SIEMENS

# Fernwartung mit WinCC flexible
# Kommunikation via Wide Area Network (WAN)

**Basiswissen** **Ausgabe 12/04**

## Vorwort

In dieser Dokumentation finden Sie eine Einführung zu den folgenden Sm@rt – Optionen von WinCC flexible:

- Sm@rtAccess
  - Verteilte Bedienplätze mit Sm@rtClients
    Bedienung an einer räumlich ausgedehnten Maschine
  - Anlagenweiter Zugriff auf Variablen über HTTP
    Lesender und schreibender Zugriff auf Variablen
  - Anbindung von Panels an die Office-Welt
    Lesender und schreibender Zugriff auf Variablen
- Sm@rtService:
  - E-Mail Support
    Versand von E-Mails auf Basis von Meldungen und Ereignissen
  - Wartungsfunktionen über WEB
    Standard-HTML-Seiten mit Service- und Wartungs-Funktionen sowie Diagnoseinformationen
  - Fernbedienung über WEB
    Mit Hilfe des Internet Explorers ein HMI-System vollständig fernsteuern

**Haftung**

Eine Haftung der Siemens AG, gleich aus welchem Rechtsgrund, für durch die Verwendung des vorliegenden Beitrags verursachte Schäden ist ausgeschlossen, soweit nicht z.B. bei Schäden an privat genutzten Sachen, Personenschäden oder wegen Vorsatzes oder grober Fahrlässigkeit zwingend gehaftet wird.

**Gewährleistung**

Bei den Beiträgen handelt es sich um ausgewählte Lösungsvorschläge zu Anfragen mit komplexen Aufgaben, die im Customer Support erarbeitet wurden. Wir weisen außerdem darauf hin, dass es nach dem Stand der Technik nicht möglich ist, Fehler in Softwareprogrammen unter allen Anwendungsbedingungen auszuschließen. Die Beiträge wurden nach bestem Wissen erstellt. Eine Haftung die über die übliche Gewährleistung für Software der Klasse C entsprechend unseren "Allgemeinen Bedingungen für die Überlassung von Softwareprodukten für Automatisierungs- und Antriebstechnik" hinaus geht, können wir jedoch nicht übernehmen. Die Programme werden im Internet als Einzellizenzen angeboten. Eine Weitergabe an Dritte ist nicht gestattet.

# Inhaltsverzeichnis

# 1 Einleitung

Mit WinCC flexible und der Option Sm@rtService, haben Sie die Möglichkeit, direkt von Ihrem Service / Wartungs- Arbeitsplatz aus, sich über das Internet mit einem Bediengerät zu verbinden.

Der zuständige Servicetechniker kann sich somit remote mit dem Bediengerät verbinden und sich dessen Bedienoberfläche direkt an seinem Service / Wartungs- Arbeitsplatz anzeigen lassen und so den laufenden Prozess beobachten. Aktualisierte WinCC flexible Projekte können auf diese Weise schneller transferiert werden.

Den Remote Zugriff können Sie für folgende Anwendungen nutzen:

- Remote administrieren
  Sie können ein Projekt vom Arbeitsplatz aus auf ein Bediengerät transferieren. Damit können Sie WinCC flexible Projekte an zentraler Stelle aktualisieren.
- Remote diagnostizieren
  Jedes Panel stellt HTML-Seiten zur Verfügung, auf denen Sie z.B. die installierte Software, Version oder Systemmeldungen mit einem Web-Browser abrufen können.
- Remote bedienen und beobachten
  Sie können ein Bediengerät von Ihrem Arbeitsplatz aus bedienen und den laufenden Prozess beobachten.



Mit der Option Sm@rtAccess können zwei HMI-Systeme miteinander kommunizieren.

- Verteilte Bedienplätze mit Sm@rtClients
  Bedienung an einer räumlich ausgedehnten Maschine
- Anlagenweiter Zugriff auf Variablen über HTTP
  Lesender und schreibender Zugriff auf Variablen
- Anbindung von Panels an die Office-Welt
  Lesender und schreibender Zugriff auf Variablen

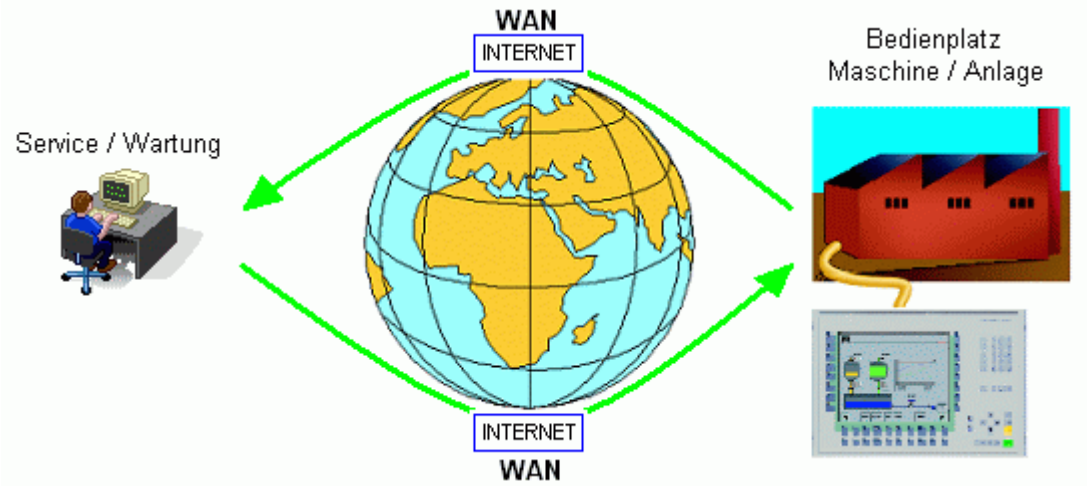
Detaillierte Informationen zu Sm@rtService und Sm@rtAccess sowie ein Anwendungsbeispiel zu diesem Thema finden Sie im Handbuch:

WinCC flexible 2004, Getting Started Optionen

**Beitrags ID: 18657078**

# 2 Automatisierungsaufgabe

Abbildung 2-1




## 2.1 Typische Beispiele

**Fall 1:**

Sie betreuen eine Kundenanlage im Ausland. In Ihrer Firma entwickeln Sie für Ihren Kunden neue Prozessabläufe. Die Rezepturdaten müssen darauf hin beim Kunden „vor-Ort“ abgeändert und die Bedienoberfläche an die neuen Prozessabläufe angepasst werden. Diese Änderung soll im laufenden Betrieb beim Kunden ohne größere Unterbrechung vorgenommen werden.

**Fall 2:**

Sie betreuen eine Kundenanlage. Der Kunde hat Schwierigkeiten mit dieser Anlage. Das Problem lässt sich am Telefon nicht klären. Sie müssen sich die Anlagenwerte „online“ anschauen.

**Fall 3:**

Es soll von einem Zentralen Standort (Warte) aus eine Fernbedienung und -beobachtung von anderen SIMATIC HMI-Systemen ermöglicht werden sowie ein Anlagenweiter Abruf von Informationen und Archivierung von Prozessdaten möglich sein.

## 2.2 Lösungsmöglichkeit

In den unter Punkt 2.1 beschriebenen Fällen 1 und 2, können Sie nun folgendes durchführen.

- Sie fahren zum Kunden und führen die Änderungen „vor Ort“ durch.
- Sie Verbinden sich von Ihrem Service / Wartungs-Arbeitsplatz aus, direkt über eine Internetverbindung, mit dem HMI Bediengerät des Kunden. (Sm@rt Service)

In dem unter Punkt 2.1 beschriebenen Fall 3, können Sie nun folgendes durchführen.

- Mit Sm@rtAccess ist es z.B. möglich, von zentraler Stelle aus (HMI-System als Kopfstation) auf die Prozesswerte der Maschine zuzugreifen und Informationen abzurufen. Prozesswerte können somit z.B. zentral archiviert bzw. ausgewertet werden, ohne direkt vor Ort zu sein.
  Für einen Zugriff auf die Prozesswerte greift die Kopfstation (z. B. PC mit WinCC flexible Runtime) greift dann über das SIMATIC HMI http Protocol auf die Variablen des entfernt liegenden Bediengerätes zu.



## 2.3 Voraussetzung

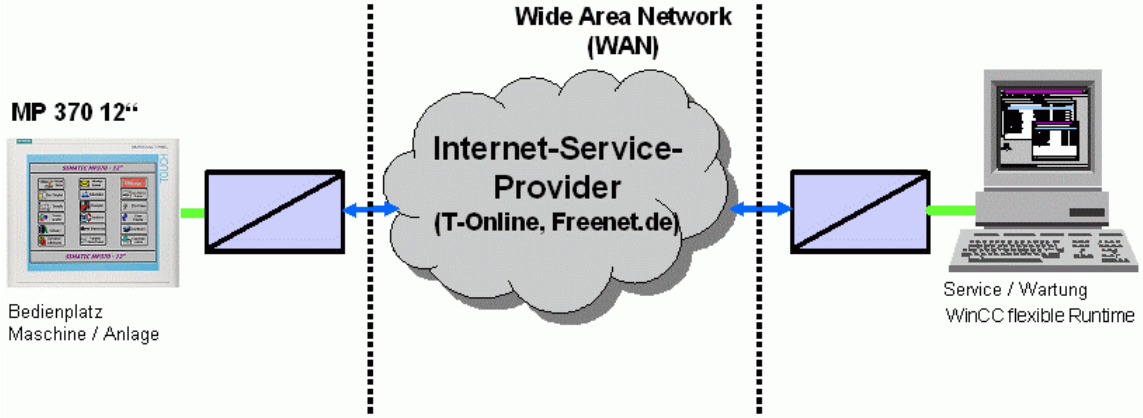
- HMI Bediengeräte ab der 270-Serie mit Ethernet Schnittstelle
- HMI Bediengerät auf Basis WinCC flexible
- HMI Bediengerät mit der Option Sm@rtService bzw. Sm@rtAccess

**Hinweis:**

- Ein SIMATIC Panel kann an ein WAN nur über Ethernet mittels eines Netzzugangsgerät (Router) angeschlossen werden. Der Router stellt die Verbindung zum Internet-Service-Provider (ISP) her.

# 3 Vernetzung über WAN

Abbildung 3-1



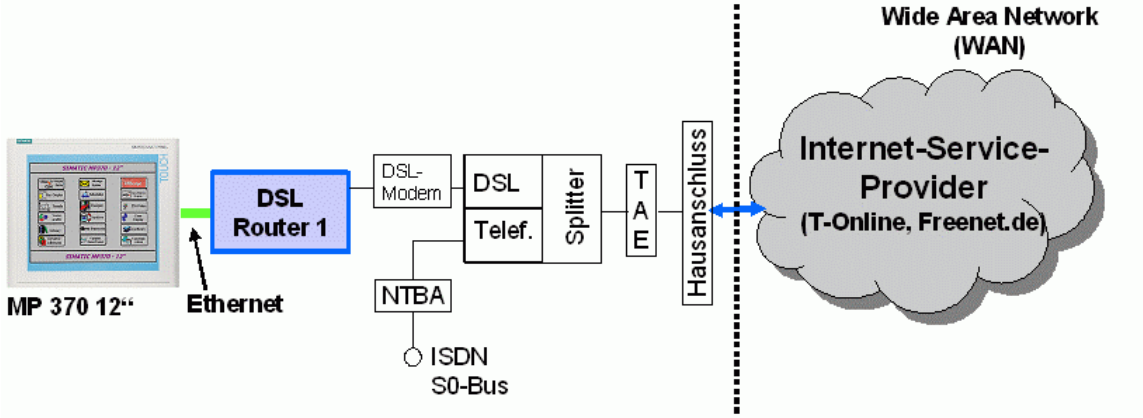



Aus dieser Aufgabenstellung ergeben sich folgende Fragen:

- Wie kann ich das Panel an das WAN (Wide Area Network) anbinden?
- Welche Hardwarekomponenten sind notwendig?
- Welche IP-Adresse hat das zu erreichende Panel?
- Wie sicher ist die Verbindung?
- Welche Einstellungen sind vorzunehmen?

## 3.1 Wie kann ich das Panel an das WAN anbinden?

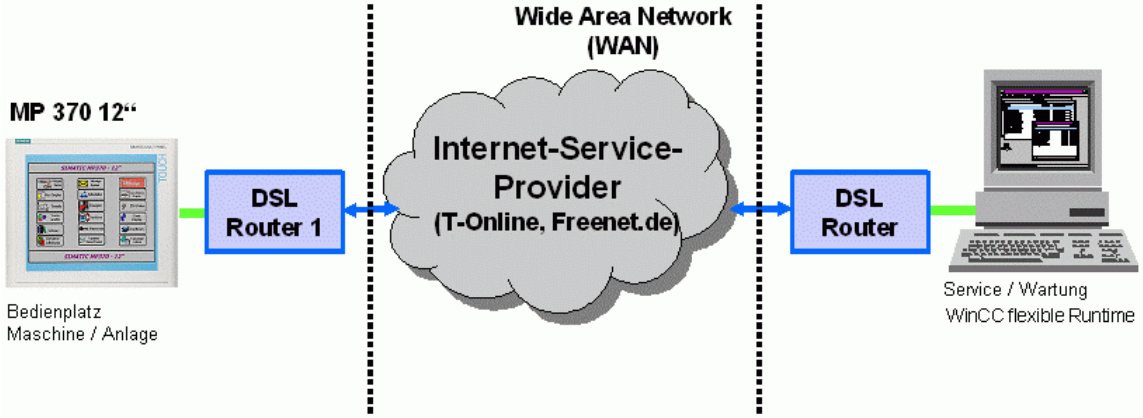
Abbildung 3-2




Ein SIMATIC Panel kann nur über Ethernet an ein Netzzugangsgerät angeschlossen werden, das eine Verbindung zum Internet-Service-Provider (ISP) aufbauen kann.
Dies ist in aller Regel ein PC oder kostengünstiger ein Router.

## 3.2 Welche Hardwarekomponenten sind notwendig?

Abbildung 3-3

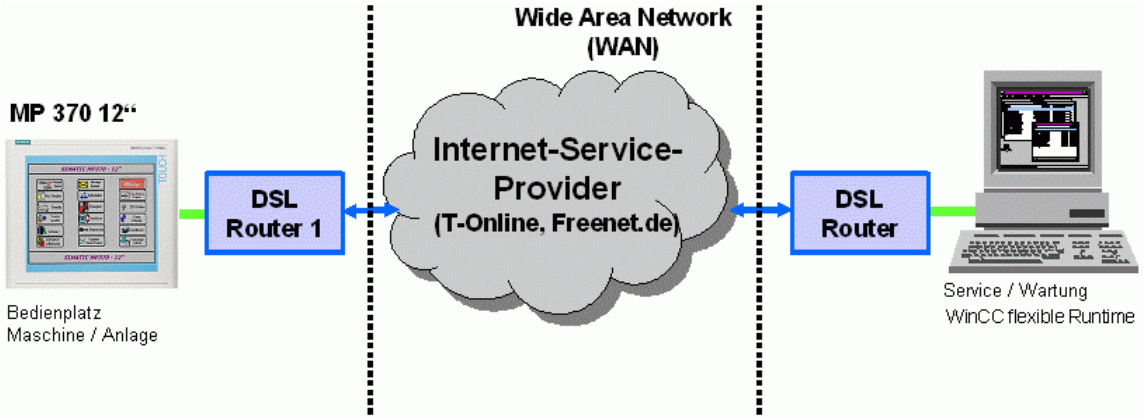



Für die Anbindung eines SIMATIC Panels ab der 270-Serie ist ein Router oder ein PC mit Netzzugang erforderlich.

Router werden mit Analog- (eher selten), ISDN oder DSL-Netzzugang angeboten. Router bieten für die Realisierung eines LANs mehrere Ethernet Ports (RJ45).

## 3.3 Welche IP-Adresse hat das zu erreichende Panel?

Abbildung 3-4

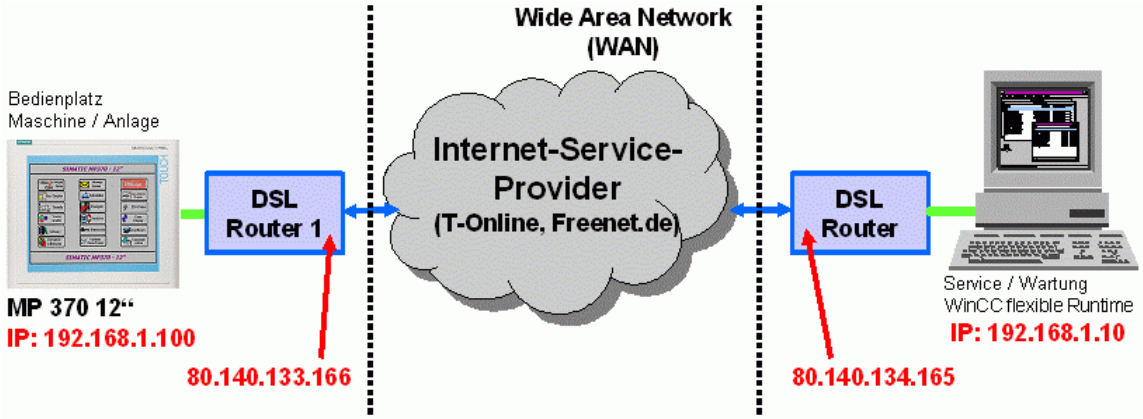



Man unterscheidet zwischen zwei Verbindungen:

- Einsatz einer statischen Verbindung
  - Die IP-Adresse wird vom Internet Service Provider (ISP) bekannt gegeben. Die IP-Adresse ist statisch, dies bedeutet, dass sich diese nach Ab- und Wiederaufbau einer Sitzung nicht ändert.
- Einsatz einer dynamischen Verbindung
  - Die IP-Adresse wird vom ISP (Internet Service Provider) dynamisch vergeben. Dies bedeutet, dass sich diese von einer zur nächsten Sitzung ändert.

## 3.4 Einsatz einer statischen Verbindung:

Abbildung 3-5



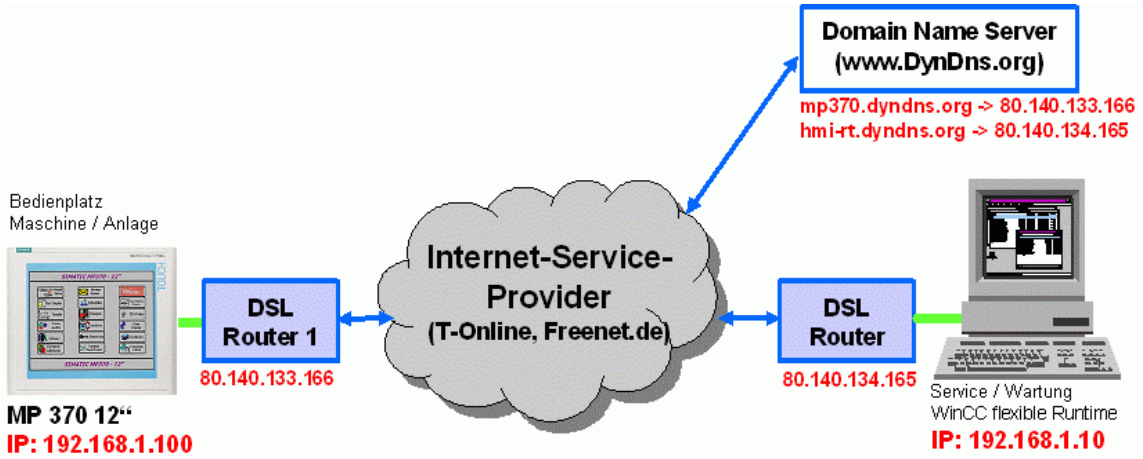



Einsatz einer statischen Verbindung:

Die IP-Adresse wird vom Internet Service Provider (ISP) bekannt gegeben z.B. 80.140.133.166
Dies ist die Adresse des Netzzugangsgerätes, das die Verbindung zum ISP über das WAN aufgebaut hat. In Verbindung mit einem SIMATIC Panel ab der 270-Serie, ist ein Router oder ein PC einzusetzen.
Der Router 1 in dem obigen Beispiel setzt die Anfrage der Gegenseite auf die Lokale IP (TCP port number) des Panels (z.B. 192.168.1.100) um.

## 3.5 Einsatz einer dynamischen Verbindung:

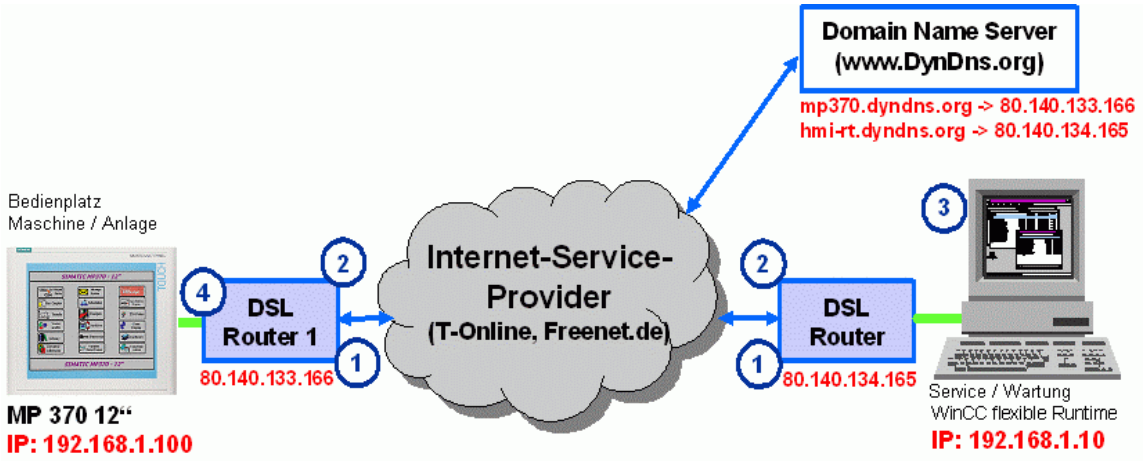
Abbildung 3-6




Einsatz einer dynamischen Verbindung:

Die IP-Adresse eines Netzteilnehmers wird vom ISP dynamisch nach Verbindungsaufbau vergeben. Dies bedeutet, dass die Adresse von einer zur nächsten Sitzung sich ändert.
Dieser Zustand ist für die Verbindung von mehreren Maschinen/Anlagen über das WAN nicht sinnvoll. Damit der Prozess der Adressbestimmung automatisiert werden kann, sind „Domain Name Server" (DNS) einzusetzen.

Abbildung 3-7






Einsatz einer dynamischen Verbindung:

1. Die DSL-Router bauen eine Verbindung zum ISP auf
   und erhalten eine dyn. IP-Adresse

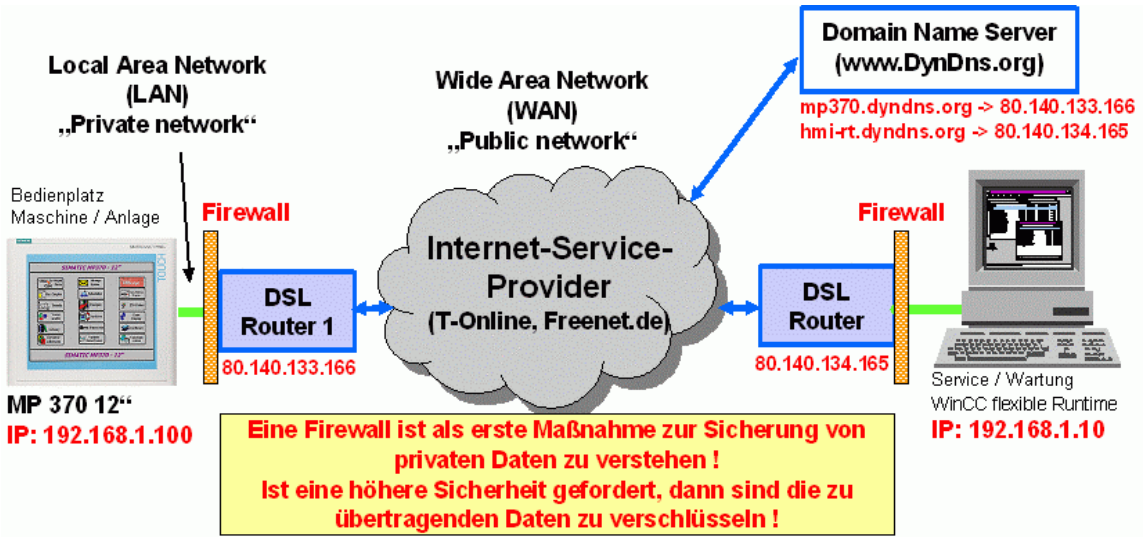
2. Die DSL-Router melden ihre IP-Adresse an einen DNS-Server

3. HMI-RT ruft Verbindung über DNS auf – z.B. mp370.dyndns.org
   Der DNS-Server routet die Anfrage auf die IP „80.140.133.166"

4. Der Router 1 setzt die Anfrage der HMI-RT auf die lokale
   IP-Adresse (TCP port number) des Panels um (z.B. 192.168.1.100)

## 3.6 Wie sicher ist die Verbindung?

Abbildung 3-8

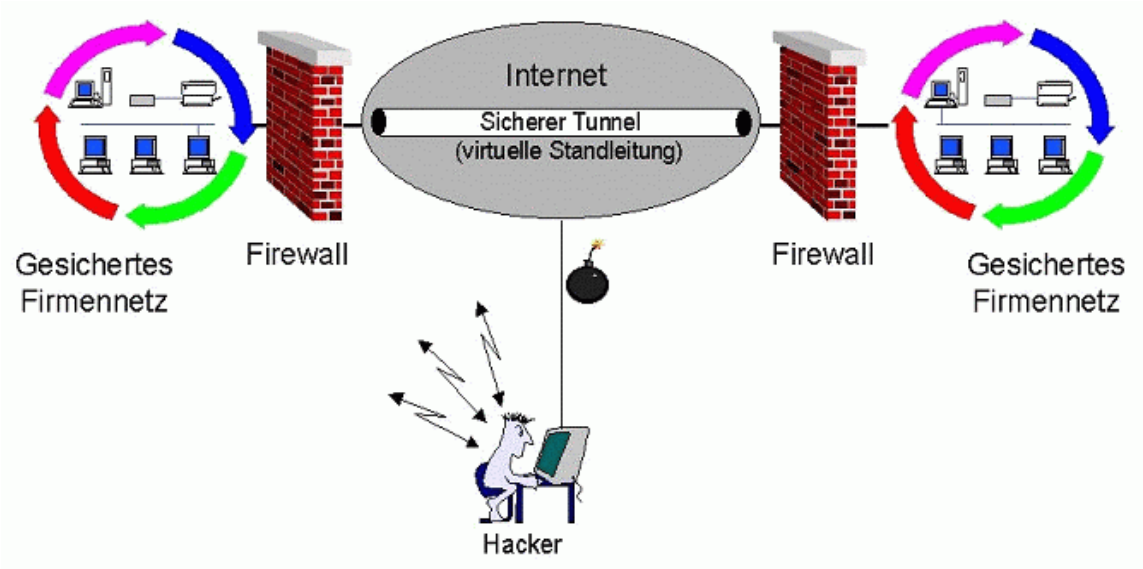



Die oben aufgeführte lokalen Netze sind mit Hilfe einer optional einzusetzenden Firewall gesichert. Die Firewall basiert in diesem Beispiel auf einer Kombination aus Hardware und Softwarelösung und ist in dem Router integriert.
Folgende Techniken werden von der Firewall typ. angewandt:
Packet filter, Application gateway, Circuite level gateway, Proxy server, Virtual Server, …

## 3.7 Virtual Private Networks - VPN

**Erhöhte Sicherheit durch Virtual Private Networks (VPN)**

Abbildung 3-9



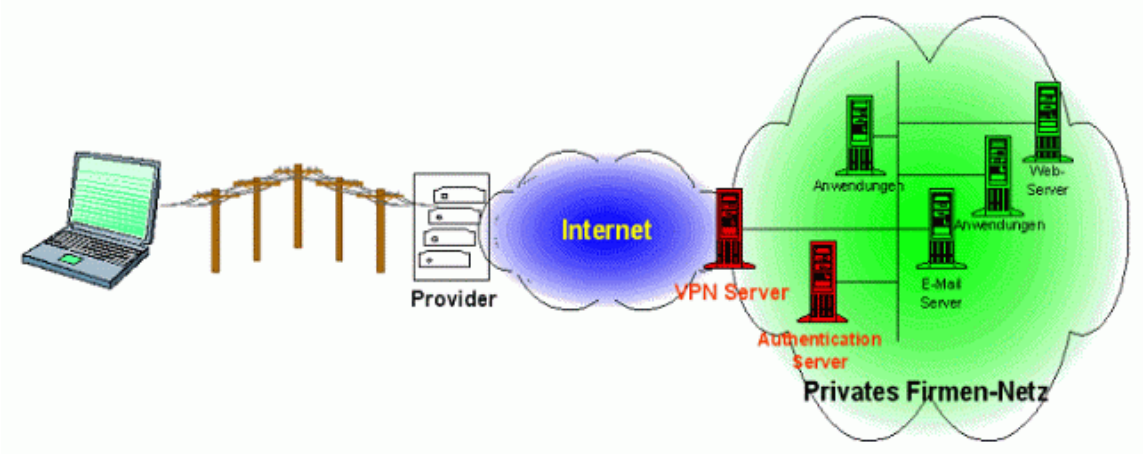



Erhöhte Sicherheit durch Virtual Private Networks (VPN):

Statt der Nutzung teurer Modemstrecken oder angemieteter Kanäle, setzt die VPN-Technik das Internet als "Trägermedium" ein.
Durch den Einsatz eines VPN ist es möglich, dass sich ein Dienstreisender (aber auch ein Mitarbeiter im Home Office) unter Nutzung des Internets in sein Firmennetzwerk einwählt. Ein VPN ist hier(mit) die günstige Alternative zu klassischen Dial-In-/ Remote Access-Lösungen.
Darüber hinaus können VPN aber auch zur Kopplung zweier Unternehmensstandorte (anstelle der von Standleitungen) eingesetzt werden (sog. Site To Site oder Branch To Branch Verbindung).

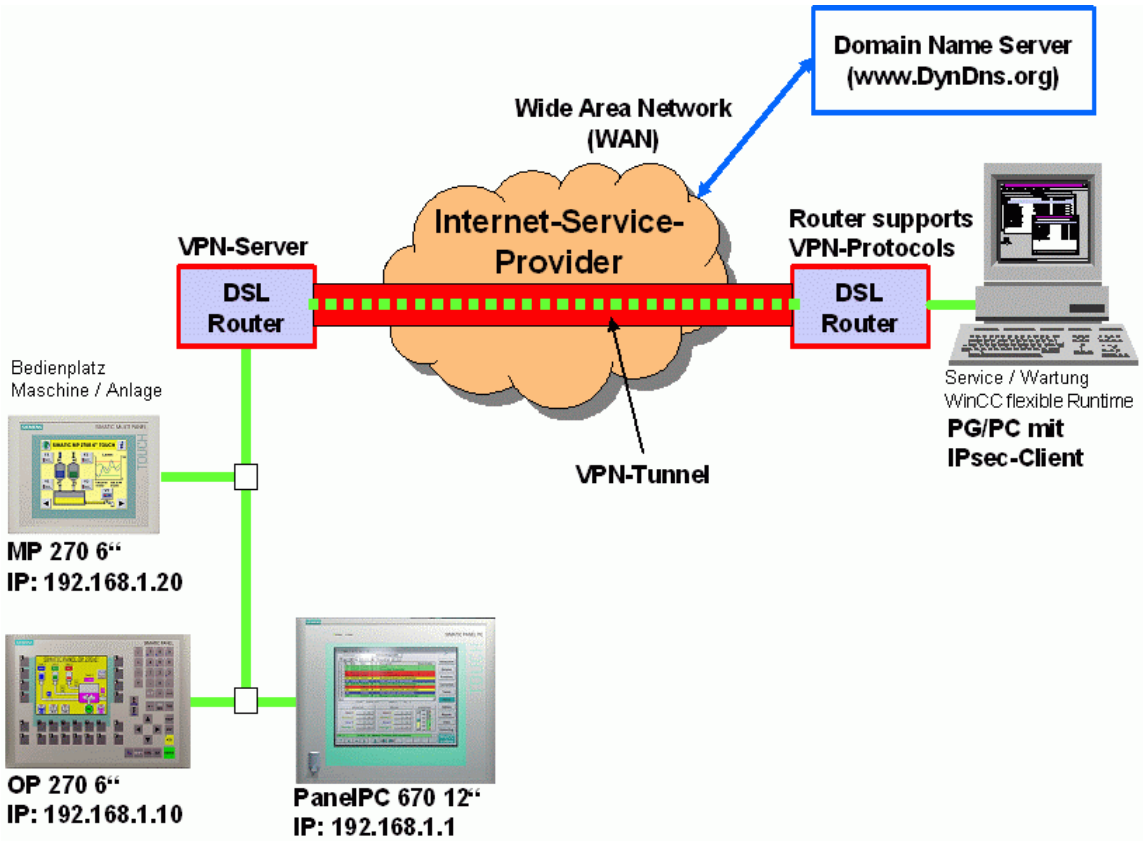
### 3.7.1 Verbindung über VPN-Tunnel (IPsec)

Abbildung 3-10




Übersichtsbild 2:

Abbildung 3-11



### 3.7.2 Vorteile von VPN-Netzwerkverbindungen im Überblick

- Virtuell
- Kostenersparnis
- Verbesserte Sicherheit
- Einfache Erweiterung von Netzwerken
- Geschwindigkeit der Implementierung
- Private IP-Adressen können im VPN weiterverwendet werden
- Integrität / Authentizität
- Verschlüsselung
- Internet Protocol Security (IPsec)



### 3.7.3 Einige Links zum Thema „VPN“ …

**Englischsprachige Inhalte**

- 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

**Deutschsprachige Inhalte**

- 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 Ergänzende Hinweise zu VPN (Virtuel Privat Network)

- **Kostenersparnis:**

Kostenersparnis ist ein wichtiger Faktor für Unternehmen, die sich in der heutigen Wirtschaftslage für den Einsatz von IP-VPNs entscheiden. Früher wurden die Standorte über eine dedizierte Standleitung oder einen PVC (Private Virtual Circuit) miteinander verbunden. IP-Netzwerke bieten den Zugriff auf das gesamte IP-Netzwerk zum Preis für nur einen Standort. Dank der gemeinsamen Infrastruktur fallen außerdem geringere Gebühren für die Konnektivität an. Mobile Benutzer und Remotebenutzer können sich bei einem IP-Netzwerk über private DFÜ-Netzwerke einwählen.

Ganz allgemein ist ein VPN ein Netzwerk, das auf einem anderen, meist öffentlichen, implementiert wird. Dieses Tunneln von 'privatem' Netzwerk durch öffentliche Netzwerke ist das Grundkonzept eines VPN. Warum sollte man nun so etwas tun? Die Erhöhung von Komplexität im eigenen Netzwerk ist nur in den seltensten Fällen erstrebenswert. Grundsätzlich ist ein VPN in all den Anwendungsfällen geeignet, in denen man Standleitungen (DDV, ISDN) oder Public-Shared Networks wie z.B. Datex-P, Frame Relay oder auch ATM einsetzt.

Die geringen Kosten kann jeder nachvollziehen, der ein klassisches WAN aufbauen musste. Die Summe aus DDVs (local loops) und WAN-Gebühren können recht beträchtliche Kosten verursachen.

Die zweite Herausforderung des klassischen Corporate Network ist die beachtliche Komplexität an Routern und Datenanbindungen. Diese kann, besonders wenn aufgrund regionaler Gegebenheiten mehr als ein Provider angebunden werden muss, leicht an die Grenzen der Beherrschbarkeit führen.

- **Virtuell:**

Eigentlich bedeutet der Begriff 'Virtuell' in VPN nichts Neues. Wenn Sie sich Datex-P, Frame Relay und ATM, ja selbst das Telefonnetz anschauen, sind das eigentlich virtuelle Netzwerke. Wenn Sie jemanden anrufen, dann verhält sich das so, als ob Sie einen direkten Draht von Ohr zu Ohr gelegt hätten. Das ist aber schlicht falsch. Tausende Telefonate werden zeitgleich über dieselbe Glasfaser geroutet. Der Draht zwischen Ihnen und unserem Gegenüber ist virtuell. Dasselbe gilt für Datex, Frame Relay und ATM.

- **Verbesserte Sicherheit:**

Bei VPN wird der Datenverkehr durch Verschlüsselung getrennt. Dadurch sind Ihre Daten vor dem unberechtigten Zugriff Dritter geschützt. Im Gegensatz zu einem VPN können bei einem Netzwerk, das auf einer privaten Standleitung basiert, derartige Übergriffe nur sehr schwer entdeckt, geschweige denn verhindert werden.

- **Einfache Erweiterung von privaten Netzwerken auf Remotestandorte:**

Für Unternehmen, die an entlegenen Orten außerhalb einer Metropole operieren, ist die Installation und der Einsatz eines privaten Netzwerks oft zu teuer. Ein VPN in einer gemischten Netzwerkumgebung ist bei einem begrenzten Budget in der Regel die einzige Alternative, um die Dienste zur Verfügung stellen zu können.

- **Geschwindigkeit der Implementierung:**

Im Gegensatz zur Einrichtung eines eigenen WAN ist bei der Implemtierung eines IP-VPN der Großteil der Infrastruktur bereits vorhanden. Dies ermöglicht eine schnelle Einrichtung und flexible Entwicklung.

- **Integrität / Authentizität:**

Eng verbunden mit der Privatheit der Kommunikation ist ihre Authentizität. Kommunikation nicht trivialer Inhalte erfordert die Sicherheit, dass der Sender der Nachricht auch derjenige ist, für den er sich ausgibt. Genauso ist die Integrität der Botschaften zu sichern. Die Botschaft muss das enthalten, was der Sender gesendet hat. In ungesicherte, oder auch zu schwach gesicherte Netzwerke können Dritte vermeintlich authentische Botschaften einspeisen, welche durchaus Schaden verursachen können. Oder aber originale Botschaften ändern.

- **Verschlüsselung:**

Da in einem globalen Umfeld niemand die physikalische Kontrolle über das gesamte Netzwerk besitzt, ist die gesamte WAN-Infrastruktur mehr oder minder als öffentlich zu betrachten. Da eine physikalische Kontrolle nicht gegeben ist, bietet sich die Kryptologie als Kontrollinstanz der virtuellen Welt an. Ein verschlüsseltes VPN – und wenn heutzutage über VPNs geredet wird, setzt man eine Verschlüsselung implizit voraus – eröffnet die Chance auf private, authentische und integere Kommunikation.

Die Betonung liegt auf Chance, denn ebenso wie physikalische Kontrolle häufig unbefriedigend erfolgt, geschieht dies auch in der virtuellen Welt. Nur können Sie in der realen Welt den defekten Zaun auch als Laie erkennen, in der virtuellen Welt hat da selbst der Experte oft Mühe. Selbst große Namen in der IT-Branche bieten keinerlei Gewähr für lückenlose Sicherheit. Von Scientologen als Zulieferanten und NSA-Schlüsseln im Kryptomodul, bis zu schlichten Designfehlern reicht hier das Spektrum.

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

Der De-facto-Standard für VPN-Software ist gegenwärtig IPSEC. Dieser offene Standard, umfasst drei Protokolle, welche in einer IPSEC-Implementierung genutzt werden (können):

- ESP, Encapsulating Security Payload, verschlüsselt und beglaubigt Daten.
- AH, Authentication Header, stellt einen Paket-Beglaubigungsdienst.
- IKE, Internet Key Exchange, handelt Verbindungsparameter, einschließlich der Schlüssel für die ersten beiden Protokolle aus.

Diese Protokolle implementieren die Verbindungssicherheit und stützen sich selbst auf eine Vielzahl von Verschlüsselungsprotokollen, u.a. auf

- DES, Data Encryption Standard, veraltet, wird aus Sicherheitsgründen von einigen Implementierungen nicht unterstützt
- triple DES
- AES, oder Rijndael Advanced Encryption Standard, DES-Nachfolger
- RSA, patentierter Public Key Algorithmus. Patentschutz ist abgelaufen
- MD5, Message Digest Algorithm
- SHA, the Secure Hash Algorithm
- Diffie-Hellman-Schlüsselaustauschprotokoll

IPSEC wird von einer Reihe von Anbietern implementiert, auf Routern, Firewalls und als Software auf Servern und Desktops. Seine Stärke ist die Quelloffenheit der eingesetzten Protokolle, sogar quelloffene Implementierungen sind verfügbar.

### 3.7.5 Welche Einstellungen sind vorzunehmen?

**Freizuschaltene Ports einer Firewall**

**Sm@rtServer:**

| | |
|---|---|
| HTTP-Zugang: | Port 5800 (laden des Java-Applets) |
| Main: | Port 5900 |

**Web-Server:**

| | |
|---|---|
| HTTP | Port 80 |
| HTTPS | Port 443 (SSL) |

| | |
|---|---|
| Ethernet Transfer | Port 2308 und 50523 |
| VPN (IPsec): | Port 500 (Internet Key Exchange Protocol IKE) |
| E-Mail (SMTP-Server): | Port 25 |

# 4 Glossar

Tabelle 4-1

| Nr. | Abkürzung | Beschreibung |
|---|---|---|
| 1 | ADSL | Abkürzung für Asymmetric Digital Subscriber Line (dt. Asymmetrische digitale Teilnehmeranschlussleitung).<br>ADSL ermöglicht die Nutzung der Infrastruktur des vorhandenen Telefonnetzes für Breitbanddienste. Auf den Kupferdoppeladern der analogen und digitalen Telefonanschlüsse (POTS bzw. ISDN) werden bei ADSL zusätzlich Daten für Internetdienste übertragen. Dazu wird das von ADSL genutzte Frequenzspektrum in mehrere Bereiche aufgeteilt. Zwischen dem Teilnehmeranschluss und der Ortsvermittlungsstelle können die Telefonie- und Datensignale so problemlos nebeneinander transportiert werden. Für die Trennung bzw. Zusammenführung der Signale sorgt auf beiden Seiten ein Splitter.<br>Asymmetrisch ist bei ADSL die maximal erreichbare Übertragungsrate in beide Richtungen - Upstream und Downstream. Für den Upstream stehen bei ADSL maximal 1,5 MBit/s zur Verfügung und für den Downstream 8 MBit/s. Da die erreichbare Übertragungsrate mit steigender Entfernung zwischen Ortsvermittlungsstelle und Teilnehmer jedoch deutlich abnimmt, sind diese Werte für die überwiegende Anzahl der Anschlüsse in der Praxis nicht zu erreichen.<br>Die asymmetrischen DSL-Varianten, bei denen für den Upstream bis zu 256 kBit/s und für den Downstream bis zu 3 MBit/s zur Verfügung stehen, eignen sich vor allem für private Nutzer und kleinere Unternehmen, die auf ihrem PC keine aufwendigen und häufig angeforderten Internetinhalte für andere Nutzer zur Verfügung stellen wollen. |
| 2 | BBAE | Abkürzung für Breitband-Anschlusseinheit (engl. Broadband Access Equipment).<br>Der BBAE bildet auf der Seite des Teilnehmeranschlusses den physikalischen Abschluss einer breitbandig genutzten Anschlussleitung. Er trennt das Anbieternetz von der Anschlussverkabelung beim Teilnehmer und bereitet die Signale für die Übermittlung über den jeweiligen Verbindungsabschnitt auf.<br>Bei ADSL-Anschlüssen beinhaltet der BBAE meist auch den Splitter, der das Breitband- und Schmalbandsignal voneinander trennt bzw. wieder zusammenführt |
| 3 | CAPI | Common Application Programming Interface.<br>Normierte Software-Schnittstelle für die Kommunikation zwischen Soft- und Hardware.<br>Mit CAPI wird ein Programm bezeichnet, das mit einer ISDN-Karte geliefert wird und deren Ansteuerung übernimmt. Andere Programme, die über die Karte Daten übertragen wollen, müssen diese Daten nur an den CAPI-Treiber übergeben. |

| | | |
|---|---|---|
| 4 | DSL | Abkürzung für Digital Subscriber Line<br>(dt. digitale Teilnehmeranschlussleitung)<br>Die DSL-Technik ermöglicht es, über herkömmliche Telefonleitungen die Datenübertragung wesentlich zu beschleunigen und bietet sich somit vor allem für die schnelle Internetnutzung an. ISDN-Dienste oder analoge Telefonie laufen dabei ungestört auf der gleichen Leitung weiter. Die hohen Übertragungsraten werden erreicht, indem man den verwendeten Frequenzbereich vergrößert. So ermöglicht ADSL Übertragungsraten von bis zu 8 MBit/s. Sehr verbreitet sind Anschlüsse mit 768 kBit/s.<br>Hinter der Bezeichnung DSL verbirgt sich eine ganze Familie von Technologien, die unter dem Sammelbegriff xDSL zusammengefasst wird. In Deutschland werden Anschlüsse für Privatkunden vor allem mit den Technologien Asymmetric DSL (ADSL) und Single Pair DSL (SDSL) angeboten. Das wesentlich verbreitetere ADSL überträgt die Internetdaten im vorhandenen Telefonnetz oberhalb der Telefoniefrequenzen zwischen 138 und 1.104 kHz. ADSL ist beispielsweise auch die Basis für das T-DSL-Angebot der Deutschen Telekom AG. |
| 5 | DynDNS | Der Begriff DynDNS steht für dynamisches DNS und soll darauf hindeuten, dass Sie als Kunde die zu einem Namen gehörige IP-Adresse selbst im DNS-Server eintragen können<br>Man kontaktiert die IP Adresse des Partners und die Verbindung steht. Da feste IP Adressen aber teuer sind, wählen sich die meisten Benutzer bei Diensteanbietern ein und bekommen eine dynamische IP Adresse zugewiesen.<br>Diese wechselt bei jeder Einwahl (daher der Ausdruck dynamisch), so dass das Auffinden eines Partnern mit dynamischer IP Adresse unmöglich ist. Hier bieten DynDNS Server im Internet Abhilfe. Sie ermöglichen das Auffinden von Partnern trotz dynamischer IP Adresse. Ist der Partner bekannt, d.h. ist seine IP Adresse bekannt, steht einer Kommunikation nichts mehr im Wege. Zur Sicherheit kann in einem zweiten Schritt die Kommunikation mit dem Partner mit Hilfe von z.B. IPSec verschlüsselt werden. |
| 6 | IPsec<br>(Internet Protocol Security) | IPSec ist ein Protokoll, das zum Aufbau einer sicheren IP-Verbindung verwendet werden kann.<br>Man unterscheidet zwei Betriebsarten:<br>1. Der Tunnelmodus<br>Bei dieser Betriebsart wird das ganze IP-Paket verschlüsselt. Der Tunnelmodus wird v.a. zur abhörsicheren Übertragung von Daten zwischen zwei Firmenstandorten oder zwischen einem privaten Computer und einem Firmennetzwerk (z.B. bei Arbeiten von Zuhause) über das Internet verwendet (VPN).<br>2. Der Transportmodus<br>Hierbei wird ausschließlich der Datenteil verschlüsselt. Dies wird für die Übertragung von kritischen Daten verwendet, z.B. bei Passwörtern |

| | | |
|---|---|---|
| 7 | ISDN | Abkürzung für Integrated Services Digital Network (dt. Dienste integrierendes digitales Fernmeldenetz)<br>Hervorstechendes Merkmal von ISDN-Telefonanschlüssen ist die Verfügbarkeit von mindestens zwei gleichzeitig nutzbaren Basiskanälen (B-Kanäle). Dadurch bleibt ein Teilnehmer auch dann telefonisch erreichbar, wenn er mit dem Internet verbunden ist oder ein Fax verschickt. Zwei parallele Telefongespräche von einem Anschluss aus sind ebenso möglich. Zudem werden höhere Übertragungsraten als mit einem analogen Anschluss erreicht: Jeder B-Kanal kann 64 kBit/s übertragen, beide zusammen also 128 kBit/s.<br>Die digitale Übertragungs- und Vermittlungstechnik von ISDN gestattet, dass am Telefonanschluss so unterschiedliche Kommunikationsarten wie Telefonieren, Faxen oder Internetverbindungen möglich sind.<br>ISDN verwendet für die Anbindung der Kunden an die Vermittlungsstelle weiterhin die Kabel des zuvor analog betriebenen Telefonnetzes. Die ISDN-Technologie nutzt diese jedoch deutlich effizienter und flexibler. Verbindungen lassen sich schneller aufbauen, die Sprachqualität ist erheblich besser und die Übertragung von Daten ist nicht nur schneller, sondern dank Fehlerkorrektur auch extrem zuverlässig. |
| 8 | NTBA | Abkürzung für Network Termination Basic Rate Access (dt. Netzabschlussgerät am Basisanschluss).<br>Der NTBA bildet den Netzabschluss des öffentlichen ISDN-Netzes. Er setzt das Signal des Netzbetreibers von dessen Zweidrahtleitung (UK0-Bus) auf eine Vierdrahtleitung (S0-Bus) um.<br>Der NTBA wird über die ISDN-Speisespannung von der Vermittlungsstelle mit Strom versorgt - der NTBA versorgt wiederum den S0-Bus. Im normalen Betriebszustand wird der NTBA dazu zusätzlich über ein Netzteil gespeist. In diesem Betriebszustand kann er bis zu vier am S0-Bus angeschlossene Endgeräte versorgen, die über keine eigene Stromversorgung verfügen.<br>Wird der NTBA ohne ein zusätzliches Netzteil betrieben bzw. fällt die Stromversorgung aus, so verwendet der NTBA die ISDN-Speisespannung des Netzbetreibers für einen Notstrombetrieb. |
| 9 | Port Forwarding | Port-Forwarding ist eine Technik, um die Abbildung von Ports auf IP-Adressen in NAT-Netzen (Network Adress Translation) zu ermöglichen. Das heisst, wenn Router-Ports fest auf eine bestimmte IP-Adresse weitergeleitet werden müssen. Diese Technik wird auch Mapping oder Port-Weiterleitung genannt und ist eine Funktion, die viele der aktuellen DSL Router anbieten. Zu diesem Zweck ist meist in den erweiterten Einstellungen des Routers eine Tabelle vorhanden, in der ein zu "mappender" Port fest einer bestimmten lokalen IP-Adresse zugeordnet wird. |
| 10 | Router | Router sind zunächst und grundsätzlich Hardware-Geräte oder Software-Programme, mit denen ein oder mehrere Rechner oder ganze Netzwerke mit anderen Netzwerken verbunden werden können. |

| | | |
|---|---|---|
| | | Der Router übernimmt dabei die Steuerungszentrale, um Verbindungsanfragen an das gewünschte Netz oder den Dienst weiterzuleiten.<br>Hardware-Router und insbesondere die heutigen ISDN- oder DSL Router verfügen über die Grundfunktionalität hinaus über DHCP-Dienste bzw. DHCP-Server, mit denen die Adressvergabe und Steuerung zentral verwaltet werden kann. Je nach Einstellung können auf die Weise ganze Netzwerke automatisch mit IP-Adressen versorgt werden, was insbesondere unerfahrenen Anwendern entgegen kommt. |
| 11 | Splitter | Splitter von engl. to split, dt. aufspalten.<br>Bei ADSL-Anschlüssen teilt der Splitter das vom Anbieternetz kommende Signal in das breitbandige ADSL-Signal und das schmalbandige ISDN-Signal bzw. analoge Telefonsignal auf. Für die Übermittlung in der Gegenrichtung werden die beiden Signalanteile hingegen zusammengeführt, sodass eine zeitgleiche Übermittlung über die Teilnehmeranschlussleitung möglich ist.<br>Der Splitter ist häufig direkt in der Breitband-Anschlusseinheit enthalten (BBAE). |
| 12 | TCP | TCP, die Abkürzung für Transmission Control Protocol, ist ein wesentlicher Bestandteil des TCP/IP-Protokolls. Es ist auf Verbindungen aufgebaut und verlangt für jedes abgeschickte Paket eine Empfangsbestätigung. |
| 13 | TCP/IP | TCP/IP Abkürzung für<br>Transmission control protocol/internet protocol. Bezeichnet zumeist die ganze Familie von Protokollen. Es wurde entwickelt, um Computer in verschiedenen Netzwerken miteinander zu verbinden.<br>Heute wird TCP/IP in vielen LANs (Local Area Network) eingesetzt und ist Basis für das weltumspannende Internet. |
| 14 | T-DSL | Die Deutsche Telekom bietet seit Ende der 90er Jahre ADSL-Anschlüsse unter dem Namen T-DSL an. T-DSL ist die meistgenutzte DSL-Variante und damit zugleich der meistgenutzte Breitbandzugang ins Internet in Deutschland. Nicht nur die Deutsche Telekom ermöglicht über die Tochtergesellschaft T-Online den T-DSL Zugang zum Internet, sondern auch eine größere Anzahl von Wiederverkäufern (Reseller). Alle setzen bei der physikalischen Kundenanbindung aber auf die Infrastruktur der Deutschen Telekom. Die restlichen Anbieter verwenden vor allem eigene ADSL-Varianten oder SDSL, das aber symmetrisch arbeitet und Datenraten bis zu 2,3 MBit/s gestattet. |
| 15 | VPN<br>(Virtual Privat Network) | Mit Hilfe eines Virtual Private Network (VPN) können Firmen Mitarbeitern von Zuhause oder firmenfremden Standorten die Möglichkeit bieten, sich in das Firmennetzwerk (Intranet) über das Internet einzuwählen. Ebenso können verschiedene Firmensitze auf diese Weise verbunden werden.<br>Der Vorteil hierbei ist, dass keine Modemstrecken oder angemietete |

| | | |
|---|---|---|
| | | Kanäle nötig sind, sondern lediglich eine Internetverbindung. Der Mitarbeiter wählt sich zunächst ins Internet ein. Anschließend wird ein verschlüsselter Kanal (Tunnel) zwischen dem VPN Client und VPN Server aufgebaut. Nach einer Authentifizierung mittels Benutzernamen und Passwort bzw. Token-Card oder öffentlichem Schlüssel/Zertifikat wird ein verschlüsselter IPSec-Tunnel aufgebaut, über den die Daten abhörsicher übertragen werden können. |
| 16 | WAN | Unter dem Begriff WAN (Wide Area Network) verstehet man Netzwerke, welche Daten über größere Entfernung transportieren als ein LAN (Local Area Network). |

# 5 Gewährleistung und Support

Für die vorstehenden/nachfolgenden Siemens-internen Informationen übernehmen wir keine Gewähr.

Eine Haftung von A&D, gleich aus welchem Rechtsgrund, für durch die Verwendung der in der Fachkommunikation beschriebenen Beispiele, Hinweise, Programme, Projektierungs- und Leistungsdaten usw. verursachte Schäden ist ausgeschlossen, soweit nicht z.B. bei Schäden an privatgenutzten Sachen, Personenschäden oder wegen Vorsatzes oder grober Fahrlässigkeit zwingend gehaftet wird.