



Beschreibung

Router elmeg T444

Deutsch

Konformitätserklärung und CE-Zeichen



Dieses Gerät erfüllt die Anforderungen der R&TTE-Richtlinie 1999/5/EG:

»Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität«.

Die Konformitätserklärung kann unter folgender Internet-Adresse eingesehen werden: <http://www.funkwerk-ec.com>.



Das auf dem Gerät befindliche Symbol mit dem durchgekreuzten Müllcontainer bedeutet, dass das Gerät am Ende der Nutzungsdauer bei den hierfür vorgesehenen Entsorgungsstellen getrennt vom normalen Hausmüll zu entsorgen ist. Weiterführende Informationen über eine individuelle Rückführung der Altgeräte finden Sie unter www.funkwerk-ec.com.

© 2005 Funkwerk Enterprise Communications GmbH - Alle Rechte vorbehalten.

Ein Nachdruck dieser Dokumentation - auch auszugsweise - ist nur zulässig mit Zustimmung des Herausgebers und genauer Nennung der Quellenangabe, unabhängig von der Art und Weise oder den Medien (mechanisch oder elektronisch), mit denen dies erfolgt.

Funktionsbeschreibungen dieser Dokumentation, die sich auf Softwareprodukte anderer Hersteller beziehen, basieren auf der zur Zeit der Erstellung oder Drucklegung verwendeten Software. Die in dieser Dokumentation verwendeten Produkt- oder Firmennamen sind unter Umständen über die Eigentümer geschützte Warenzeichen.

Inhaltsverzeichnis

Einleitung	1
Router der TK-Anlage elmeg T444.	1
Einwahl ins LAN (RAS)	2
RAS Callback:	2
Direkte Verbindung (DHCP)	3
Grundeinstellung der TK-Anlage	3
Funktionen des Routers	4
Konfigurationsbeispiele.	9
Adressvergabe per DHCP -Empfohlene Konfiguration - (Grundeinstellung).	9
Beispielkonfiguration eines Netzwerkes mit gemischter Adressvergabe.	14
Überprüfen der LAN-Clients (PCs).	16
Überprüfen der TCP/IP Konfiguration	17
Konfiguration des Internetzuganges an einem PC.	20
Firewall-Filter konfigurieren	21
Filter-Wizard	24
Filter Update.	27

Einleitung

Router der TK-Anlage elmeg T444

Die TK-Anlage elmeg T444 verfügt über einen integrierten Router. Über diesen Router können Sie den Zugang zum Internet bereitstellen und mehrere PCs vernetzen.

Was ist ein Router?

Ein Router ermöglicht den LAN-Clients (Rechner, PC in einem Netzwerk) eines Netzwerkes (LAN -local area network) den Zugang zu einem anderen Netzwerk, z.B. dem Internet. Der Zugang zum Internet wird dabei von verschiedenen Internet-Service-Providern (ISP) zur Verfügung gestellt.

Der Router sucht dabei einen Weg, auf dem der Datenaustausch zwischen den LAN-Clients im lokalen Netzwerk und dem Internet erfolgt. Die Anbindung an das Internet kann über eine xDSL-Verbindung und / oder eine ISDN-Verbindung hergestellt werden.

Der Router der TK-Anlage

Der Router der TK-Anlage verfügt über einen WAN/xDSL-Anschluss (LAN2) und über einen LAN-Anschluss (LAN1). Über den WAN/xDSL-Anschluss wird die TK-Anlage an ein anderes Netzwerk, z.B. das Internet angeschlossen. Für die Verbindung in das Internet können Sie hier ein DSL- oder Kabelmodem anschließen.

Die LAN-Anschlüsse sind für Ihr lokales Netzwerk. Hier können Sie bis zu zwei PCs mit eingebauter Netzwerkkarte direkt anschließen. Möchten Sie mehr als zwei PCs vernetzen, kann dieses über einen zusätzlichen HUB / Switch, HomePN (optionales Modul, nicht im Lieferumfang enthalten) oder den USB-Anschluss erfolgen.

LAN1 stellt sich automatisch (von 10 Mbit/s halbduplex bis 100 Mbit/s vollduplex) auf das mit der Gegenstelle (PC) erreichbare Maximum der Übertragungsrate ein.

Die so angeschlossenen PCs sind Bestandteil Ihres lokalen Netzwerkes und können z. B. Dateien tauschen oder über den Router die eingerichteten Internet-Verbindungen nutzen. Alle verbundenen LAN-Clients werden über das TCP/IP-Protokoll in das lokale Netzwerk eingebunden.

Über RAS-Einwahl können sich weitere PCs mit Ihrem Netzwerk verbinden. Hier wird immer die IP-Adresse, auch wenn der DHCP-Server ausgeschaltet ist, von der TK-Anlage vergeben. Sie können in der Konfigurierung unter »Adresszuordnung« den DHCP-Server ausschalten und die Startadresse für RAS eingeben. Die 11 IP-Adressen werden dann automatisch für RAS reserviert.

RAS (Remote Access Service) ermöglicht es, z.B. einem Außendienstmitarbeiter von Extern auf ein lokales Netzwerk und über das Netzwerk auf das Internet zuzugreifen. Der Zugriff von Extern muss über einen ISDN Anschluss erfolgen. Der externe Zugang ist über einen Benutzernamen und ein Passwort geschützt. Wird die Verbindung nur von einem externen Ziel ausgeführt, kann die Rufnummer als zusätzlicher Schutz überwacht werden. Beachten Sie, dass dieser Zugang nicht über eine Firewall geschützt ist!

Bitte beachten Sie die weiteren Hinweise zum Anschluss eines PCs in der Bedienungsanleitung der TK-Anlage.

Welche Internet-Verbindungen werden unterstützt?

Sie können mit Ihrer TK-Anlage die Verbindung ins Internet auf folgende Arten herstellen:

- Über ISDN-Wählverbindungen (mittels PPP-Protokoll mit einem oder zwei ISDN B-Kanälen, also mit 64 kBit/s oder 128 kBit/s, Internet by call ist vorgeleistet).
Für diese Verbindungen benötigen Sie als Zugangsdaten die anzuwählende Rufnummer, den Benutzernamen (Username), das Passwort, ggf. weitere Angaben wie IP-Adresse des Nameservers und Angaben über verwendete Datenkompression (VJH).
- Über xDSL (z. B. ADSL - T-DSL) in Verbindung mit einem zu Ihrem ISP kompatiblen DSL-Modem per PPPoE.
Für diese Verbindungen benötigen Sie als Zugangsdaten den Benutzernamen (Username) und das Passwort.
- Über xDSL (z. B: SDSL) in Verbindung mit einem zu Ihrem ISP kompatiblen DSL-Modem mit fester öffentlicher IP-Adresse. Für diese Verbindungen benötigen Sie die Ihnen zugeordnete öffentliche IP-Adresse, die IP-Adresse des nächsten Gateways (next hop) und die IP-Adresse des Nameservers ihres Providers.

- Tunneling. Hier werden Datenpakete eines Protokolls in den Rahmen eines anderen Protokolls gepackt, um sie im Internet weiter zu leiten. Beim Empfänger wird der Rahmen wieder entfernt und das Datenpaket wird mit dem ursprünglichen Protokoll weitergeleitet. Durch das Tunneln können inkompatible Netze überwunden werden oder Sicherheits- und Kostenaspekte (z.B. PPTP) sollen genutzt werden. Als Zugangsdaten benötigen Sie normalerweise nur Usernamen und Passwort. Geben Sie bitte alle Daten an, die Ihnen Ihr Provider zusätzlich vorgibt (z.B. Rufnummer, IP-Adresse und DNS-Server).

In der Konfigurierung der TK-Anlage werden die ISP eingerichtet, die Sie für Internetverbindungen nutzen möchten. Sie können bis zu 10 ISP einrichten. Zu jedem ISP können Sie weitere Einstellungen, z.B. Benutzername, Passwort, Rufnummer, ... vornehmen. Weiterhin können Sie einstellen, ob die Verbindung zum Internet automatisch hergestellt (Grundeinstellung) werden soll und ob bei erfolglosem Verbindungsaufbau der nächste ISP in der Liste ausgewählt wird (Fallback).

Erhält der Router der TK-Anlage die Anforderung einer Internetverbindung, wird diese über den ersten ISP in der Liste aufgebaut. Ist die Verbindung erfolgreich, können alle Clients im Netz auf das Internet zugreifen. Wird die Internetverbindung nicht mehr benötigt (Inaktivität), wird sie nach Ablauf der eingestellten Zeit automatisch beendet.

Kann eine Internetverbindung nicht über den ausgewählten ISP aufgebaut werden, wird versucht, die Verbindung über den nächsten ISP in der Liste aufzubauen (Fallback).

Nach Beenden der Internetverbindung wird bei nächsten Verbindungsaufbau wieder mit dem ersten ISP in der Liste begonnen.

Weitere Hinweise zum Einrichten der ISP und zum Verbindungsaufbau in das Internet, finden Sie in der Bedienungsanleitung der TK-Anlage.

Wenn in Ihrem Netzwerk z.B. »Hubs« installiert sind oder eine Verbindung aus dem Internet besteht, kann es sein, dass weiterhin Datenpakete zum Router geschickt werden und die Verbindung nicht abgebaut werden kann.

Einwahl ins LAN (RAS)

Der Remote Access Server (RAS) ermöglicht es, z.B. einem Außendienstmitarbeiter von Extern auf ein lokales Netzwerk und über das Netzwerk auf das Internet zuzugreifen. Der Zugriff von Extern kann über einen ISDN Anschluss erfolgen.

Der externe Zugang ist über einen Benutzernamen und ein Passwort geschützt. Wird die Verbindung nur von einem externen Ziel ausgeführt, kann die Rufnummer als zusätzlicher Schutz überwacht werden. Für bis zu 8 Benutzer kann der Zugang freigeschaltet werden. Für jeden Benutzer kann eine Windows-Freigabe (Zugriff auf Computer, Dateien oder Drucker) und eine Internet-Freigabe eingerichtet werden.

Einem PC, der sich über RAS in das lokale Netzwerk einwählt, wird vom integrierten DHCP-Server automatisch eine IP-Adresse zugewiesen.

RAS Callback:

Wenn Sie bei Verbindungen in Ihr Firmennetzwerk die Verbindungskosten die Firma tragen soll, wird die RAS-Verbindung als Rückruf konfiguriert. Hierzu wird von Ihnen eine kurze, für Sie kostenpflichtige Verbindung zum Firmennetzwerk aufgebaut, um einen Rückruf einzuleiten. Die TK-Anlage in Ihrer Firma ruft dann zurück und die folgende Verbindungszeit ist für Sie kostenfrei. In der Konfigurierung können Sie für den entsprechenden RAS-Zugang eine Rufnummer eintragen. Ein Rückruf ist dann nur von dieser Rufnummer aus möglich. Wird keine Rufnummer eingetragen, ist der Rückruf von jeder Rufnummer aus möglich.

DHCP-Server und IP-Adressvergabe

Über DHCP (Dynamic Host Configuration Protocol) können PC mit einem wesentlichen Teil der für LAN- und Internetzugang erforderlichen Konfiguration versehen werden. Der in der TK-Anlage integrierte DHCP-Server ist in der Lage, bis zu 100 PC (Clients) mit der entsprechenden Konfiguration zu versorgen. Die IP-Adressen werden den Clients dynamisch zugeordnet. Der DHCP-Server-Dienst der TK-Anlage ist im Grundzustand eingeschaltet.

Die Konfiguration des integrierten DHCP-Servers können Sie unter »Netzwerk-Adresszuordnung« vornehmen.

Die erste IP-Adresse, die vom DHCP-Server vergeben wird, können Sie konfigurieren. Entsprechend der Anzahl der zu vergebenen IP-Adressen werden diese in aufsteigender Reihenfolge an die PC (DHCP-Clients) vergeben.

Für PCs, die über RAS in das lokale Netzwerk eingebunden sind, sind immer 11 zusätzliche IP-Adressen für den DHCP-Server reserviert. Ist der integrierte DHCP-Server eingeschaltet, werden für RAS-Clients immer die 11 IP-Adressen verwendet, die auf den eingerichteten DHCP-Adressbereich folgen.

Bei ausgeschaltetem DHCP-Server werden immer die 11 IP-Adressen, die auf die eingestellte DHCP-Start-Adresse folgen, für RAS-Clients verwendet.

Direkte Verbindung (DHCP)

Über diese Einstellung können Sie eine direkte WAN-Verbindung mit automatischer Vergabe der IP-Adresse über DHCP nutzen. Hierbei wird die IP-Adresse nicht vom Router Ihrer TK-Anlage vergeben sondern vom Netz in das der Router eingebunden ist. Dazu muss das DHCP des Routers in der Konfigurierung ausgeschaltet werden

Grundeinstellung der TK-Anlage

IP-Adressen des lokalen Netzes in der Grundeinstellung

Sie können die TK-Anlage bereits in der Grundeinstellung als Router für den Internetzugang Ihres lokalen Netzes nutzen. Sie müssen in der Konfigurierung der TK-Anlage den Internet-Service-Provider einrichten, die Sie nutzen möchten.

Die IP-Adressen Ihres lokalen Netzes sind dann wie folgt verteilt:

192.168.1.1 bis 192.168.1.49	Frei verfügbare IP-Adressen, z.B. für LAN-Clients mit fester IP-Adresse
192.168.1.50 bis 192.168.1.69	IP-Adressen, die von der TK-Anlage als DHCP-Server an entsprechende LAN-Clients vergeben werden. (Anzahl der DHCP-Clients: 20)
192.168.1.70 bis 192.168.1.80	Reservierte IP-Adressen (11) RAS. Diese Adressen müssen immer reserviert bleiben und dürfen nicht als feste IP-Adressen vergeben werden.
192.168.1.81 bis 192.168.1.249	Frei verfügbare IP-Adressen, z.B. für LAN-Clients mit fester IP-Adresse
192.168.1.250	IP-Adresse der TK-Anlage
192.168.1.251 bis 192.168.1.254	Frei verfügbare IP-Adressen, z.B. für LAN-Clients mit fester IP-Adresse

Bitte beachten Sie, dass jede IP-Adresse nur einmal vergeben werden darf. Die erste und die letzte IP-Adresse eines Netzes dürfen nicht an LAN-Clients vergeben werden. In diesem Beispiel: 192.168.1.0 und 192.168.1.255.

Beispiel für den Tipp:

255.255.255.0	Subnetzmaske für alle Komponenten im Netzwerk (TK-Anlage, LAN-Clients, ...)
192.168.1.250	IP-Adresse des Gateways (TK-Anlage)
192.168.1.250	IP-Adresse des DNS-Servers (TK-Anlage). Die TK-Anlage übernimmt auch die Aufgaben eines DNS-Proxys in der Vertretung für die DNS-Server der ISPs.

Was sind IP-Adressen und Subnetzmasken

In der Grundeinstellung sind bereits IP-Adresse und Subnetzmaske für den Router der TK-Anlage eingestellt. Beide Werte sind jeweils 4 Byte lang.

IP-Adresse:	192.168.1.250
Subnetzmaske:	255.255.255.0

Bei der IP-Adresse handelt es sich um eine Adresse, die für private lokale Netzwerke reserviert ist.

Durch die Subnetzmaske wird festgelegt, dass es sich hierbei um ein Netz der Klasse C handelt, indem bis zu 254 LAN-Clients vernetzt werden können. Anhand der Subnetzmaske kann eine IP-Adresse in die Netzwerkadresse und in die Hostadresse (Adresse des PCs) aufgeteilt werden.

Beispiel anhand der TK-Anlage:

IP-Adresse der TK-Anlage:	192.168.1.250
IP-Netzmaske der TK-Anlage:	255.255.255.0
Netzwerkteil der IP-Adressen:	192.168.1.xxx
Hostteil der Adresse:	x.x.x.250
Erste verwendbare IP-Adresse:	192.168.1.1 (Netzmaske: 255.255.255.0)
Letzte verwendbare IP-Adresse:	192.168.1.254 (Netzmaske: 255.255.255.0)

Die verwendbaren IP-Adressen können Sie den einzelnen LAN-Clients manuell zuweisen oder per DHCP durch die TK-Anlage zuweisen lassen. Dabei darf jedoch keine IP-Adresse zur gleichen Zeit von mehr als einem Client verwendet werden. Das bedeutet bezogen auf obiges Beispiel, dass die Adresse 192.168.1.250 nicht erneut vergeben werden darf, da diese bereits von der TK-Anlage verwendet wird.

Damit alle LAN-Clients sich in dem gleichen IP-Netz befinden, darf der Netzwerkteil der IP-Adresse nicht verändert werden. Ein PC mit der IP-Adresse 192.168.2.1 befindet sich in einem anderen Netz. Ein PC aus dem Netz der TK-Anlage würde diesen PC nicht im eigenen Netzwerk finden.

Außerdem muss auf allen LAN-Clients des gleichen Netzwerkes auch die gleiche Subnetzmaske eingetragen werden.

Funktionen des Routers

Automatischer Internetzugang, Fallback

In der TK-Anlage können mehrere Internetzugänge (ISP - Internet Service Provider) eingerichtet werden. Der Internetzugang kann über die WAN-Schnittstelle (z.B. DSL-Anschluss) oder über einen ISDN-Anschluss hergestellt werden. Bei Bedarf kann die Verbindung zum Internet automatisch aufgebaut werden. Ist der gewählte ISP nicht erreichbar, wird automatisch der nächste ISP in der Liste ausgewählt.

Short Hold

Short Hold bedeutet, dass die TK-Anlage nach einer konfigurierbaren Zeitspanne automatisch die Internetverbindung abbaut, wenn keine Daten mit dem Internet ausgetauscht werden. Diese Zeit kann für jeden eingerichteten ISP separat eingestellt werden.

Bei häufigen kurzen Internetzugängen z.B. E-Mail-Abrufe kann dieses zu erhöhten Verbindungskosten kommen, da die Verbindung immer für die Dauer der Haltezeit aufrecht erhalten wird.

Dynamik-ISDN

Bei einem Internetzugang über den ISDN-Anschluss können wahlweise auch die beiden B-Kanäle des Anschlusses gebündelt werden, um höhere Datenübertragungsraten zu erreichen. Ist eine Internetverbindung mit Kanalbündelung aktiv und ein B-Kanal wird für eine Telefonie- oder Faxverbindung benötigt, wird ein B-Kanal der Internetverbindung getrennt. Nach Beendigung der Sprachverbindung wird der B-Kanal wieder automatisch für die Internetverbindung verwendet. Diese Funktion steht bei kommenden und gehenden Sprachverbindungen zur Verfügung.

Dieses Leistungsmerkmal setzt die Installation des ISDN Speedmanagers oder den Internetzugang über den Router voraus! In der Installation von T-Online ist der Speedmanager enthalten.

Rufzustellung bei Besetzt:

Wenn Sie gerade im Internet surfen, und zum Download zwei B-Kanäle nutzen, sind Sie telefonisch von Extern nicht mehr erreichbar. Da die Signalisierung eines weiteren Anrufes über den D-Kanal erfolgt, hat Ihre Telefonanlage je nach Einstellung die Möglichkeit, einen B-Kanal gezielt abzuschalten und Sie können das Gespräch annehmen. Die folgenden Einstellung können im PC-Konfigurator eingestellt werden.

Ablehnen:

Dem Anrufer wird Besetzt signalisiert, beide B-Kanäle bleiben aktiv.

Interne Rufnummer:

Ein B-Kanal wird abgeschaltet (der Anrufer hört dabei kurzzeitig Wartemusik, siehe auch Seite) und der Anruf wird beim unter »Interne Rufnummer« eingetragenen Teilnehmer signalisiert. Dieses Endgerät darf sich nicht am gleichen ISDN-Bus oder USB-Anschluss wie der PC befinden.

Weiterschaltung (Call Deflection) zu externer Rufnummer :

Ein B-Kanal wird abgeschaltet und der Anruf beim unter »Externe Rufnummer« eingetragenen Teilnehmer signalisiert. Sie können das Gespräch aber auch in der Vermittlungsstelle zu einem externen Teilnehmer weiterleiten lassen, dann bleiben beide B-Kanäle aktiv. Anrufe können so weitervermittelt werden (z.B. T-NetBox oder Handy), ohne dass ein B-Kanal der Telefonanlage belegt wird.

Normale Anrufverteilung:

Ein B-Kanal wird abgeschaltet und der Anruf beim in der »Anrufzuordnung« der »Externen Rufnummer« eingetragenen Teilnehmern signalisiert.

Dynamik-ISDN für gehende Verbindungen

Wenn Sie gerade im Internet surfen, und zum Download zwei B-Kanäle nutzen, können Sie nicht mehr nach Extern telefonieren. Ihre Telefonanlage hat je nach PC-Konfigurierung die Möglichkeit, einen B-Kanal gezielt abzuschalten, damit Sie telefonieren können.

DHCP-Server

Über DHCP (Dynamic Host Control Protocol) können PCs mit einem wesentlichen Teil der für LAN- und Internetzugang erforderlichen Konfigurierung automatisch versehen werden. Der integrierte DHCP-Server ist in der Lage, mehrere PCs (LAN-Clients) mit der entsprechenden Konfigurierung zu versorgen. Die IP-Adressen werden den Clients dynamisch zugeordnet. Diese Betriebsart wird empfohlen, da somit die umständliche manuelle Konfiguration der IP-Adressen der PC entfällt.

DNS-Server

Der DNS-Server (Domain Name Server) übernimmt in einem Netzwerk die Namensauflösung. Dabei werden IP-Adressen von PCs (z.B. LAN-Clients) zu Namen aufgelöst. Für den Zugriff oder die Suche nach einem PC müssen Sie daher nicht seine IP-Adresse sondern seinen Namen kennen. Der DNS-Server kann auch Namen auflösen, die sich nicht im lokalen Netzwerk befinden.

DNS-Proxy

Ein Proxy übernimmt die Stellvertreter-Funktion des lokalen Netzwerkes (LAN) in einem anderen / externen Netzwerk. Der DNS-Proxy nimmt dabei die Namensabfragen von LAN-Clients entgegen und stellt Sie als eigene Anfragen in das externe Netzwerk, z.B. in das Internet. Anschließend nimmt er die Antwort aus dem externen Netzwerk entgegen und leitet Sie an den ursprünglich anfragenden LAN-Client weiter. Außerdem wird das Ergebnis der Anfrage für eine konfigurierte Zeit gespeichert, um die nächste gleichartige Anfrage selbst zu beantworten.

Dynamic DNS

Mit Dynamic DNS können Sie in Ihrem lokalen Netzwerk auch eigene Internetdienste (z.B. WEB-, FTP- oder Email-Server) anbieten. Dafür benötigen Sie normalerweise eine Standleitung oder eine fest IP-Adresse, damit Sie immer unter der gleichen Adresse erreichbar sind (z.B. www.Funkwerk-ec.com).

Bei jeder Einwahl in das Internet wird Ihnen jedoch vom ISP eine neue IP-Adresse zugewiesen. Mit Dynamic DNS können Sie diese automatisch (dynamische) IP-Adresse mit einem festen Namen verknüpfen. Der Router informiert dabei Ihren Anbieter des Dynamic DNS-Dienstes (z.B. www.dyndns.org) automatisch über die neu IP-Adresse. Internetanfragen für Ihre Webdienste werden über Ihren Anbieter automatisch zu Ihrer dynamischen IP-Adresse weitergeleitet.

Anwendung von Dynamic DNS

- Richten Sie bei einem Dynamic DNS-Anbieter eine Internet-Adresse ein. Zum Beispiel bei »www.dyndns.org« die Adresse »www.meine-homepage.dyndns.org«.
- Konfigurieren Sie den LAN-Client Ihres Netzwerkes, auf dem Sie die Webdienste anbieten möchten, mit einer festen IP-Adresse. Zum Beispiel richten wir einen Web-Server mit der IP-Adresse 192.168.1.200 ein.
- Aktivieren Sie im Router die Dynamic DNS-Funktion und tragen Sie die Internet-Adresse Ihres Dynamic DNS-Anbieters ein (Im Beispiel www.dyndns.org). Ergänzen Sie in der Firewall die notwendigen Filter, um den PC mit den Webdiensten von Extern zu erreichen.
 - Konfigurieren Sie ein Portmapping für Port 80 (HTTP-Protokoll) auf die IP-Adresse 192.168.1.200.
 - Richten Sie die Filter ein, die kommende und gehende WAN-Verbindungen auf Port 80 erlaubt.
- Bei jeder Internetverbindung, informiert der Router automatisch Ihren Dynamic DNS-Anbieter über Ihre aktuelle dynamische IP-Adresse. Die Informationen über die IP-Adresse werden nach dem Neuaufbau einer Internetverbindung und auch während einer bestehenden Internetverbindung übermittelt.
- Ein PC im Internet gibt die Adresse »www.meine-homepage.dyndns.org« ein. Er erreicht damit Ihren Dynamic DNS-Anbieter. Der Anbieter leitet die Verbindung zu Ihrer aktuellen dynamischen IP-Adresse um.
- Die kommende Verbindung wird gemäß den konfigurierten Filtern behandelt. Im Beispiel wird die kommende WAN-Verbindung auf Port 80 an den LAN-Client mit der IP-Adresse 192.168.1.200 weitergeleitet. Auf dem PC fremden PC werden die verfügbaren Internet-Seiten auf Ihren Web-Server angezeigt.

NAT

NAT (Network Address Translation) dient zum Schutz der angeschlossenen LAN-Clients gegen Angriffe aus dem Internet. Dabei werden interne IP-Adressen nicht an das Internet weitergegeben. Der Router übernimmt die Übersetzung ins Internet und verteilt die ankommenden Datenpakete intern. Dadurch wird nur eine externe IP-Adresse benötigt. Die internen IP-Adressen werden vor Angriffen von Extern geschützt. Da die internen IP-Adressen nicht erreichbar sind, können sie nicht für Hacker als Angriffsziel dienen.

Packet Filter Firewall

Die integrierte Packet Filter Firewall bietet Ihnen zusätzliche Sicherheit gegen Angriffe aus dem Internet. Eine Firewall stellt eine logische Mauer für Datenpakete zwischen dem Internet und dem LAN dar, die für bestimmte Pakete »Löcher« (Firewall-Regeln, auch als Filter bezeichnet) enthält und damit gewünschte Datenpakete passieren lässt. Die Filter werden durch beschriebenen Regeln, deren Konfiguration Expertenwissen über die TCP/IP-Protokollfamilie voraussetzt. Die Firewall ihrer TK-Anlage kann aber sehr leicht durch einen Filter Wizard konfiguriert werden, bei dem Sie lediglich angeben müssen, ob Sie bestimmten, durch Klartextbeschreibung benannten Applikationen den Internetzugang ermöglichen wollen.

Portmapping

Sie möchten von Extern über das Internet auf einen Ihrer PCs zugreifen. Normalerweise sollte dieser Zugang über die Firewall verhindert werden. Wenn Sie das Portmapping nutzen, wird von Extern auf einen von Ihnen freigegebenen Port des Routers zugegriffen. Der Router leitet den Zugriff dann auf den vorgegebenen Port des PCs im Netzwerk weiter. Diesem PC muss eine feste IP-Adresse zugewiesen werden. Wenn der PC Datenpakete zurückschickt, werden IP-Adresse und Portnummer des PCs vom Router durch die Nummer des Portmapping-Ports und die Router IP ersetzt. Für Externe aus dem Internet sieht es dann so aus, als ob nur eine Verbindung mit dem Router besteht.

Beachten Sie, dass bei Einsatz des Portmapping die Firewall für die hierfür freigegebenen Ports unwirksam ist. Der Ziel-PC in Ihrem LAN ist möglicherweise Angriffen schutzlos ausgeliefert.

Portmapping einzusetzen ist sinnvoll, wenn Sie z. B. einen Spieleserver selbst betreiben möchten.

- Diesen können Sie über das Internet anderen Nutzern zugänglich machen.
- Oder wenn bestimmte Peer-to-Peer Filesharing-Software eingesetzt werden soll, die eine höhere Downloadbandbreite ermöglicht.

- Wenn der entsprechende PC in Ihrem LAN auch aus dem Internet erreichbar sein soll (dieses ist bei Standardkonfiguration durch NAT nicht möglich). In diesen Fällen müssen bestimmte UDP und TCP Ports auf einen PC im LAN weitergeleitet werden.

RAS-Server

Der Remote Access Server (RAS) ermöglicht es, z.B. einem Außendienstmitarbeiter von Extern auf ein lokales Netzwerk und über das Netzwerk auf das Internet zuzugreifen. Der Zugriff von Extern kann über einen ISDN Anschluss erfolgen.

Der externe Zugang ist über einen Benutzernamen und ein Passwort geschützt. Wird die Verbindung nur von einem externen Ziel ausgeführt, kann die Rufnummer als zusätzlicher Schutz überwacht werden. Der Zugang kann für mehrere Benutzer individuell freigeschaltet werden. Für jeden Benutzer kann eine Windows-Freigabe (Zugriff auf Computer, Dateien oder Drucker) und eine Internet-Freigabe eingerichtet werden.

Beachten Sie, dass dieser Zugang nicht über eine Firewall geschützt ist!

Einem PC, der sich über RAS in das lokale Netzwerk einwählt, wird vom integrierten DHCP-Server automatisch eine IP-Adresse zugewiesen.

Zeitgesteuerte Routersperre

Über den Kalender oder eine manuelle Funktion der TK-Anlage haben Sie die Möglichkeit, Internetzugänge nur zu bestimmten Tageszeiten zu ermöglichen. Die Festlegung erfolgt über den dem Router in der Konfiguration zugeordneten Kalender. Hierbei ist festgelegt, dass im Nachtbetrieb keine Internet-Verbindungen möglich sind. Setzen Sie daher die Schaltpunkte entsprechend. Ab der Version 4 der Systemtelefone CS290/CS410 kann eine Umschaltung über Funktionstasten der Telefone erfolgen, die dann bis zur nächsten kalenderbedingten Umschaltung bestehen bleibt.

LAN-CAPI

Für Ihr Netzwerk wird Ihnen ein Programm »CAPI im LAN« mitgeliefert. Dieses Programm kann auf jedem PC im Netzwerk installiert werden. Damit haben Sie die Möglichkeit, Ihre CAPI-Anwendung zentral über eine Schnittstelle, die TK-Anlage, zu betreiben. Sie müssen in keinem PC eine ISDN-Karte installieren. Beachten Sie, dass die verwendete Software für die CAPI-Anwendung bestimmten Lizenzvereinbarungen mit dem Hersteller der Software bedarf. Das Programm »CAPI im LAN« ist lizenzfrei.

LAN-TAPI

Für Ihr Netzwerk wird Ihnen ein Programm »TAPI im LAN« mitgeliefert. Dieses Programm kann auf jedem PC im Netzwerk installiert werden. Damit haben Sie die Möglichkeit, Ihre TAPI-Anwendung zentral über eine Schnittstelle, die TK-Anlage, zu betreiben. Sie müssen in keinem PC eine ISDN-Karte installieren. Beachten Sie, dass die verwendete Software für die TAPI-Anwendung bestimmten Lizenzvereinbarungen mit dem Hersteller der Software bedarf. Das Programm »TAPI im LAN« ist lizenzfrei.

Sperren des Internetzugangs durch den Provider

Nach mehreren fehlerhaften Eingaben von Benutzernamen oder Paßwort sperrt der Provider den Internetzugang für eine bestimmte Zeit. Um das zu verhindern, lässt der Router nur drei Versuche zu. Anschließend müssen Sie den Router erst neu konfigurieren und dann Benutzernamen und Paßwort korrekt eingeben. Danach muss der Router über das ControlCenter wieder entsperrt werden.

Verbindungstest

Sie können eine Verbindung zu Ihrem Provider testen, ohne dass eine Verbindung aufgebaut wird. In der Konfiguration befindet sich in der Providerauswahl ein Eintrag »Verbindungstest T-Online für DSL und ISDN. Wählen Sie diesen Eintrag als ersten Provider aus und speichern Sie ihn in der TK-Anlage. Über das ControlCenter können Sie dann manuell eine Internetverbindung aufbauen, dessen Ergebnis nach einigen Sekunden angezeigt wird. Hierbei wird allerdings keine wirkliche Internetverbindung aufgebaut. Ist das Ergebnis positiv, löschen Sie den eingetragenen Provider und verwenden Sie anschließend zum Aufbau der Internetverbindung die von Ihrem Provider vorgegebenen Einstellungen zum Eintrag in die Konfiguration..

Routersteuerung über das Systemtelefon

Ab Version 4 kann bei den Systemtelefonen CS290 / CS410 /CS400xt eine Funktionstaste zur Routersteuerung eingerichtet werden.

LED Einstellungen

Über die Konfigurierung der TK-Anlage können die Leuchtdioden bis auf die LED »Betrieb« ausgeschaltet werden. Nach dem erneuten Einschalten der LEDs kann die LED »ISDN« möglicherweise einen falschen Status anzeigen. Bitte trennen Sie daher den externen ISDN-Anschluss für eine kurze Zeit vom NT.

Statusanzeige CAPI / TAPI im ControlCenter

Über das Menü des ControlCenters werden Informationen zur Überwachung der CAPI- TAPI-Funktionen angezeigt. Die jeweilige Anzeige erfolgt nur wenn auf dem PC TAPI- und CAPI-Client installiert sind.

- Besteht eine TAPI-Verbindung zur TK-Anlage, wird die Anzahl der zurzeit genutzten TAPI-Lizenzen (max. 10) angezeigt.
- Besteht eine CAPI-Verbindung zur TK-Anlage, wird die Anzahl der zurzeit genutzten CAPI-Lizenzen (max. 10) und die Belegung der internen und externen B-Kanäle (jeweils max. 2) angezeigt.

Konfigurationsbeispiele

Adressvergabe per DHCP -Empfohlene Konfiguration - (Grundeinstellung)

Durch die Adressvergabe per DHCP entsteht der geringste Konfigurationsaufwand in der TK-Anlage und auf den Clients (PCs).

Sie können einen LAN-Client des Netzwerkes so konfigurieren, dass er seine IP-Adresse beim Starten automatisch von einem DHCP-Server aus der TK-Anlage zugewiesen bekommt. In der Konfiguration des LAN-Clients (PCs) müssen dann keine IP-Adressen oder Subnetzmasken eingetragen werden.

Was ist bei dieser Konfiguration zu beachten?

TK-Anlage:

Die TK-Anlage ist für die Adressvergabe per DHCP in der Grundeinstellung bereits vorkonfiguriert.

Es ist lediglich erforderlich, einen ISP (Internet Service Provider) auszuwählen. Bitte folgen Sie dazu den Hinweisen im Handbuch oder dem Faltblatt »Der schnelle Weg ins Internet«.

Der DHCP-Server ist im Auslieferungszustand bereits aktiviert und vorkonfiguriert. Bei Bedarf können Sie die Startadresse (erste IP-Adresse, die per DHCP vergeben wird) und die maximale Anzahl der LAN-Clients (PCs) festlegen.

LAN-Client (PC) Konfiguration:

PCs mit Betriebssystemen ab Windows 98SE sind in der Standardeinstellung für die Adressvergabe per DHCP bereits korrekt konfiguriert.

Wenn auf dem LAN-Client (PC) bereits andere Internetverbindungen z.B. über ein Modem oder eine ISDN-Karte eingerichtet wurde, beachten Sie bitte die Hinweise im Abschnitt »Einstellungen im Internet Explorer / Internetoptionen von Windows« in diesem Dokument.

Bitte beachten Sie, dass Veränderungen an den Windows Netzwerkeinstellungen auf den LAN-Clients (PCs) schwerwiegende Auswirkungen haben können. Möglicherweise werden andere Verbindungen oder Applikationen ebenfalls von den Änderungen beeinflusst. Für den Fall, dass Ihre Netzwerkkonfiguration bereits verändert wurde, halten Sie bitte Rücksprache mit Ihrem Systemadministrator. Erstellen Sie falls notwendig eine Datensicherung. Die im Folgenden dargestellte Konfiguration stellt nur eine Möglichkeit dar. Diese Einstellungen werden empfohlen. Je nachdem welche Infrastruktur bei Ihnen vorhanden ist, kann es sinnvoll sein, eine andere Konfiguration zu wählen.

Sollte es notwendig sein, die Netzwerkeinstellungen von Windows in die Grundeinstellung zurückzusetzen, gehen Sie bitte folgendermaßen vor:

Beispiel Windows 98SE /ME:

- Öffnen Sie die Systemsteuerung über das Startmenü von Windows.
- Windows 98SE: Öffnen Sie den Ordner »Netzwerk«
- Windows ME: Wählen Sie »Netzwerkumgebung« mit einem rechten Mausklick, wählen Sie »Eigenschaften«.
- Wählen Sie das Protokoll »TCP/IP« und betätigen Sie »Eigenschaften«.

Der mit der TK-Anlage verbundene Netzwerkadapter benötigt eine Anbindung an das TCP/IP Protokoll, welches Bestandteil von Windows ist. Es kann erforderlich sein, dieses Protokoll manuell hinzuzufügen. Insbesondere, wenn bereits eine Einzelplatz Version des T-DSL Treibers installiert wurde, ist es möglich, dass der Netzwerkadapter nur eine Bindung an das T-DSL / PPPoE Protokoll hat. Fügen Sie dann das TCP/IP Protokoll manuell über die Schaltflächen »Hinzufügen«, »Protokoll«, »Microsoft«, »TCP/IP« hinzu.

- Wählen Sie jetzt aus, dass der PC seine IP-Adresse automatisch beziehen soll. Alle weiteren Einstellungen wie z.B. DHCP, Netzwerkmaske, Gateway und DNS-Server sollten deaktiviert oder leer sein. Die TK-Anlage übermittelt alle erforderlichen Einstellung automatisch per DHCP an den Client (PC).
- Bestätigen Sie Ihre Einstellungen mit OK.

Beispiel Windows 2000 und Windows XP:

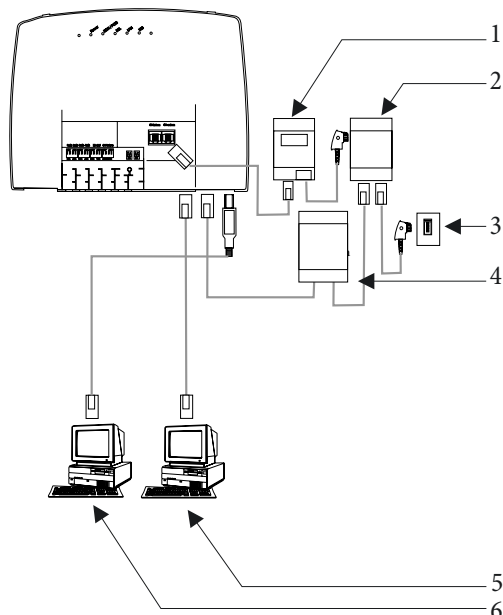
- Öffnen Sie die Systemsteuerung über das Startmenü von Windows.
- Öffnen Sie unter Windows 2000 den Ordner »Netzwerk- und DFÜ-Verbindungen«.
- Öffnen Sie unter Windows XP den Ordner »Netzwerkverbindungen«.
- Wählen Sie die »LAN-Verbindung« für die Verbindung mit der TK-Anlage mit einem rechten Mausklick und betätigen Sie anschließend »Eigenschaften«.
- Wählen Sie das Protokoll »TCP/IP« und betätigen Sie »Eigenschaften«.
- Wählen Sie jetzt aus, dass der PC seine IP-Adresse automatisch beziehen soll. Alle weiteren Einstellungen wie z.B. DHCP, Netzwerkmaske, Gateway und DNS-Server sollten deaktiviert oder leer sein. Die TK-Anlage übermittelt alle erforderlichen Einstellungen automatisch per DHCP an den Client (PC).
- Bestätigen Sie Ihre Einstellungen mit OK.

Bitte beachten Sie auch die Hinweise in der Dokumentation und der Hilfe Ihres Betriebssystems.

Sollte es nicht möglich sein, eine Verbindung zur TK-Anlage oder zum Internet aufzubauen, lesen Sie bitte den Abschnitt »Überprüfen LAN-Client (PC) Konfiguration« in diesem Dokument.

Beispielkonfiguration eines Netzwerkes mit DHCP Adressvergabe

Konfigurierung der TK-Anlage in der Grundeinstellung



- 1 - NTBA
- 2 - NTBA / Splitter
- 3 - Anschluss des Netzbetreibers
- 4 - Modem
- 5 - Netzwerk PC 2 am HUB / Switch
- 6 - PC 1 am USB-Anschluss

IP-Adresse der TK-Anlage: 192.168.1.250

Subnetzmaske: 255.255.255.0

Startadresse DHCP: 192.168.1.50

Anzahl DHCP-Adressen: 20

PC1

IP über DHCP:	192.168.1.50 wird automatisch per DHCP übermittelt.
Gateway:	wird automatisch per DHCP übermittelt.
DNS-Server:	wird automatisch per DHCP übermittelt.
Subnetzmaske:	wird automatisch per DHCP übermittelt.

PC2

IP über DHCP:	192.168.1.53 wird automatisch per DHCP übermittelt.
Gateway:	wird automatisch per DHCP übermittelt.
DNS-Server:	wird automatisch per DHCP übermittelt.
Subnetzmaske:	wird automatisch per DHCP übermittelt.

Die IP-Adressen der Clients (PCs) können in diesem Beispiel im Bereich zwischen 192.168.1.50 und 192.168.1.69 liegen. Die Zuteilung der IP-Adressen erfolgt in der Reihenfolge, in der die Clients (PCs) diese anfordern (z.B. durch Einschalten des PCs). Wird ein IP-Adresse freigegeben (z.B. durch Ausschalten des PCs), steht die IP-Adresse für eine erneute Vergabe wieder zur Verfügung.

Adressvergabe ohne DHCP (feste / gemischte IP-Adressen)

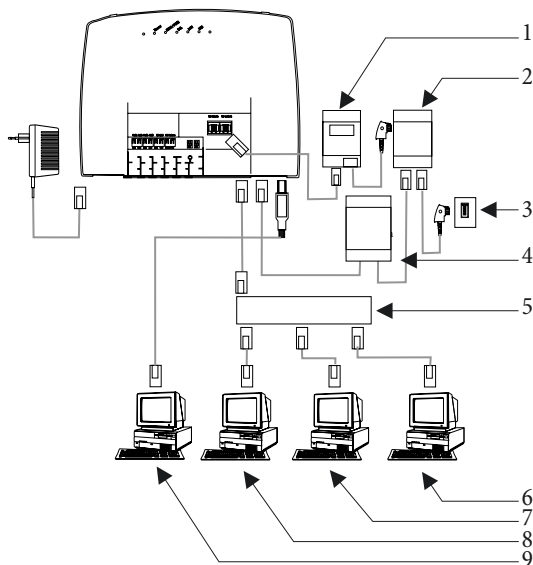
Sie können in einem Netzwerk auf einen DHCP-Server verzichten oder ergänzend zu DHCP-Clients auch AN-Clients (PCs) mit festen IP-Adressen einrichten.

Durch die Konfiguration ohne DHCP entsteht ein höherer Aufwand bei der Einrichtung des Netzwerks. Haben Sie noch keine Erfahrungen mit der Windows Netzwerkkonfiguration gesammelt, empfehlen wir Ihnen die Konfiguration per DHCP.

Was ist bei dieser Konfiguration zu beachten?**TK-Anlage:**

Der DHCP-Server der TK-Anlage kann über die Konfiguration deaktiviert werden.

Die IP-Adresse und Subnetzmaske der TK-Anlage muss möglicherweise an die auf den LAN-Clients (PCs) vorhandenen Einstellungen angepasst werden. Hinweise hierzu erhalten Sie in der Online Hilfe des Konfigurators.



- 1 - NTBA
- 2 - NTBA / Splitter
- 3 - Anschluss des Netzbetreibers
- 4 - Modem
- 5 - Externer HUB / Switch über LAN2 (100 MBit/s)
- 6 - Netzwerk PC 4 am HUB / Switch
- 7 - Netzwerk PC3 am HUB / Switch
- 8 - Netzwerk PC2 am HUB / Switch
- 9 - PC 1 am USB-Anschluss

LAN-Client (PC) Konfiguration

Folgende Mindesteinstellungen müssen Sie manuell vornehmen:

- IP-Adresse des LAN-Clients (PCs)
- Netzmaske / Subnetzmaske (sind auch in dem Router der TK-Anlage eingetragen)
- IP-Adresse der TK-Anlage als Gateway (Schnittstelle zu anderen Netzen, z.B. zum Internet)
- IP-Adresse der TK-Anlage als DNS-Server (Server, der die Internet-Adressen in IP-Adressen umsetzt)

Bitte beachten Sie die Hinweise zur Adressvergabe auf den vorangegangenen Seiten.

Einstellungen eines PCs mit einem Windows-Betriebssystem

Bei den nachfolgend beschriebenen Abläufen handelt es sich nur um Beispiele, die je nach Betriebssystem und Konfiguration des PCs abweichen können.

Bitte beachten Sie, dass Veränderungen an den Windows Netzwerkeinstellungen auf den LAN-Clients (PCs) schwerwiegende Auswirkungen haben können. Möglicherweise werden andere Verbindungen oder Applikationen ebenfalls von den Änderungen beeinflusst. Für den Fall, dass Ihre Netzwerkkonfiguration bereits verändert wurde, halten Sie bitte Rücksprache mit Ihrem Systemadministrator. Erstellen Sie falls notwendig eine Datensicherung. Die im Folgenden dargestellte Konfiguration stellt nur eine Möglichkeit dar. Diese Einstellungen werden empfohlen. Je nachdem, welche Infrastruktur bei Ihnen vorhanden ist, kann es sinnvoll sein, eine andere Konfiguration zu wählen.

Beispiel Windows 98SE und Windows ME:

- Öffnen Sie die Systemsteuerung über das Startmenü von Windows.
- Öffnen Sie den Ordner »Netzwerk«.

- Wählen Sie das Protokoll »TCP/IP« und betätigen Sie »Eigenschaften«.
- Wählen Sie jetzt aus, ob der PC seine Adresse automatisch von einem DHCP-Server beziehen oder eine feste IP-Adresse erhalten soll. Verändern oder ergänzen Sie die Einstellungen für Netzwerkmaske, Gateway und DNS-Server. Bitte entnehmen Sie die einzustellenden Parameter der Beispielkonfiguration mit gemischter Adressvergabe oder der Beispielkonfiguration mit fester Adressvergabe auf den folgenden Seiten.
- Bestätigen Sie Ihre Einstellungen mit OK.

Beispiel Windows 2000 und Windows XP

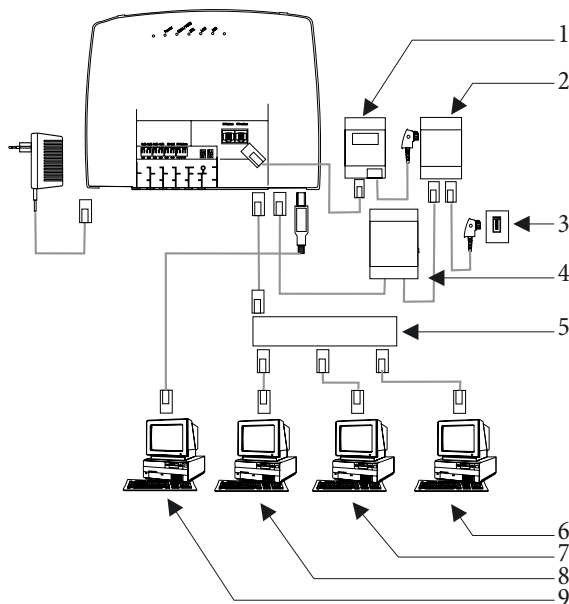
- Öffnen Sie die Systemsteuerung über das Startmenü von Windows.
- Öffnen Sie unter Windows 2000 den Ordner »Netzwerk- und DFÜ-Verbindungen«.
- Öffnen Sie unter Windows XP den Ordner »Netzwerkverbindungen«.
- Wählen Sie die »LAN-Verbindung« mit einem rechten Mausklick und betätigen Sie anschließend »Eigenschaften«.
- Wählen Sie das Protokoll »TCP/IP« und betätigen Sie »Eigenschaften«.
- Wählen Sie jetzt aus, ob der PC seine Adresse automatisch von einem DHCP-Server beziehen oder eine feste IP-Adresse erhalten soll. Verändern oder ergänzen Sie die Einstellungen für Netzwerkmaske, Gateway und DNS-Server. Bitte entnehmen Sie die einzustellenden Parameter der Beispielkonfiguration mit gemischter Adressvergabe oder der Beispielkonfiguration mit fester Adressvergabe auf den folgenden Seiten.
- Bestätigen Sie Ihre Einstellungen mit OK.

Bitte beachten Sie auch die Hinweise in der Dokumentation und der Hilfe Ihres Betriebssystems.

Es ist auch möglich, einen Teil der IP-Adressen manuell zu vergeben und die restlichen per DHCP zuzuweisen. Bitte achten Sie darauf, dass sich die IP-Adresse des Routers und manuell vergebene IP-Adressen nicht im Bereich der verfügbaren DHCP-Adressen befinden.

Beispielkonfiguration eines Netzwerkes mit gemischter Adressvergabe

Feste IP-Adressen und per DHCP-Server vergebene IP-Adressen



- 1 - NTBA
- 2 - NTBA / Splitter
- 3 - Anschluss des Netzbetreibers
- 4 - Modem
- 5 - Externer HUB / Switch über LAN2 (100 MBit/s)
- 6 - Netzwerk PC 4 am HUB / Switch
- 7 - Netzwerk PC 3 am HUB / Switch
- 8 - Netzwerk PC 2 am HUB / Switch
- 9 - PC 1 am USB-Anschluss

IP-Adresse der TK-Anlage: 192.168.1.250
Subnetzmaske: 255.255.255.0
Startadresse DHCP: 192.168.1.50
Anzahl DHCP-Adressen: 20

PC1

Feste IP: 192.168.1.91
Gateway: 192.168.1.250
DNS-Server: 192.168.1.250
Subnetzmaske: 255.255.255.0

PC2

Feste IP: 192.168.1.93
Gateway: 192.168.1.250
DNS-Server: 192.168.1.250
Subnetzmaske: 255.255.255.0

PC3

IP über DHCP: 192.168.1.50 wird automatisch per DHCP übermittelt.
Gateway: wird automatisch per DHCP übermittelt.

DNS-Server: wird automatisch per DHCP übermittelt.
 Subnetzmaske: wird automatisch per DHCP übermittelt.

PC4

IP über DHCP: 192.168.1.51 wird automatisch per DHCP übermittelt.
 Gateway: wird automatisch per DHCP übermittelt.
 DNS-Server: wird automatisch per DHCP übermittelt.
 Subnetzmaske: wird automatisch per DHCP übermittelt.

Beispielkonfiguration eines Netzwerkes mit fester Adressvergabe

IP-Adresse der TK-Anlage: 192.168.1.250
 Subnetzmaske: 255.255.255.0
 Startadresse DHCP: DHCP Server ist ausgeschaltet.
 Anzahl DHCP-Adressen: DHCP Server ist ausgeschaltet.

PC1

Feste IP: 192.168.1.81
 Gateway: 192.168.1.250
 DNS-Server: 192.168.1.250
 Subnetzmaske: 255.255.255.0

PC3

Feste IP: 192.168.1.83
 Gateway: 192.168.1.250
 DNS-Server: 192.168.1.250
 Subnetzmaske: 255.255.255.0

PC4

Feste IP: 192.168.1.84
 Gateway: 192.168.1.250
 DNS-Server: 192.168.1.250
 Subnetzmaske: 255.255.255.0

PC5

Feste IP:	192.168.1.85
Gateway:	192.168.1.250
DNS-Server:	192.168.1.250
Subnetzmaske:	255.255.255.0

Überprüfen der LAN-Clients (PCs)**Konfiguration unter den Betriebssystemen Windows 98SE/ME/2000/XP**

Sollte es nicht möglich sein, eine Verbindung zur TK-Anlage oder zum Internet aufzubauen, können Sie anhand der folgenden Hinweise die Konfiguration der LAN-Clients (PCs) überprüfen.

Der hier beschriebene Ablauf setzt die empfohlene Konfiguration Adressvergabe per DHCP voraus.

Der PC ist über Ethernet (Buchse LAN1) mit der TK-Anlage verbunden.

- Überprüfen Sie, ob der im LAN-Client (PC) installierte Netzwerkadapter (Ethernetadapter oder USB) korrekt mit der TK-Anlage verbunden ist. Der Verbindungsstatus wird über die LEDs der TK-Anlage angezeigt. Eine Beschreibung der LEDs finden Sie in der Bedienungsanleitung der TK-Anlage.
- Überprüfen Sie, ob dem LAN-Client (PC) eine IP-Adresse von der TK-Anlage zugewiesen wurde (siehe Seite im Abschnitt »Überprüfen der TCP/IP Konfiguration«).
- Überprüfen Sie, ob in der TK-Anlage ein Internet Service Provider (ISP) konfiguriert ist (siehe dazu Bedienungsanleitung der TK-Anlage, Faltblatt »Der schnelle Weg ins Internet« oder Online-Hilfe der TK-Anlage).
- Überprüfen Sie, ob Ihr PC eine korrekte Konfiguration des Internet Browsers hat (siehe Seite im Abschnitt »Einstellungen im Internet Explorer / Internetoptionen von Windows«).
- Wenn die Einstellungen wie oben beschrieben vorgenommen wurden, stellt die TK-Anlage bei Anforderung durch eine Applikation (z.B. Öffnen des Internet Explorer, Eingabe einer Internet-Adresse und Bestätigen der Eingabe mit »Enter«) automatisch eine Verbindung zum Internet her (Grundeinstellung).
- Überprüfen Sie, ob der automatische Verbindungsaufbau zum Internet deaktiviert wurde (siehe Konfigurator »Netzwerk«, »Internet«, dann muss die Verbindung über das ControlCenter manuell hergestellt werden).

Der PC ist über USB mit der TK-Anlage verbunden.

- An dem USB Anschluss der TK-Anlage können Sie nur einen LAN-Client (PC) mit dem Betriebssystemen Windows 98SE/ ME/ 2000/XP betreiben.
- Beim ersten Verbinden des PCs mit der TK-Anlage wird automatisch der erforderliche USB Treiber installiert. Der Treiber befindet sich auf der mitgelieferten CD-ROM.
- Bitte folgen Sie nach erfolgreicher Installation des USB-Treibers dem für Ethernet-LAN-Clients beschriebenen Ablauf.

Der mitgelieferte USB-Treiber (RNDIS) bindet sich in den Geräte-Manager der Windows Systemsteuerung als virtueller Netzwerkadapter ein. Die Kommunikation zwischen der TK-Anlage und dem über USB angeschlossenen PC erfolgt über das TCP-IP Protokoll. Über dieses Protokoll werden auch die Daten für LAN-CAPI übertragen.

Überprüfen der TCP/IP Konfiguration

In den nachfolgend beschriebenen Beispielen wird von der empfohlenen Netzwerkkonfiguration mit automatischer Adressvergabe ausgegangen. Das heißt, dass die LAN-Clients Ihre IP-Adresse per DHCP beziehen (»IP-Adresse automatisch beziehen«) und der DHCP-Server in der TK-Anlage eingeschaltet ist (Grundeinstellung).

Windows 98SE / ME

- Starten Sie das Programm Winipcfg.
Wählen Sie im Startmenü von Windows »Ausführen ...«. Geben Sie »winipcfg« in das Eingabefeld ein und bestätigen Sie Ihre Eingabe mit OK. Betätigen Sie anschließend den Button »Weitere Info«.

The screenshot shows the 'IP-Konfiguration' window with the following settings:

Section	Field	Value
Host-Info	Hostname	VNSLAP-3
	DNS-Server	192.168.1.250
	Knotentyp	Broadcast
	NetBIOS-Bereichs-ID	
	IP-Routing aktiviert	<input type="checkbox"/>
	WINS-Proxy aktiviert	<input type="checkbox"/>
Ethernet Netzwerkkarteninfo	Netzwerkkartenname	FE574B-3Com Megahertz 10/100 LAN PCCard
	Netzwerkkartenadresse	00-00-86-5F-02-BA
	IP-Adresse	192.168.1.50
	Subnet Mask	255.255.255.0
	Standard-Gateway	192.168.1.250
	DHCP-Server	192.168.1.250
	Erster WINS-Server	
	Zweiter WINS-Server	
	IP-Adresse erteilt am	31.07.02 09:54:16
	IP-Adresse gültig bis	31.07.02 10:54:16

Annotations on the right side of the screenshot:

- Aktuelle IP-Adresse der TK-Anlage als DNS-Server.
- Netzwerkadapter auswählen, der mit der TK-Anlage verbunden ist.
- Aktuelle IP-Adresse des Netzwerkadapters (Clients).
- Aktuelle IP-Adresse der TK-Anlage als Gateway und DHCP-Server.

- In der Grundeinstellung der TK-Anlage sind die im Screenshot enthaltenen Werte eingestellt. Die IP Adresse liegt je nach Anzahl der verbundenen Clients (PCs) im Bereich von 192.168.1.50 bis 192.168.1.69. Wenn diese Werte angezeigt werden, sind der Netzwerkadapter und die Windows Netzwerkeinstellungen korrekt konfiguriert. Sollte das Programm »Winipcfg« andere Werte anzeigen, betätigen Sie bitte die Schaltflächen »Alles freigeben« und danach »Alles aktualisieren«.

Zeigt das Programm Winipcfg immer noch andere Daten an, kann dieses folgende Gründe haben:

- Es wurden bereits Änderungen an der Grundeinstellung der TK-Anlage im Konfigurator vorgenommen.
- Die Windows Netzwerkkonfiguration des Clients (PCs) entspricht nicht der Grundeinstellung.
- Die Installation des Netzwerkadapters im Client (PC) ist fehlerhaft oder der Netzwerkadapter ist nicht korrekt mit der TK-Anlage verbunden. Bitte überprüfen Sie Ihre Installation wie in der Bedienungsanleitung der TK-Anlage (Abschnitt Montage und Inbetriebnahme) beschrieben.
- Das TCP/IP Protokoll ist nicht auf dem PC installiert oder hat keine Bindung zu dem mit der TK-Anlage verbundenen Netzwerkadapter.

Windows 2000

- Starten Sie das Programm ipconfig.
Wählen Sie im Startmenü von Windows »Ausführen ...«. Geben Sie »cmd« in das Eingabefeld ein und bestätigen Sie Ihre Eingabe mit OK. Geben Sie »ipconfig/all« ein und bestätigen Sie mit der Entertaste.

```

C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig/all

Windows 2000-IP-Konfiguration

    Hostname . . . . . : PMD-Test-AK
    Primäres DNS-Suffix . . . . . :
    Knotentyp . . . . . : Broadcastadapter
    IP-Routing aktiviert. . . . . : Nein
    WINS-Proxy aktiviert. . . . . : Nein

Ethernetadapter "LAN-Verbindung":

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : 3Com EtherLink XL 10/100 PCI-TX-NIC
    (3C905B-TX)
    Physikalische Adresse . . . . . : 00-A0-24-59-64-43
    DHCP-aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . . . : Ja
    IP-Adresse. . . . . : 192.168.1.50
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.1.250
    DHCP-Server . . . . . : 192.168.1.250
    DNS-Server . . . . . : 192.168.1.250
    Lease erhalten. . . . . : Freitag, 9. August 2002 14:35:04
    Lease läuft ab. . . . . : Freitag, 9. August 2002 15:35:04

C:\>
  
```

- Aktuelle IP-Adresse der TK-Anlage als Gateway, DHCP-Server und DNS-Server.
- Aktuelle IP-Adresse des Netzwerkadapters (Clients).
- Netzwerkadapter auswählen, der mit der TK-Anlage verbunden ist.

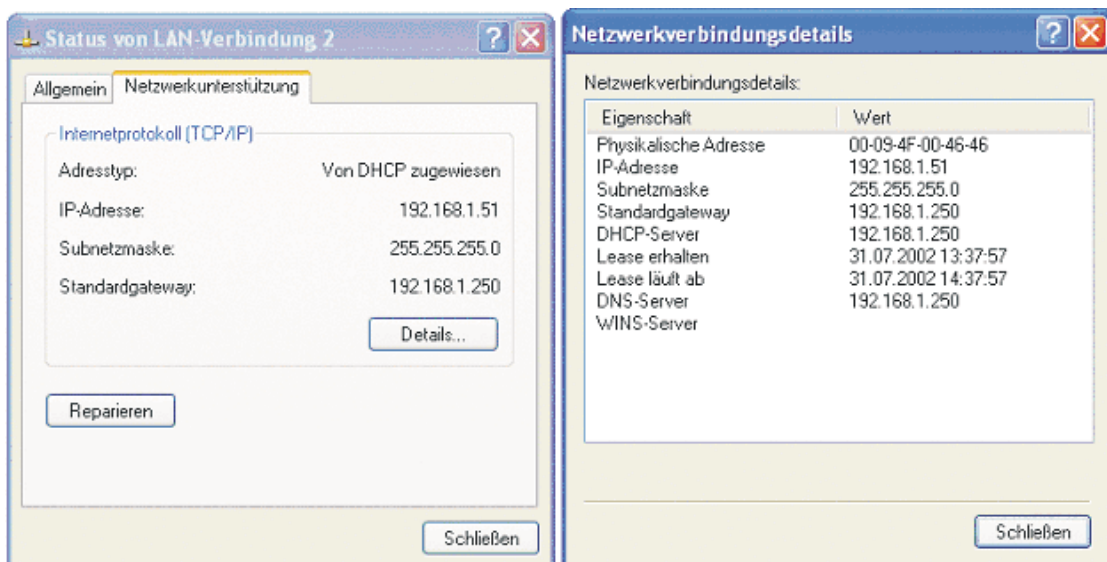
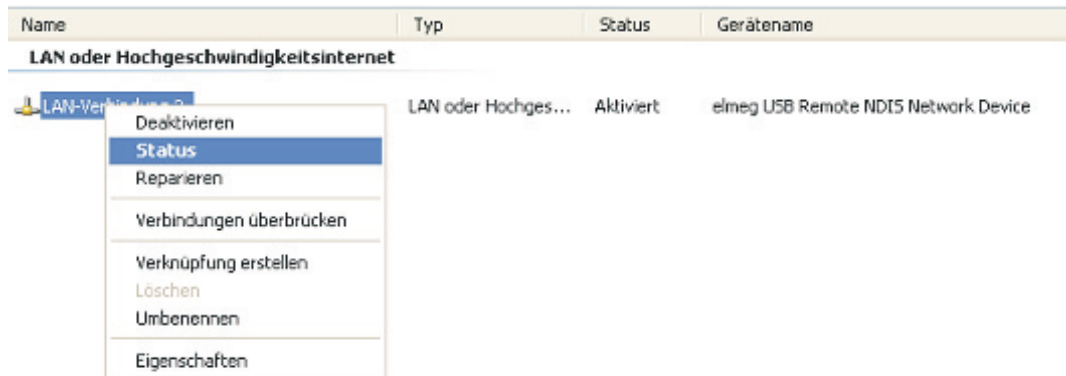
- In der Grundeinstellung der TK-Anlage sind die im Screenshot enthaltenen Werte eingestellt. Die IP Adresse liegt je nach Anzahl der verbundenen Clients (PCs) im Bereich von 192.168.1.50 bis 192.168.1.69. Wenn diese Werte angezeigt werden, sind der Netzwerkadapter und die Windows Netzwerkeinstellungen korrekt konfiguriert.
- Der Wert für die physikalische Adresse ist für jeden Netzwerkadapter verschieden. Die Werte für Lease sind abhängig vom Zeitpunkt des Einschaltens des PCs.

Werden andere Daten angezeigt, kann dieses folgende Gründe haben:

- Es wurden bereits Änderungen an der Grundeinstellung der TK-Anlage im Konfigurator vorgenommen.
- Die Windows Netzwerkkonfiguration des Clients (PCs) entspricht nicht der Grundeinstellung.
- Die Installation des Netzwerkadapters im Client (PC) ist fehlerhaft oder der Netzwerkadapter ist nicht korrekt mit der TK-Anlage verbunden. Bitte überprüfen Sie Ihre Installation wie in der Bedienungsanleitung der TK-Anlage (Abschnitt Montage und Inbetriebnahme) beschrieben.
- Das TCP/IP Protokoll ist nicht auf dem PC installiert oder hat keine Bindung zu dem mit der TK-Anlage verbundenen Netzwerkadapter.

Windows XP

- Öffnen Sie die Windows XP Netzwerkverbindungen. Wählen Sie den mit der TK-Anlage verbundenen Netzwerkadapter mit einem rechten Mausklick aus und betätigen Sie anschließend »Status«.



- In der Grundeinstellung der TK-Anlage sind die im Screenshot enthaltenen Werte eingestellt. Die IP Adresse liegt je nach Anzahl der verbundenen Clients (PCs) im Bereich von 192.168.1.50 bis 192.168.1.69. Wenn diese Werte angezeigt werden, sind der Netzwerkadapter und die Windows Netzwerkeinstellungen korrekt konfiguriert. Sollten andere Werte angezeigt werden, betätigen Sie bitte die Schaltfläche »Reparieren«.
- Der Wert für die physikalische Adresse ist für jeden Netzwerkadapter verschieden. Die Werte für Lease sind abhängig vom Zeitpunkt des Einschaltens des PCs.

Werden immer noch andere Daten angezeigt, kann dieses folgende Gründe haben:

- Es wurden bereits Änderungen an der Grundeinstellung der TK-Anlage im Konfigurator vorgenommen.
- Die Windows Netzwerkkonfiguration des Clients (PCs) entspricht nicht der Grundeinstellung.
- Die Installation des Netzwerkadapters im Client (PC) ist fehlerhaft oder der Netzwerkadapter ist nicht korrekt mit der TK-Anlage verbunden. Bitte überprüfen Sie Ihre Installation wie in der Bedienungsanleitung der TK-Anlage (Abschnitt Montage und Inbetriebnahme) beschrieben.
- Das TCP/IP Protokoll ist nicht auf dem PC installiert oder hat keine Bindung zu dem mit der TK-Anlage verbundenen Netzwerkadapter.

Konfiguration des Internetzuganges an einem PC

Haben Sie bisher eine Internetverbindung über das DFÜ-Netzwerk von Windows genutzt, wurde diese in Form einer »Wählverbindung« (über analog oder ISDN) aufgebaut. Der Beginn und das Ende einer Internetverbindung konnte durch die Programme automatisch eingeleitet werden.

Wenn Sie eine Internetverbindung über den Router der TK-Anlage aufbauen, ist das für jeden PC eine normale Netzwerkverbindung. Soll ein PC eine Internetverbindung nutzen, wird dieses dem Router des Netzes mitgeteilt, der als Gateway die Verbindung zu anderen Netzen herstellt. Der Router, in unserem Beispiel die TK-Anlage, baut dann eine Verbindung zu einem der konfigurierten Internet-Service-Provider auf. Diese Verbindung wird gemäß der Konfigurierung der TK-Anlage automatisch auf- oder abgebaut. Die Konfigurierung der Internet-Service-Provider erfolgt über den Konfigurator der TK-Anlage.

Einstellungen im Internet Explorer / Internetoptionen von Windows

Die folgende Beschreibung zeigt für die unterschiedlichen Betriebssysteme die Einstellungen von Internet-Verbindungen. Gehen Sie für Ihr Betriebssystem wie unten beschrieben vor und aktivieren Sie die entsprechende Option.

Windows 98SE:

Startmenü - Einstellungen - Systemsteuerung - Internetoptionen - Verbindungen

Windows ME:

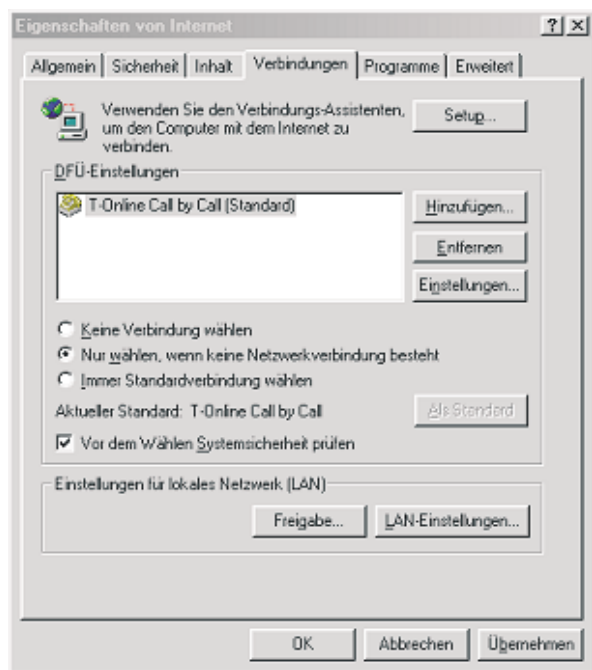
Startmenü - Einstellungen - Systemsteuerung - Internetoptionen - Verbindungen

Windows 2000:

Startmenü - Einstellungen - Systemsteuerung - Internetoptionen - Verbindungen

Windows XP:

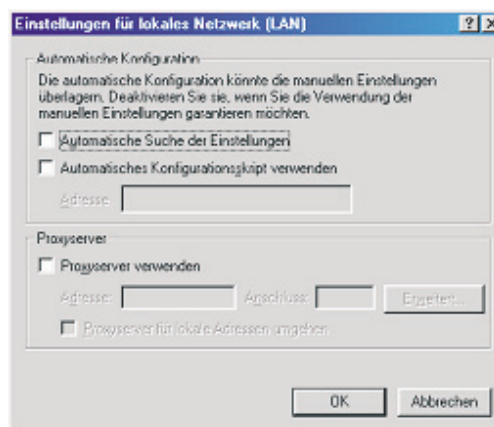
Startmenü - Einstellungen - Systemsteuerung - Netzwerk- und Internetverbindungen - Internetoptionen - Verbindungen



Auf dem Client eingerichtete DFÜ-Verbindungen werden, angezeigt. Sie werden für den Internetzugang mit der TK-Anlage nicht benötigt.

Aktivieren Sie hier die Option »Keine Verbindung wählen«. Sie können zusätzlich zur TK-Anlage auch über andere Geräte das Internet anwählen. Dazu ist die Option »Nur wählen, wenn keine Netzwerkverbindung besteht« erforderlich.

Unter »LAN-Einstellungen« sind keine Einstellungen erforderlich.



Firewall-Filter konfigurieren

Filter können Sie nur im »Professional Configurator« einrichten.

Benutzerdefinierte Filter für den in die TK-Anlage integrierten Router mit Packet Filter Firewall lassen sich unter »Netzwerk« »Filter« konfigurieren.

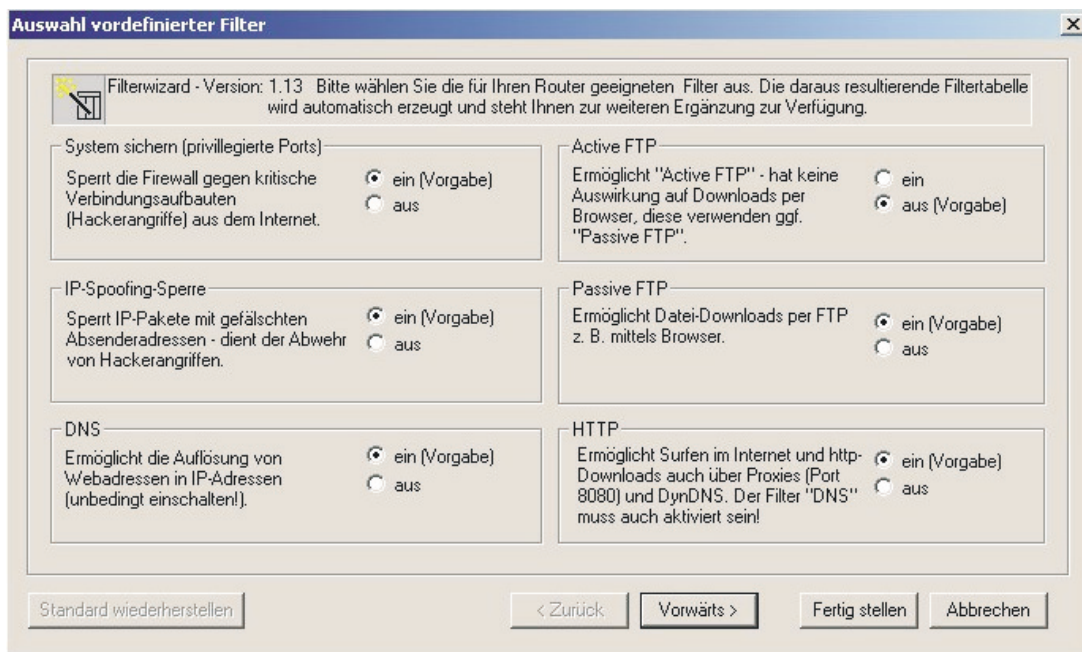
Wir empfehlen die Filter der Firewall mit Hilfe des Filter Wizard zu erstellen, um die anwendungsgerechte Konfiguration der Firewall sicher zu stellen. Damit können Datenpakete aus dem Internet, die möglicherweise Verbindungsgebühren verursachen, abgewehrt werden. Sonst kann z. B. die Funktion des »automatischer Verbindungsabbau« nicht in jedem Fall gewährleistet werden. Es kann vorkommen, dass aus dem Internet ein Portscan (meist Vorstufe eines Hackerangriffes) stattfindet, der von der Firewall der TK-Anlage mit »Ablehnungspaketen« beantwortet wird. Dabei kann aber trotzdem Datenverkehr erzeugt werden, der einen automatischen Verbindungsabbau verhindert.

Die vorbereiteten Filter der Filter-Wizard sind nach besten Wissen gestaltet. Es kann keine Gewähr für die Funktion der Filter übernommen werden. Der Einsatz einer Firewall sollte unbedingt durch die Verwendung von Virenschanner-Software auf allen PCs begleitet werden! Firewall und Virenschanner decken unterschiedliche Bereiche der Datensicherheit ab und können sich ideal ergänzen, nie aber ersetzen.

Zur Einrichtung selbstdefinierter Filter betätigen Sie die Schaltfläche »Neu ...« oder ändern Sie einen existierenden Eintrag in der Filterliste durch Doppelklick des gewünschten Eintrages. Eine Erläuterung zur Funktion der Filter erhalten Sie, wenn sie den Button »Hilfe« betätigen.

Grundsätzliches über die Konfiguration der Firewall

Um die Firewall zu konfigurieren, sind genaue Kenntnisse der IP-Protokollfamilie unbedingt notwendig. Sollten Sie diese Kenntnisse nicht besitzen, empfehlen wir die Verwendung des Filter Wizards.



Die Firewall funktioniert wie eine Kette von Regeln, durch die jedes IP-Paket geleitet wird. Trifft eine Regel auf ein Paket zu, wird die mit dieser Regel verbundene Aktion ausgeführt (Paket akzeptieren, ablehnen oder portmap ausführen). Alle Regeln finden Sie in der Liste unter Netzwerk/ Filter. Bitte beachten Sie, dass bei bestimmten Konfigurationen die Reihenfolge der Filter für die Funktion der Firewall eine entscheidende Bedeutung haben kann. Aus diesem Grund können Sie nach Markieren einer Filterregel die Reihenfolge der Regeln in der Tabelle mit den Schaltflächen [nach oben] und [nach unten] beeinflussen.

Trifft keine Regel auf das IP-Paket zu, so entscheidet eine übergreifende, grundsätzliche Regel am Ende der Kette über die durchzuführende Aktion (Verhalten nach letzter Filterregel).

Zu Beginn der Filterkonfiguration müssen Sie daher diese übergreifende Regel, das Verhalten ..., festlegen. Sie können hierbei zwischen »Akzeptieren« oder »Verwerfen« auswählen.

Die allgemein als sicher bezeichnete Vorgehensweise ist die Ablehnung des Paketes, da bei einer solchen Konfiguration nur die Pakete zulässig sind, für die eine explizite (und damit wissentlich eingerichtete) Regel existiert.

Für die Definition der Filter ist zu berücksichtigen, dass auf allen LAN-Ports (LAN1, LAN2, dem USB - Anschluss) alle Pakete erlaubt sind. Daher müssen keine Filterregeln für das Passieren von IP-Paketen aus dem LAN in Richtung TK-Anlage / Router und für deren »Rückweg« erstellt werden.

Um für die Erstellung von Filtern eine Abstraktion zu erreichen, sind vier Platzhalter vorgesehen:

LAN_ADDR	Steht für die LAN-Adresse des Routers, bezogen auf die Defaultkonfiguration also 192.168.1.250 mit der Netzmaske 255.255.255.0 (192.168.1.250 / 24).
LAN_NET	Steht für alle LAN-Adressen, bezogen auf die Defaultkonfiguration also 192.168.1.0 mit der Netzmaske 255.255.255.0 (192.168.1.0 / 24).
WAN_ADDR	Steht für die WAN-Adresse des Routers, die bei Verwendung von PPPoE oder PPP dynamisch vom ISP zugewiesen wird. Durch die dynamische Zuweisung wird bei jeder Herstellung der Verbindung mit dem Internet eine IP-Adresse aus dem Volumen Ihres ISPs für den WAN-Port vergeben. Die WAN-Adresse kann in diesen Fällen während der Konfiguration nicht als absoluter Wert für die Filterkonfiguration eingegeben werden. PPPoE ist z. B. für T-DSL erforderlich, PPP wird bei Verbindungen in das Internet per ISDN-Einwahl verwendet. Haben Sie eine feste öffentliche IP-Adresse für Ihren Internetzugang von Ihrem Provider zugewiesen bekommen, wird diese für WAN_ADDR verwendet. Nach Zuweisung der IP-Adresse auf dem WAN-Port (bzw. ISDN-Kanal) wird die Firewall automatisch entsprechend der definierten Regeln angepasst.
WAN_NET	Steht für alle WAN-Adressen, die sich im gleichen IP-Subnetz befinden wie der WAN-Port. Derzeit findet dieser Parameter keine Anwendung, ggf. spielt dieser Platzhalter bei künftigen Software-Updates eine Rolle.

Folgende Parameter können konfiguriert werden:

Name des Filters	Jedem Filter muss ein eindeutiger Name zugewiesen werden. Wählen Sie die Namen so, dass die jeweilige Funktion des Filter eindeutig bezeichnet wird, so können Sie bei späterer Änderung leichter den Überblick bewahren.
Aktion	Ausgewählt werden können die Optionen allow, deny, discard und portmap. Die Wahl von »allow« lässt alle Pakete passieren, die den Parametern des jeweiligen Filters entsprechen. Wird »deny« ausgewählt, so werden entsprechende IP-Pakete verworfen und der Absender informiert. »discard« sorgt dafür, dass das Paket verworfen wird, ohne den Absender zu informieren. Die Option »portmap« erlaubt das gezielte Weiterleiten von Paketen der Protokolle TCP und UDP an die IP-Adresse eines PCs im LAN.
TCP Flag	Soll eine TCP-Verbindung hergestellt werden (z. B. für den Download von Dateien), so werden für den Verbindungsaufbau in den hieran beteiligten Paketen bestimmte Bitmuster gesetzt, die TCP-Flags. Die Auswahl »aufbauende Verbindung« steht für das SYN-Flag, die Auswahl »aufgebaute Verbindung« steht für das »Established Flag«
Protokolle	Als Protokolle sind UDP, TCP, ICMP und »alle Protokolle« wählbar. Die Wahl des Protokolls beeinflusst ggf. weitere Optionen, da z. B. für UDP keine TCP-Flags zur Verfügung stehen und für ICMP kein Port, dafür aber bestimmte Protokollarten.
Interface	Hier definieren Sie die Schnittstelle, für den entsprechenden Filter. Gegenwärtig wird in den meisten Fällen die Einstellung »WAN« sinnvoll sein, da auf den internen Schnittstellen alle Pakete zulässig sind.
Connection	In diesem Feld wird die Richtung der IP-Pakete festgelegt, für die der konfigurierte Filter gültig ist. Mögliche Parameter: in, out und in/out (bidirektional).

Quelladressdefinition	In diesem Feld legen Sie die Ursprungsadresse der IP-Pakete fest, für die dieser Filter gültig ist. Bitte beachten Sie die durch Platzhalter möglichen Abstraktionen.
Zieladressdefinition	In diesem Feld legen Sie die Zieladresse der IP-Pakete fest, für die dieser Filter gültig ist. Bitte beachten Sie die durch Platzhalter möglichen Abstraktionen.
Warnhinweis für Port-Protokollzugehörigkeit	Wird versucht, in das Feld für den TCP-Port einen unbekannt Namen einzutragen, so erscheint eine Warnmeldung. Sollte diese als störend empfunden werden, so kann die Meldung durch Entfernen des entsprechenden Häkchens unterdrückt werden.

Beispiel zur Konfiguration eines Filters für die Freigabe der Firewall für das Web-Browsen

Zuerst wird das Verhalten nach letzter Filterregel auf »Verwerfen« eingestellt.

Um Seiten des World Wide Web darstellen zu können, müssen die IP-Pakete zweier Dienste durch die Firewall geleitet werden: DNS zur Namensauflösung und der »html-Datenstrom«. Wird eine URL in den Web-Browser eingegeben, so löst der Browser per DNS-Abfrage den Klarnamen (z. B. www.Telekom.de) in eine IP-Adresse auf (in diesem Beispiel 217.160.73.88) auf. Danach stellt der Browser zu dieser IP-Adresse per TCP/IP mindestens eine Verbindung her. Daraus leitet sich folgende Filterkonfiguration ab:

Für DNS (Protokollname: domain) ist das UDP- und das TCP-Protokoll auf den Ziel-Port 53 eines beliebigen DNS-Servers von jedem unprivilegierten Port freizugeben, entsprechendes gilt für den Rückweg.

Für http-Requests ist für das TCP-Protokoll über das WAN-Interface von unprivilegierten Ports der Zugriff auf beliebige Zieladressen für den Port 80 zu ermöglichen. Der Rückweg für Antwortpakete muss entsprechend freigegeben werden: Von beliebigen IP-Adressen aus dem Internet (0.0.0.0 / 0) von Port 80 auf unprivilegierte Ports der WAN-Adresse der TK-Anlage.

Beispiel zur Konfiguration eines Portmapping – Eintrages für die Firewall für das ssh – Protokoll

Das ssh Protokoll (secure shell) wird u. a. verwendet, um Webserver zu administrieren oder um VPN – Tunnel zu realisieren. Per ssh – Protokoll werden die Daten verschlüsselt übertragen (das ist für die Konfiguration der Firewall allerdings ohne Belang). Üblicherweise wird der Port 22 des Protokolls TCP verwendet. Im Beispiel hat der Webserver in Ihrem LAN die IP-Adresse 192.168.1.42 fest zugeordnet. Für diesen Webserver in Ihrem LAN soll der Administrations-Zugriff per ssh aus dem Internet ermöglicht werden. Beachten Sie bitte, dass Sie äquivalente Filter für den Port 80 benötigen, wenn die Inhalte des Webservers aus dem Internet zugänglich sein sollen

Basierend auf diesen Informationen müssen bei einem voreingestellten »Verhalten nach letzter Filterregel à Discard« drei Regeln für die Firewall erstellt werden:

- ssh_MAP: Dieser Filter leitet eintreffende Pakete von beliebigen IP-Adressen und unprivilegierten Ports auf die internetseitige IP-Adresse des Routerteils der TK-Anlage weiter an den Rechner mit der IP-Adresse 192.168.1.42, der Port 22 wird beibehalten.
- ssh_WAN_in: Dieser Filter erlaubt eintreffenden Paketen von beliebigen IP-Adressen und unprivilegierten Ports auf die internetseitige IP-Adresse des Routerteils der TK-Anlage.
- ssh_WAN_out: Dieser Filter erlaubt ausgehenden Paketen von Port 22 das Passieren des WAN-Interfaces (das ist der Anschluss des DSL-Modems oder die ISDN-Wählverbindung in das Internet) zu beliebigen IP-Adressen und unprivilegierten Ports.

Filtername	TCP-Flag	Interface	Aktion	Protokoll	Connection	Quell-IP	Quell-Port	Ziel-IP	Ziel-Port
Netbios-Sperre	keines	WAN	discard	UDP	out	0.0.0.0/0	137-139	0.0.0.0/0	any
ssh_portmap	keines	WAN	portmap	TCP	in	0.0.0.0/0	22	192.168.1.42	22
ssh_WAN_in	keines	WAN	allow	TCP	in	0.0.0.0/0	any	WAN_ADDR	22
ssh_WAN_out	keines	WAN	allow	TCP	out	WAN_ADDR	22	0.0.0.0/0	any

Der PC in Ihrem LAN mit der IP-Adresse 192.168.1.42 ist damit auf dem Port 22/TCP in keiner Weise durch die Firewall in Ihrer TK-Anlage geschützt! Die Zugriffsmöglichkeiten können ggf. eingegrenzt werden, wenn die Zugriffe immer von einem Internetanschluss mit fester IP-Adresse (z. B. T-Interconnect) ausgeführt werden. In diesem Fall sollten die Einträge, die »0.0.0.0/0« enthalten, auf die bekannte IP-Adresse der Gegenstelle angepasst werden (0.0.0.0/0 ist ein Stellvertreter aller IP-Adressen).

Wenn Sie eine Kombination aus Filtern, die per Filter Wizard erstellt wurden und eigenen Filtern bzw. Portmap-Einträgen verwenden wollen, prüfen Sie bitte die Reihenfolge der Regeln in der Tabelle (die Reihenfolge kann mit den Schaltflächen »nach oben« und »nach unten« verändert werden). Im Filter Wizard wird der Filter »System sichern« angeboten, der alle Pakete sperrt, die an sog. privilegierte Ports gerichtet sind. Dieser Filter würde der im Beispiel konfigurierten Funktionalität entgegen stehen, da der ssh-Port (22) ein privilegierter Port ist. Es wird ausdrücklich empfohlen, alle nicht benötigten privilegierten Ports zu sperren, daher kann es sinnvoll sein, den per Filter Wizard konfigurierten Filter entsprechend angepasst oder an passender Position in der Tabelle zu verwenden.

Wenn Sie nicht wissen, welche Ports für bestimmte Applikationen oder zum Erreichen bestimmter Teilnahmeprivilegien an Tauschnetzwerken mittels Portmapping vom Router Ihrer TK-Anlage auf den LAN-PC geleitet werden müssen, so geben Sie in eine Internet-Suchmaschine den Namen der Applikation sowie die Begriffe »port« und »firewall« ein, meist finden Sie so leicht Konfigurationshinweise. Sie können mit einer Portmap-Regel einen einzelnen Port oder Portbereiche weiterleiten (z. B. 4661-4665).

Filter-Wizard

Die Firewall wird so konfiguriert, dass alle Datenpakete, für die keine explizite Regel (Filter) existiert, die das Passieren des Paketes erlauben würde, verworfen werden. Diese Vorgehensweise führt dazu, dass die Konfiguration der Firewall etwas aufwändiger ist, allerdings ist weniger wahrscheinlich, dass »vergessen« wird, Paketen das Passieren der Firewall zu untersagen.

Einige Filter enthalten Regeln zum Ablehnen von Paketen, die bei der gewählten grundsätzlichen Konfiguration der Firewall eigentlich nicht erforderlich wären, denn die Firewall lehnt nach der Konfiguration per Wizard alle nicht per Filter freigegebenen Pakete ab. Die o. g. Ablehnungsregeln sind trotzdem enthalten, um bei bestimmten Angriffen die für den Angriff verwendeten Pakete möglichst früh zu verwerfen und nicht durch die gesamte Kette von Filterregeln laufen lassen zu müssen, was die Performance der Firewall im Falle eines Angriffs erhöht.

Beispiele für vordefinierte Filter im Filter-Wizard

Die Hilfe zu den verschiedenen Filtern des Filter-Wizard finden Sie in der Datei »Filter_Info.txt« im Installationsverzeichnis der WIN-Tools (z.B. »C:\Programme\elmeg WIN-Tools\WIN-Tools V6.02\filterinfo«) oder durch betätigen des Buttons »Hilfe«.

System sichern

Dieser Filter sperrt die Firewall gegen Verbindungsaufbauten auf den privilegierten Ports (0 ... 1023) für TCP und UDP. Über die privilegierten Ports werden die meisten relevanten Datendienste angeboten (Namensauflösung, Dateitransfer, etc.).

IP-Spoofing-Sperre

Dieser Filter sperrt die Firewall gegen das Vortäuschen von Paketen »auf der falschen Seite« der Firewall. So werden Datenpakete, die anhand ihrer IP-Adresse eindeutig in das LAN gehören würden, von einem Angreifer aus dem Internet jedoch auf den Anschluss für das DSL-Modem geleitet werden ignoriert (entsprechendes gilt für ISDN-Verbindungen in das Internet).

DNS-Filter

Dieser Filter ermöglicht die Namensauflösung (Zuordnung von IP-Adressen zu URLs), indem sowohl UDP als auch TCP-Pakete gehend auf Port 53 und kommend von Port 53 freigegeben werden. Durch die Freigabe von TCP werden auch längere Antworten und Zonentransfers ermöglicht. Wird dieser Filter abgeschaltet, so können keine DNS-Anfragen die Firewall passieren!

Active FTP - Filter

Dieser Filter ermöglicht zusammen mit einem entsprechenden Softwaremodul in der Firewall active FTP. Active FTP unterscheidet sich von passiver FTP dadurch, dass der FTP-Server auf Anforderung der Clients eine Verbindung für den Datentransfer aufbaut (das gilt sowohl für die Antwort auf den FTP-Befehl »ls« als auch für den Dateitransfer selbst). Problematisch ist dabei, dass der Verbindungsaufbau vom FTP-Server auf einen beliebigen, unprivilegierten Port des FTP-Clients erfolgt und daher ein sehr großer Bereich der Firewall freigegeben werden muss.

Gehende Verbindungen auf die Ports 20 und 21 sowie kommende Verbindungen von diesen Ports auf unprivilegierte Ports werden freigegeben.

Passive FTP - Filter

Dieser Filter ermöglicht den Dateitransfer per FTP, wobei die Verbindung immer vom FTP-Client aufgebaut wird. Gehende Verbindungen auf den Port 21 sowie kommende Verbindungen von diesem Port auf unprivilegierte Ports werden freigegeben.

HTTP - Filter

Dieser Filter ermöglicht das Webbrowsen, in dem Pakete auf die Ports 80 und 8080 (für die Verwendung von http-Proxies) für gehende Verbindungen und von diesen Ports kommende Pakete auf unprivilegierte Ports freigegeben werden.

HTTPS - Filter

Dieser Filter ermöglicht das gesicherte Webbrowsen, in dem Pakete auf den Port 443 für gehende Verbindungen und von diesem Port kommende Pakete auf unprivilegierte Ports freigegeben werden. Das Protokoll https wird oft für Homebanking und Onlineshopping eingesetzt, es werden http-Verbindungen für die Übertragung von durch Verschlüsselung geschützten Paketen verwendet.

HBCI - Filter

Dieser Filter ermöglicht den Einsatz von HBCI für das Homebanking, in dem Pakete auf den Port 3000 für gehende Verbindungen und von diesem Port kommende Pakete auf unprivilegierte Ports freigegeben werden.

E-Mail Senden - Filter

Dieser Filter ermöglicht das Übertragen von emails per SMTP (= email senden), in dem Pakete auf den Port 25 für gehende Verbindungen und von diesem Port kommende Pakete auf unprivilegierte Ports freigegeben werden.

E-Mail Empfang - Filter

Dieser Filter ermöglicht das Übertragen von emails per POP (= email empfangen), in dem Pakete auf den Port 110 für gehende Verbindungen und von diesem Port kommende Pakete auf unprivilegierte Ports freigegeben werden.

ICMP(all) - Filter

Dieser Filter ermöglicht die Verwendung des Dienstprogrammes »ping«, um z. B. die Erreichbarkeit von Rechnern im Internet und Übertragungsdauer von IP-Paketen zu diesen Rechnern zu messen. Hilfreich ist das z. B. bei Internet-Spielen, um den am schnellsten antwortenden Server zu finden. Wird dieser Filter eingeschaltet, so kann auch die TK-Anlage per »ping« erreicht werden, allerdings kein Rechner im LAN »hinter« der TK-Anlage, da diese durch NAT geschützt sind. Dieser Filter schaltet alle ICMP-Protokolle frei, nicht nur die für »ping« verwendeten. Ggf. können Sie diesen Filter noch weiter eingrenzen, in dem nur die ICMP-Protokolle 0 und 8 freigegeben werden (echo-request, echo-reply). Sollten Sie diesen Filter nicht einschalten, so erhöhen Sie die Sicherheit weiter, da die Firewall dann nicht ohne weiteres von einem Portscan-Programm per einfachem »ping« gefunden werden kann.

SSH - Filter

Dieser Filter ermöglicht die Verwendung des Dienstprogrammes 443 auf Rechner im Internet, in dem Pakete auf den Port xxx für gehende Verbindungen und von diesem Port kommende Pakete auf unprivilegierte Ports freigegeben werden.

TELNET - Filter

Dieser Filter ermöglicht die Verwendung des Dienstprogrammes telnet auf Rechner im Internet, in dem Pakete auf den Port 23 für gehende Verbindungen und von diesem Port kommende Pakete auf unprivilegierte Ports freigegeben werden.

P2P - Filter

Dieser Filter ermöglicht die Verwendung von Peer to Peer (P2P) Filesharing Software. Um ein einziges Filter für die verschiedensten P2P Systeme anbieten zu können, wurden folgende Portfreigaben vorgesehen:

Kommende Pakete:

- von Port 80 auf unprivilegierte Ports
- von Port 1214 auf unprivilegierte Ports

- von unprivilegierten Ports auf Port 80
- von unprivilegierten Ports auf unprivilegierte Ports

Gehende Pakete:

- von unprivilegierten Ports auf Port 80
- von unprivilegierten Ports auf Port 1214
- von unprivilegierten Ports auf Port 4661
- von unprivilegierten Ports auf unprivilegierte Ports. Dieser Filter öffnet die Firewall sehr weit!

Gaming - Filter

- Dieser Filter ermöglicht die Verwendung von Internet-Spielen. Es wurden folgende Portfreigaben vorgesehen:

Kommende Pakete:

- von Port 7002 auf unprivilegierte Ports für TCP von unprivilegierten Ports auf unprivilegierte Ports für UDP

Gehende Pakete:

- von Port 7002 auf unprivilegierte Ports für TCP von unprivilegierten Ports auf unprivilegierte Ports für UDP

Realplayer - Filter

Dieser Filter ermöglicht die Verwendung des Realplayer für das Streaming von Audio und Video. Es wurden folgende Portfreigaben vorgesehen:

Kommende Pakete:

- von Port 554 auf unprivilegierte Ports für TCP
- von Port 7002 auf unprivilegierte Ports für TCP
- von unprivilegierten Ports auf Ports 6970 - 7170 für UDP

Gehende Pakete:

- von unprivilegierten Ports auf Port 554 für TCP
- von unprivilegierten Ports auf Port 7070 für TCP

Mediaplayer - Filter

Dieser Filter ermöglicht die Verwendung des Realplayer für das Streaming von Audio und Video. Es wurden folgende Portfreigaben vorgesehen:

Kommende Pakete:

- von Port 1755 auf unprivilegierte Ports für UDP

- von Port 1755 auf unprivilegierte Ports für TCP

Gehende Pakete:

- von unprivilegierten Ports auf Port 1755 für UDP
- von unprivilegierten Ports auf Port 1755 für TCP

Filter Update

Da es erforderlich sein kann, die Konfiguration der Firewall mit einem Update zu versehen, um ggf. neue Applikationen zu ermöglichen oder bestimmte Hacker-Angriffe aus dem Internet abwehren zu können, arbeitet der Filter Wizard mit einer Beschreibungsdatei, die Sie leicht updaten können, ohne zwangsläufig ein Softwareupdate in die TK-Anlage oder den PC einspielen zu müssen.

Bitte prüfen Sie in regelmäßigen Abständen die Verfügbarkeit neuer Beschreibungsdateien (Namen: »filterwizardtab.txt« und »Filter_Info.txt«) auf <http://www.Funkwerk-ec.com>. Beide Dateien gehören zusammen: Die Datei »filterwizardtab.txt« steuert das Verhalten des Filter Wizard, die Datei »Filter_Info.txt« enthält in leicht lesbarer Form eine detaillierte Beschreibung der im Filter Wizard zur Verfügung stehenden Optionen (siehe nachfolgende Tipps).

Sollten Sie dort eine neuere Version der Beschreibungsdateien finden, so können Sie diese auf Ihren PC herunterladen und dabei die vorhandenen Dateien überschreiben. Sie finden die Beschreibungsdateien im Unterverzeichnis »filterinfo«, das sich unter dem Installationsverzeichnis der Konfigurationssoftware Ihrer TK-Anlage befindet, z. B. »C:\Programme\elmeg WIN-Tools\WIN-Tools V6.02\filterinfo« - hier finden Sie u. a. die Dateien »filterwizardtab.txt« und »Filter_Info.txt«.

Wenn Sie anschliessend den Filter Wizard aus der Konfigurationssoftware erneut starten und die Schaltfläche »Standard wiederherstellen« betätigen, stehen die neuen Filter sofort zur Verfügung.

Sollte die Schaltfläche »Standard wiederherstellen« grau hinterlegt sein, so ändern Sie eine der vorgegebenen Filtereinstellungen (einen beliebigen Filter ein- oder ausschalten), dann wird die Schaltfläche aktiviert. Im Konfigurationszweig »Netzwerk«, »Filter« finden Sie eine Schaltfläche »Hilfe«. Der durch betätigen dieser Schaltfläche angezeigte Text wird direkt der Datei »Filter_Info.txt« entnommen, somit ist auch die Hilfe für die Filter des Filter Wizard ohne Softwareupdate aktualisierbar.

Stichwortverzeichnis

A

Adressvergabe per DHCP	9
Automatischer Internetzugang	4

C

CAPI im LAN	7
CE-Zeichen	2

D

DHCP-Server	2,5
Direkte Verbindung (DHCP)	3
DNS-Proxy.	5
DNS-Server	5
Dynamic DNS	5
Dynamik-ISDN	4
Dynamik-ISDN für gehende Rufe.	5

E

Einstellungen im Internet Explorer	20
Einwahl ins LAN	2

F

Fallback	4
Filter-Wizard	24
Firewall.	6
Firewall-Filter konfigurieren.	21

G

Grundeinstellung	3
----------------------------	---

I

Internetoptionen von Windows	20
Internet-Verbindungen	1
Internetzugang an einem PC konfigurieren	20
IP-Adressen	3
IP-Adressvergabe	2

K

Konfiguration des Internetzuges an einem PC	20
Konfigurationsbeispiele	9
Konfigurieren der Firewall-Filter	21
Konformitätserklärung	2

L

LAN-CAPI	7
LAN-Clients überprüfen	16

LAN-TAPI.	7
LED Einstellungen	8

N

NAT	6
Netzwerk	
gemischte Adressvergabe	14
mit DHCP Adressvergabe	10
ohne DHCP Adressvergabe	11

P

Packet Filter Firewall	6
Portmapping	6

R

RAS.	2
RAS Callback:	2
RAS-Server	7
Router	1
Routersteuerung	7

S

Short Hold.	4
Speedmanager.	4
Sperren des Internetzuges	7
Statusanzeige CAPI / TAPI i.	8
Subnetzmasken	3

T

TAPI im LAN	7
TCP/IP Konfiguration überprüfen	17
Windows 2000	18
Windows 98SE / ME	17
Windows XP.	19
Tunneling	2

U

Überprüfen der LAN-Clients	16
--------------------------------------	----

V

Verbindungstest	7
---------------------------	---

W

Windows-Betriebssystem	12
----------------------------------	----

Z

Zeitgesteuerte Routersperre	7
---------------------------------------	---

Reparaturservice

Tonfunk GmbH
Reparaturservice
Unternehmenspark 2 / Halle D
Woltorfer Str. 77
31224 Peine

Endkunden-Hotline
0900 1510 110
pro Minute 0,62 EURO

Mo. - Fr.
08.00 Uhr bis 17.00 Uhr

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
<http://www.funkwerk-ec.com>

Änderungen vorbehalten

Ausgabe 1

5116 000000.0

300905