccess allows you to access process values for the machine and retrieve information from a central location (HMI system serving as a head end). This means that process values can be archived or analyzed centrally, for example, without having to be directly on site. In order to access the process values, the head end (e.g. a PC with WinCC flexible Runtime) accesses the tags on the remote operator panel via the SIMATIC HMI http protocol.

2.3 Precondition

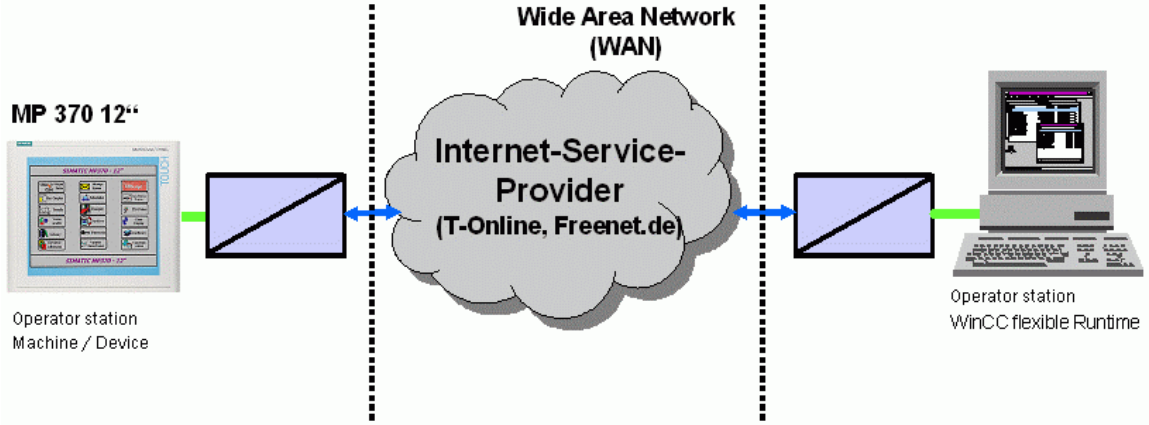
- HMI operator panels from the 270 series with an Ethernet interface
- HMI operator panel on the basis of WinCC flexible
- HMI operator panel with the Sm@rtService or Sm@rtAccess option.

Note:

- A SIMATIC panel can only be connected to a WAN via Ethernet using a network access device (router). The router establishes the connection with the Internet service provider (ISP).

3 Networking via WAN

Fig. 3-1

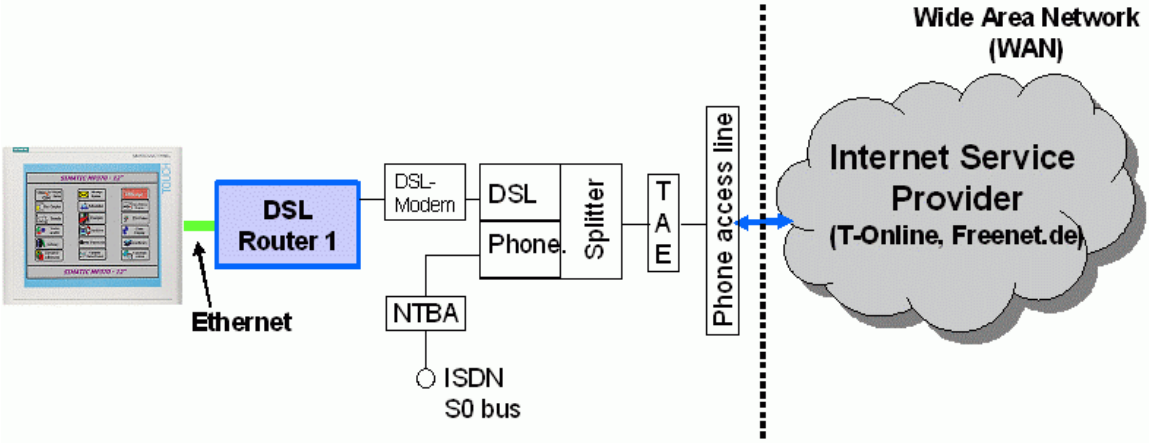


This task gives rise to the following questions:

- How can I connect the panel to the WAN (wide area network)?
- Which hardware components does this involve?
- What is the IP address of the panel that I wish to contact?
- How secure is the connection?
- Which settings need to be configured?

3.1 How can I connect the panel to the WAN?

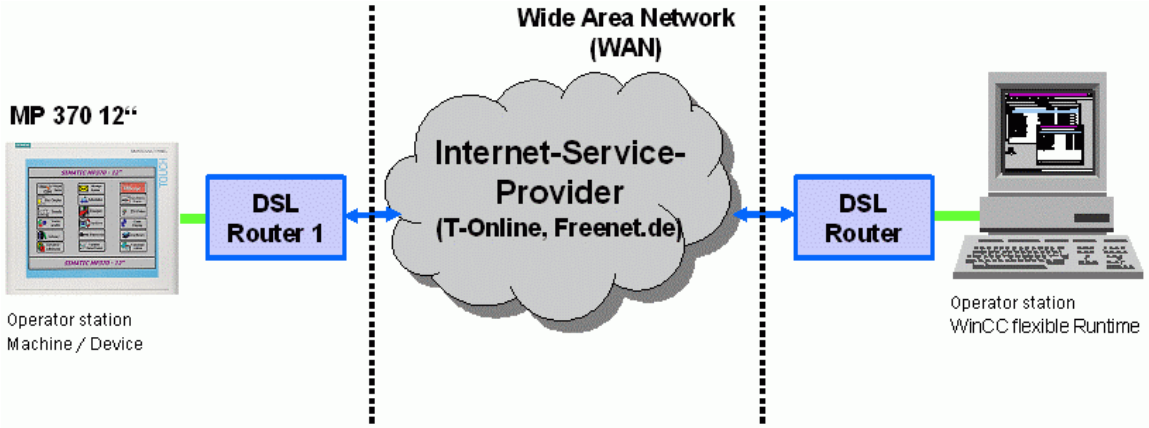
Fig. 3-2



A SIMATIC panel can only be connected by Ethernet to a network access device that can create a connection to the Internet service provider (ISP). This is generally a PC or, more cost-efficiently, a router.

3.2 Which hardware components does this involve?

Fig. 3-3

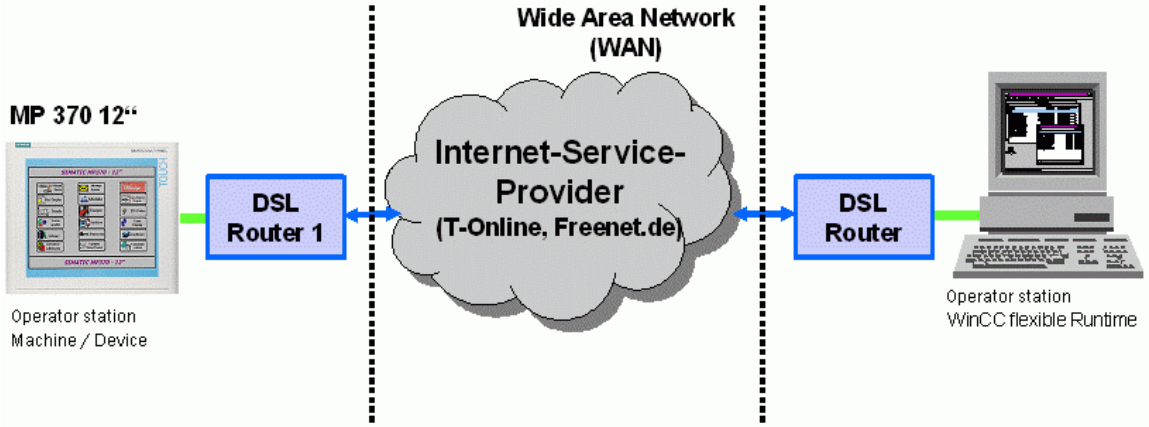


You require a router or a PC with network access in order to connect a SIMATIC panel from the 270 series.

Routers are available with analog (rather rare), ISDN or DSL network access. Routers feature several Ethernet ports (RJ45) for creating a LAN.

3.3 What is the IP address of the panel that I wish to contact?

Fig. 3-4

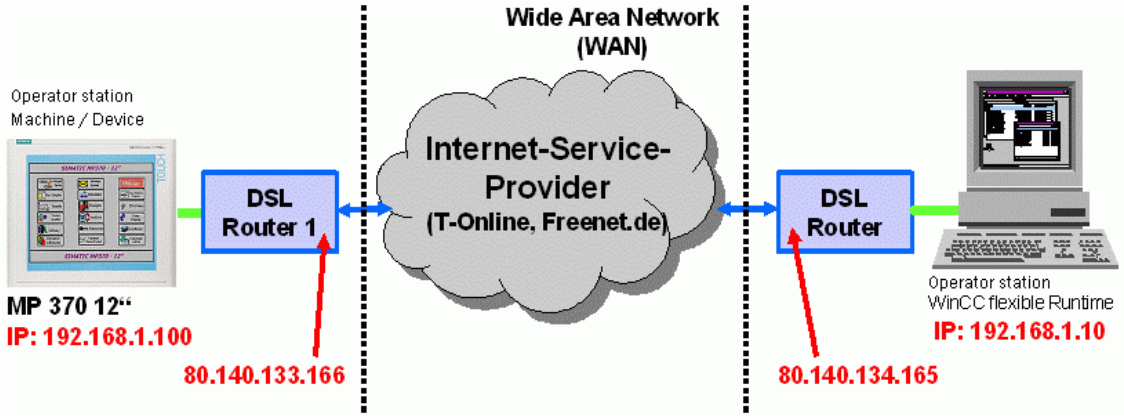


A distinction is made between two connections:

- Using a static connection
  - The IP address is disclosed by the Internet service provider (ISP). The IP address is static; i.e. it does not change after a session has been disconnected and re-connected.
- Using a dynamic connection
  - The IP address is assigned dynamically by the ISP (Internet service provider). This means that it changes from one session to the next.

3.4 Using a static connection:

Fig. 3-5

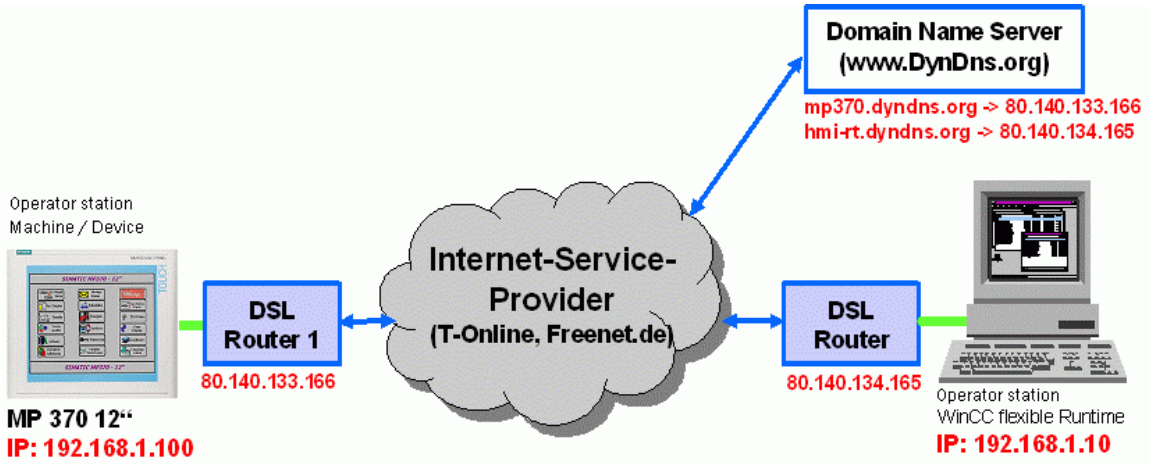


Using a static connection:

The IP address is disclosed by the Internet service provider (ISP), e.g. 80.140.133.166
This is the address of the network access device that has created the connection to the ISP via the WAN. A router or PC needs to be used in connection with a SIMATIC panel from the 270 series.
Router 1 in the example above diverts the request from the other side to the panel's local IP (TCP port number) (e.g. 192.168.1.100).

3.5 Using a dynamic connection:

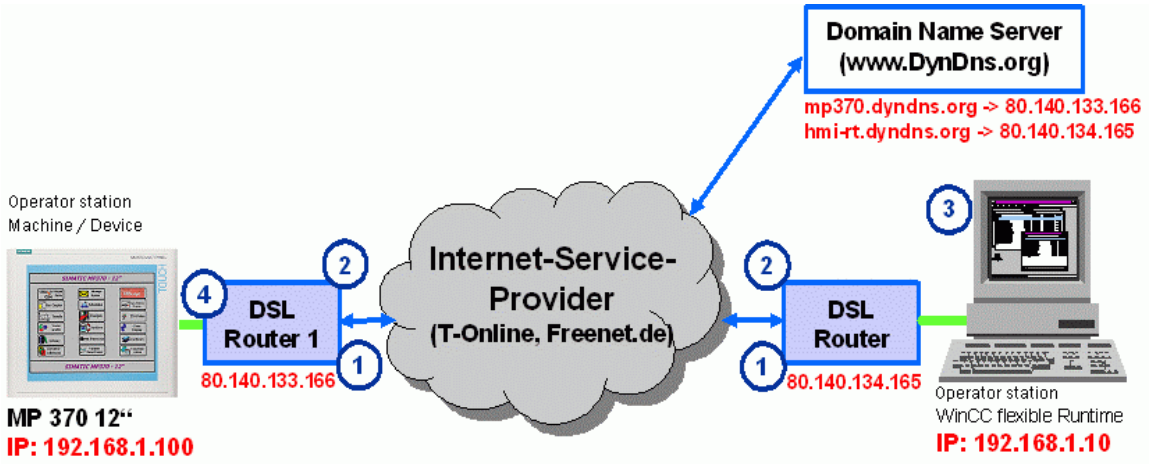
Fig. 3-6



Using a dynamic connection:

The network subscriber's IP address is allocated dynamically by the ISP after the connection has been established. This means that the address changes from one session to the next.
This status doesn't make sense for connecting several machines/systems via the WAN. Domain name servers (DNS) are to be used to enable the addressing process to be automated.

Fig. 3-7



Using a dynamic connection:

1. The DSL routers establish a connection with the ISP and are assigned a dynamic IP address

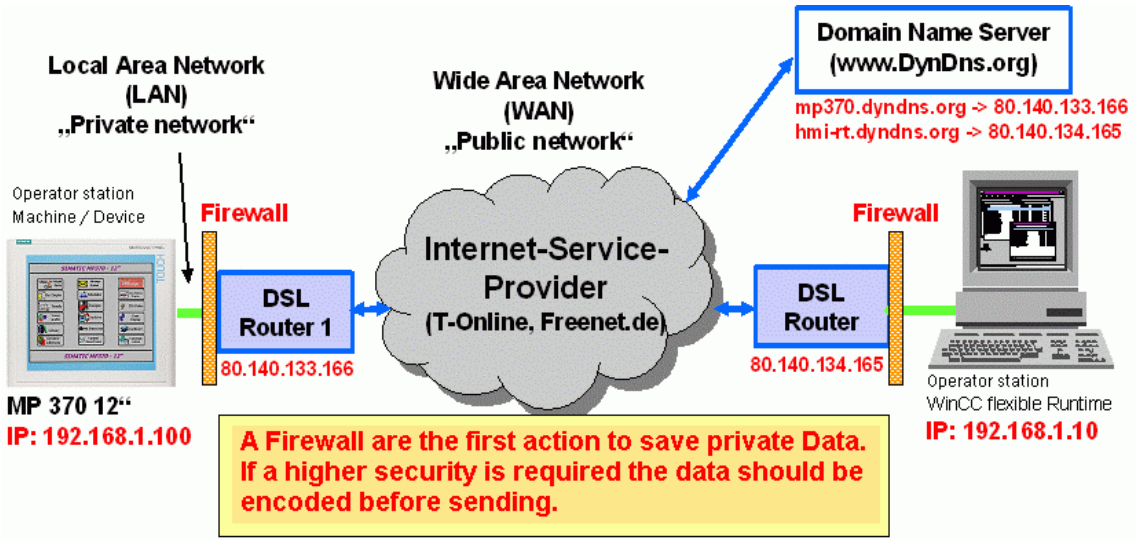
2. The DSL routers signal their IP address to a DNS server

3. HMI-RT calls up a connection via DNS – e.g. mp370.dyndns.org
   The DNS server routes the request to IP "80.140.133.166"

4. Router 1 diverts the HMI-RT's request to the local IP address
   (TCP port number) on the panel (e.g. 192.168.1.100)

3.6 How secure is the connection?

Fig. 3-8

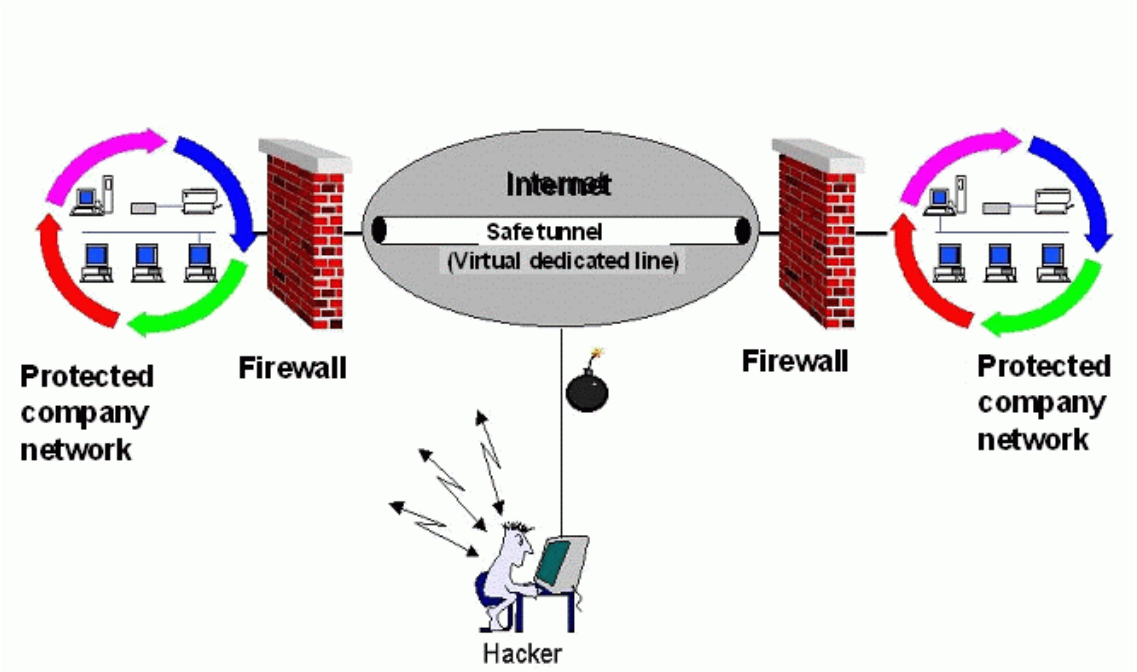


The local networks listed above can be secured with the aid of an optional firewall. In this example the firewall is based on a combination of hardware and software and is integrated into the router.
The following technology is typically applied by the firewall:
Packet filter, application gateway, circuit level gateway, proxy server, virtual server, …

3.7 Virtual Private Networks - VPN

Increased security through virtual private networks (VPN)

Fig. 3-9



Increased security through virtual private networks (VPN):

Instead of using expensive modem routes or leased channels, VPN technology uses the Internet as a "carrier medium".
Using a VPN enables someone who goes on business trips (or who works from home) to connect to the company Intranet using the Internet. This makes a VPN the cost-efficient alternative to classical dial-in / remote access solutions.
However, VPNs can additionally be used to link two company sites (instead of dedicated lines) (site-to-site or branch-to-branch connections).

3.7.1 Connection via a VPN tunnel (IPsec)

Fig. 3-10

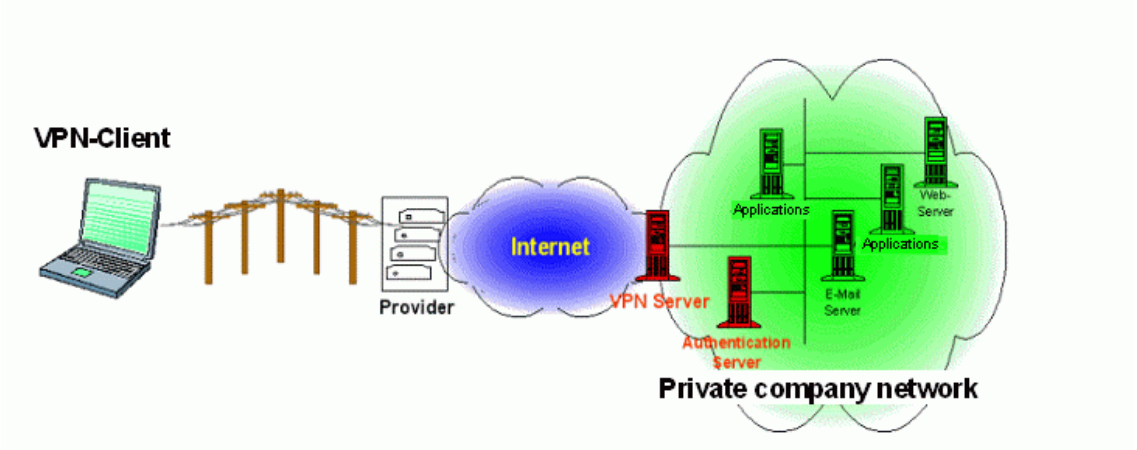
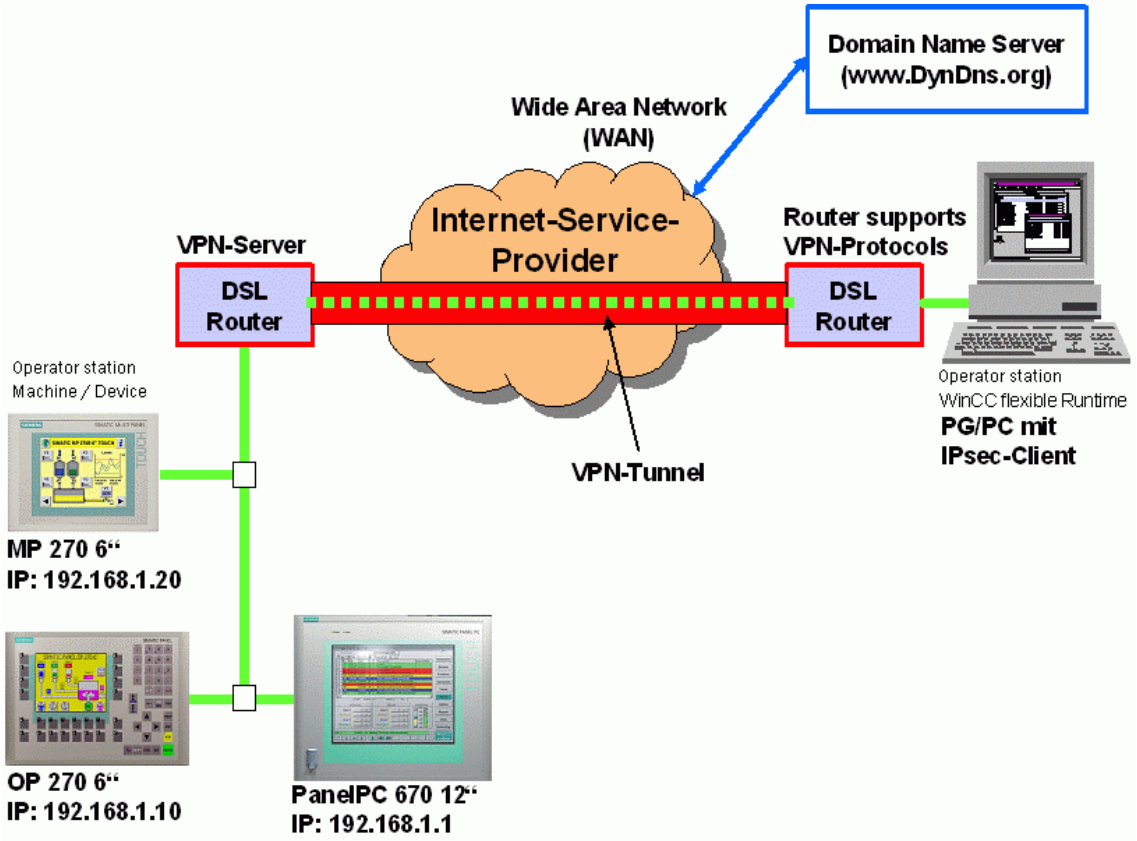


Fig. 3-11



3.7.2 Overview of the advantages of VPN network connections

- Virtual
- Cost savings
- Improved security
- Simple expansion of networks
- Speed of implementation
- Private IP addresses can be re-used in the VPN
- Integrity / Authenticity
- Encryption
- Internet Protocol Security (IPsec)

3.7.3 Some links to the topic of "VPN" …

Material in English

- http://www.vpnc.org
- http://www.intranetjournal.com/foundation/tunneling.shtml
- http://security.ittoolbox.com/documents/document.asp?i=3195
- http://computer.howstuffworks.com/vpn.htm
- http://www.bintec.de

Material in German

- http://www.itseccity.de
- http://www.itseccity.de/?url=/content/fachbeitraege/grundlagen/020525_fac_gru_verio.html
- http://home.t-online.de/home/TschiTschi/vpn.htm
- http://www.bintec.de

3.7.4 Additional information about the VPN (Virtual Private Network)

- **Cost savings:**

Cost savings are an important factor for businesses that opt to use IP-VPNs in the current economic climate. The sites were previously linked by a dedicated line or by a PVC (private virtual circuit). IP networks provide access to the whole IP network for the price of only one site. Thanks to the shared infrastructure, connectivity charges are also lower. Mobile users and remote users can connect to an IP network via private networks.

Generally speaking, a VPN is a network which is implemented on another, generally public, network. This process of tunneling from a 'private' network through public networks is the basic concept of a VPN. Why should something like this be done now? Increasing complexity in your own network is only worthwhile in very rare cases. As a general rule, a VPN is suitable in all applications where dedicated lines (DDV, ISDN) or public-shared networks such as Datex-P, Frame Relay or ATM are used.

The low costs can be verified by anyone who has had to set up a classic WAN. The total costs resulting from DDVs (local loops) and WAN charges can prove to be very high.

The second challenge embodied in the classic corporate network is the considerable complexity in terms of routers and data links. This can easily become difficult to manage, in particular if links are required to more than one provider on account of regional circumstances.

- **Virtual:**

There is no new meaning in the term 'Virtual' in VPN. If you look at Datex-P, Frame Relay and ATM, or even at the telephone network, they are actually virtual networks. If you call someone, it is as if you have set up a direct wire ear-to-ear. However, that perception is simply incorrect. Thousands of phone calls are routed via the same fiber-optic cable at the same time. The wire between you and the other person is virtual. This is also true of Datex, Frame Relay and ATM.

- **Improved security:**

In VPN, data traffic is separated by means of encryption. This protects your data from unauthorized access by third parties. In contrast to a VPN, this sort of hacking is very difficult to detect, let alone prevent, in a network that is based on a private dedicated line.

- **Simple expansion of private networks to remote locations:**

Installing and operating a private network is often too costly an option to contemplate for businesses in remote locations outside a city. Where budgetary constraints apply, a VPN in a mixed network environment is generally the only alternative for providing the services.

- **Speed of implementation:**

In contrast to setting up a separate WAN, when implementing an IP-VPN, much of the infrastructure is already in place. This allows the network to be set up quickly and developed flexibly.

- **Integrity / Authenticity:**

The privacy of the communication is closely linked to its authenticity. The communication of material that is not trivial in nature requires an assurance that the person sending the message is who he claims to be. The integrity of the messages also has to be ensured. The message must contain the information that the sender has sent. Outsiders may feed supposedly authentic messages into networks where security is weak or non-existent, with damaging consequences; or tamper with original messages.

- **Encryption:**

Since no-one within a global environment has physical control over the whole network, the entire WAN infrastructure has to be regarded, to a greater or lesser degree, as public. Since physical control does not exist, cryptology is the method of control used in the virtual world. An encrypted VPN - and when people talk about VPNs nowadays, encryption is implicitly presumed – provides a chance for communication with privacy, authenticity and integrity.

'Chance' being the operative word because just as physical control is frequently unsatisfactory, so too is this also the case in the virtual environment. Only in real life can you, as a lay person, spot a damaged fence; experts often have difficulty spotting this in virtual applications. Even big names in IT don't offer any guarantee of absolute security. With everything from scientologists as suppliers and NSA keys in the crypto module to simple design errors.

- **Internet Protocol Security (IPsec):**

The de facto standard for VPN software is currently IPSEC. This open standard comprises three protocols that can be/are used in an IPSEC implementation:

- ESP, Encapsulating Security Payload, encrypts and certifies data.
- AH, Authentication Header, provides a package certification service.
- IKE, Internet Key Exchange, negotiates connection parameters, including the keys, for the first two protocols.

These protocols implement connection security and are based themselves on a number of encryption protocols, including

- DES, Data Encryption Standard, obsolete, not supported by some implementations for security reasons
- Triple DES
- AES, or Rijndael Advanced Encryption Standard, successor to DES
- RSA, patented public key algorithm. Patent has expired
- MD5, Message Digest Algorithm
- SHA, the Secure Hash Algorithm
- Diffie Hellman key exchange protocol

IPSEC is implemented by a series of providers on routers, firewalls and as software on servers and desktops. Its strength is the open source nature of the protocols used; there are even open source implementations available.

3.7.5 Which settings need to be configured?

Ports to be enabled on a firewall

Sm@rtService:

HTTP access:	Port 5800 (loading the Java applet)
Main:	Port 5900

Web server:

HTTP	Port 80
HTTPS	Port 443 (SSL)

Ethernet transfer	Ports 2308 and 50523
VPN (IPsec):	Port 500 (Internet Key Exchange Protocol IKE)
E-mail (SMTP server):	Port 25

4 Glossary

Table 4-1

No.	Abbreviation	Description
1	ADSL	Stands for Asymmetric Digital Subscriber Line. ADSL supports the use of the infrastructure in the existing phone network for broadband utilities. Additional data for Internet utilities is transmitted on the copper two-core conductors of the analog and digital telephone lines (POTS or ISDN) in the case of ADSL. For this purpose, the spectrum of frequency used by ADSL is divided into several sections. This enables the telephony and data signals to be transported side-by-side between the subscriber's line and the local exchange. There is a splitter on either side to separate and combine the signals. In ADSL, the maximum transmission rate that can be achieved is asymmetric in both directions, upstream and downstream. ADSL supports upstream transmission of up to 1.5 MBit/s and downstream of up to 8 MBit/s. However, as the transmission rate which can be achieved drops significantly the further apart the local exchange and subscriber are, these values cannot be achieved in practice for the majority of lines. The asymmetric DSL variants, in which there is a speed of up to 256 kBit/s available for upstream and up to 3 MBit/s available for downstream, are particularly suitable for private users and small businesses who do not wish to make large volumes of frequently requested Internet content available on their PC for other users.
2	BBAE	Stands for Broadband Access Equipment. The BBAE represents a subscriber's terminal connection to a line that is used for broadband. It separates the provider network from the subscriber line cable and conditions the signals for transmission via the connection element. In the case of ADSL connections, the BBAE generally also features the splitter that separates the broadband and narrow band signals from one another and combines them again.
3	CAPI	Stands for Common Application Programming Interface. A standardized software interface for communication between software and hardware. CAPI is the name of a program which is supplied with an ISDN card and which is used to activate it. Other programs that wish to transmit data via the card only have to pass this data on to the CAPI driver.
4	DSL	Stands for Digital Subscriber Line. DSL technology enables data transmission to be accelerated substantially via conventional phone lines, making it especially suitable for high-speed Internet use. ISDN services or analog telephony continue to run undisrupted on the same line. The high transmission rates are achieved by enlarging the frequency range

		used. For example, ADSL supports transmission rates of up to 8 MBit/s. Lines with capacities of 768 kBit/s are very common. The name DSL represents a whole family of technologies that are combined under the collective term xDSL. In Germany, lines for private customers are mainly offered with asymmetric DSL (ADSL) and single pair DSL (SDSL) technologies. ADSL, which is much more common, transmits the Internet data in the existing telephone network above telephony frequencies between 138 and 1,104 kHz. For example, ADSL is also the basis for the T-DSL product offered by Deutsche Telekom AG.
5	DynDNS	The term DynDNS stands for dynamic DNS and is meant to indicate that you as the customer can enter the IP address belonging to a name in the DNS server yourself. The partner's IP address is contacted, and the connection is established. However, since fixed IP addresses are expensive, most users connect to service providers and are assigned a dynamic IP address. This changes every time you connect (hence the term dynamic), making it impossible to locate a partner with a dynamic IP address. DynDNS servers on the Internet offer assistance in this respect. They enable partners to be located despite their dynamic IP address. If the partner is known, i.e. if its IP address is known, there is nothing to prevent communication. In the interests of security, communication with the partner can be encrypted with the aid of IPSec, for example, in a second step.
6	IPsec (Internet Protocol Security)	IPSec is a protocol that can be used to establish a secure IP connection. A distinction is made between two modes: 1. Tunnel mode The entire IP package is encrypted in this mode. Tunnel mode is primarily used to transmit data between two company locations or between a private PC and a company network (to enable staff to work from home, for example) via the Internet secure from monitoring (VPN). 2. Transport mode Here only the data part is encrypted. This is used to transmit critical data, e.g. in passwords.
7	ISDN	Stands for Integrated Services Digital Network. The striking feature of ISDN phone lines is that there are at least two basic access channels (B-channels) available for use simultaneously. This means that a subscriber is contactable by phone whenever it is online or sending a fax. It also supports two parallel phone calls from one line. In addition, higher transmission rates are possible than with an analog line. Each B-channel can transmit 64 kBit/s, i.e. the two together support 128 kBit/s. ISDN digital transmission and switching technology supports diverse forms of communication on the phone line such as telephony, faxing

		or Internet connections. ISDN continues to use the cabling from the previous analog telephone network in order to connect the customers to the exchange. However, ISDN technology uses this with much greater efficiency and flexibility. Connections can be established more quickly, speech quality is much improved, and not only is data transmission is quicker, it is also extremely reliable thanks to error correction.
8	NTBA	Stands for Network Termination Basic Rate Access. The NTBA forms the network termination to the public ISDN network. It converts the signal from the network provider from its two-wire line (UK0 bus) to a four-wire line (S0 bus). The exchange supplies current to the NTBA via the ISDN supply voltage – the NTBA, in turn, supplies the S0 bus. In normal operating mode, power is also fed to the NTBA via a power supply unit. In this mode it can supply up to four terminals which are connected to the S0 bus and which do not possess a power supply of their own. If the NTBA is operated without an additional power supply unit or if the power supply fails, the NTBA uses the network provider's ISDN supply voltage in order to operate on standby.
9	Port Forwarding	Port forwarding is a technology which supports the mapping of ports to IP addresses in NAT networks (Network Address Translation), i.e. if router ports have to be forwarded permanently to a specific IP address. This mapping technology is a function offered by many of the current DSL routers. For this purpose, the advanced settings for the router generally include a table in which a port that has to be mapped is permanently allocated to a specific local IP address.
10	Routers	Routers are first and foremost hardware devices or software programs that can be used to connect one or more computers or whole networks to other networks. The router acts as the control center in order to forward connection requests to the required network or the service. In addition to their basic functionality, hardware routers and, in particular, the current ISDN or DSL routers possess DHCP services or servers which can be used to manage address allocation and control centrally. Depending on the settings, IP addresses can be supplied in this way to whole networks, which is beneficial to inexperienced users, in particular.
11	Splitters	Splitters In ADSL lines, the splitter divides the incoming signal from the provider network into the broadband ADSL signal and the narrow band ISDN signal or analog telephone signal. For transmission in the opposite direction, the two parts of the signal are combined to facilitate simultaneous transmission via the subscriber line. The splitter is frequently contained directly in the broadband access equipment (BBAE).

12	TCP	TCP, which stands for Transmission Control Protocol, is an important component of the TCP/IP protocol. It is based on connections and requests receipt of confirmation for every package sent.
13	TCP/IP	TCP/IP stands for Transmission Control Protocol/Internet Protocol. This generally refers to the whole family of protocols. It was developed to facilitate connection between computers in different networks. Nowadays TCP/IP is used in many LANs (Local Area Networks) and is the basis for the world wide web.
14	T-DSL	Deutsche Telekom has been offering DSL lines under the name T-DSL since the late 90s. T-DSL is the most commonly used variant of DSL, which also makes it the most common type of broadband Internet access in Germany. Deutsche Telekom is not the only organization which offers T-DSL access to the Internet via its subsidiary T-Online, this is also available from a relatively large number of resellers. However, they all use Deutsche Telekom infrastructure to establish the physical link to the customer. The remaining providers primarily use their own versions of ADSL or else SDSL, although this works symmetrically and supports data rates of up to 2.3 MBit/s.
15	VPN (Virtual Private Network)	Company employees can use a Virtual Private Network (VPN) to connect to the company network (Intranet) from home or from locations outside the company via the Internet. A number of company sites can also be linked this way. The advantage of this is that there is no need for modem links or leased channels, simply a connection to the Internet. The employee connects to the Internet first of all. An encrypted channel (tunnel) is then established between the VPN client and VPN server. Following authentication via user name and password, token card or public key/certificate, an encrypted IPSec tunnel is set up via which data can be transmitted without risk of being monitored.
16	WAN	The term WAN (Wide Area Network) refers to networks which transmit data over a larger distance than a LAN (Local Area Network).

5 Warranty and Support

No liability is accepted for the foregoing or following internal Siemens information.

A&D accepts no liability, regardless of the legal grounds, for damages arising from the use of the examples, tips, programs, configuration and performance data, etc. described in Expert Communications, apart from the statutory liability accepted, for example, for damage to items used for personal purposes, personal accidents or for malicious intent or gross negligence.