LANCOM™ Referenzhandbuch

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52070 Aachen

Deutschland

www.lancom.de

Würselen, July 2003

02A/0703

Ein Wort vorab

Benutzerhandbuch und *LANCOM*-Referenzhandbuch

Die Dokumentation Ihres Gerätes besteht aus mehreren Teilen: Dem Benutzerhandbuch und dem *LANCOM*-Referenzhandbuch.

Sie lesen derzeit das Referenzhandbuch. Es ergänzt das Benutzerhandbuch zu Ihrem Gerät um Themen, die übergreifend für mehrere *LANCOM* gelten. Dazu gehören beispielsweise:

- Konfiguration und Management (*LANtools*, *WEBconfig*, Fernkonfiguration)
- Erweiterte Sicherheits- und Firewalleinstellungen
- Server-Dienste (DHCP, DNS, NTP, Gebührenmanagement)
- Quality-of-Service-, Routing- und WAN-Funktionen

Gültigkeit

Das vorliegende Referenzhandbuch gilt für alle *LANCOM*-Router und Access-Points mit einem Firmwarestand Version 2.90 oder besser.

An der Erstellung dieser Dokumentation …

… haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres *LANCOM* Produktes anzubieten.

Sollten Sie dennoch einen Fehler finden, oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an:

info@lancom.de

Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.de rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' unter 'Know-how' viele Antworten auf „häufig gestellte Fragen". Darüber hinaus bietet Ihnen die Wissensdatenbank (KnowledgeBase) einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Dokumentation stehen für Sie jederzeit zum Download bereit.

Außerdem steht Ihnen der LANCOM Systems-Support zur Verfügung. Telefonnummern und Kontaktadressen des LANCOM Systems-Supports finden Sie in einem separaten Beileger oder auf der LANCOM Systems-Homepage.

Hinweis-Symbole	
	Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.
	Wichtiger Hinweis, der beachtet werden sollte.
	Zusätzliche Informationen, deren Beachtung hilfreich sein kann aber nicht erforderlich ist.

Spezielle Formatierungen im Fließtext	
Fett	Menübefehle, Befehlsknöpfe (Buttons) oder Eingabefelder
Code	Ein- und Ausgaben im Konsolenmodus
<Wert>	Stellvertreter für einen konkreten Wert
Kursiv	Hinweise und Produktnamen

DE

Inhalt

DE

DE

DE

1 Konfiguration und Management

In diesem Kapitel geben wir Ihnen einen Überblick, mit welchen Mitteln und über welche Wege Sie auf das Gerät zugreifen können, um erweiterte Einstellungen vorzunehmen. Sie finden Beschreibungen zu folgenden Themen:

- Konfigurationstools
- Kontroll- und Diagnosefunktionen von Gerät und Software
- Sicherung und Wiederherstellung kompletter Konfigurationen
- Installation neuer Firmware im Gerät

1.1 Mittel und Wege für die Konfiguration

LANCOM sind flexible Geräte, die verschiedene Mittel (sprich Software) und Wege (in Form von Kommunikationszugängen) für die Konfiguration unterstützen. Zunächst der Blick auf die möglichen Wege.

Einen *LANCOM* können Sie über bis zu drei verschiedene Zugänge erreichen (je nach verfügbaren Anschlüssen):

- über das angeschlossene Netzwerk (sowohl LAN als auch WAN – Inband)
- über die Konfigurations-Schnittstelle (Config-Schnittstelle) des Routers (auch Outband genannt)
- Fernkonfiguration über den ISDN-Anschluss

Was unterscheidet nun diese drei Wege?

Zum einen die Verfügbarkeit: Die Konfiguration über Outband ist immer verfügbar. Die Inband-Konfiguration ist jedoch z.B. nicht mehr möglich, wenn das übertragende Netzwerk gestört ist. Auch die Fernkonfiguration ist abhängig von einer ISDN-Verbindung.

Zum anderen die Anforderungen an zusätzliche Hard- und Software: Die Inband-Konfiguration benötigt einen der ohnehin vorhandenen Rechner im LAN oder WAN und nur noch eine geeignete Software, beispielsweise *LANconfig* oder *WEBconfig* (vgl. folgender Abschnitt). Die Outband-Konfiguration braucht zusätzlich zur Konfigurationssoftware noch einen Rechner mit serieller Schnittstelle. Für die ISDN-Fernkonfiguration sind die Voraussetzungen am umfangreichsten: Neben einem ISDN-Anschluss am

DE

LANCOM wird im Konfigurations-PC ein ISDN-Adapter oder Zugriff über *LANCAPI* auf einen weiteren *LANCOM* mit ISDN-Schnittstelle benötigt.

1.2 Software zur Konfiguration

Die Situationen, in denen konfiguriert wird, unterscheiden sich – aber auch die persönlichen Ansprüche und Vorlieben der Ausführenden. *LANCOM*-Router verfügen daher über ein breites Angebot von Konfigurationssoftware:

- ***LANconfig*** – menügeführt, übersichtlich und einfach lassen sich nahezu alle Parameter eines *LANCOM* einstellen. Unterstützt Outband-, Inband- und Fernkonfiguration, auch für mehrere Geräte gleichzeitig.
- ***WEBconfig*** – diese Software ist fest eingebaut im Router. Auf dem Konfigurationsrechner wird nur ein Web-Browser vorausgesetzt. *WEBconfig* ist dadurch betriebssystemunabhängig. Unterstützt werden Inband- und Fernkonfiguration.
- **SNMP** – geräteunabhängige Programme zum Management von IP-Netzwerken basieren üblicherweise auf dem Protokoll SNMP. Über SNMP können Sie auf *LANCOM* inband und mittels Fernkonfiguration zugreifen.
- **Terminalprogramm, Telnet** – ein *LANCOM* kann mit einem Terminalprogramm über die Config-Schnittstelle (z.B. HyperTerminal) oder innerhalb eines IP-Netzwerks (z.B. Telnet) konfiguriert werden.
- **TFTP** – innerhalb von IP-Netzwerken (Inband- und Fernkonfiguration) kann begrenzt auch das Dateiübertragungs-Protokoll TFTP verwendet werden.

Bitte beachten Sie, dass alle Verfahren auf dieselben Konfigurationsdaten zugreifen. Wenn Sie beispielsweise in LANconfig Einstellungen ändern, hat dies auch direkte Auswirkungen auf die Werte unter WEBconfig und Telnet.

1.2.1 Konfiguration über *LANconfig*

Rufen Sie *LANconfig* z.B. aus der Windows-Startleiste auf mit **Start** / **Programme** / **LANCOM** / ***LANconfig***. *LANconfig* sucht nun automatisch im lokalen Netz nach Geräten. Wird dabei ein noch nicht konfiguriertes Gerät im lokalen Netz gefunden, startet *LANconfig* selbstständig den Setup-Assistenten.

Neue Geräte suchen

Um die Suche eines neuen Geräts manuell einzuleiten, klicken Sie auf die Schaltfläche **Suchen** oder rufen den Befehl über **Gerät** / **Suchen** auf. *LANconfig* erkundigt sich dann, wo es suchen soll. Bei der Inband-Lösung reicht hier die Auswahl des lokalen Netzes, und los geht's.

Sobald *LANconfig* mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.

Der erweiterte Funktionsumfang für Profis

Für die Konfiguration der Geräte mit *LANconfig* stehen zwei verschiedene Darstellungsmöglichkeiten zur Auswahl:

- In der 'einfachen Darstellung' werden nur die Einstellungen angezeigt, die für übliche Anwendungsfälle benötigt werden.
- In der 'vollständigen Darstellung' werden alle verfügbaren Einstellungen angezeigt. Einige davon sollten nur von erfahrenen Benutzern verändert werden.

Wählen Sie den Darstellungsmodus im Menü **Ansicht** / **Optionen**.

Ein Doppelklick auf den Eintrag für das markierte Gerät, der Klick auf die Schaltfläche **Konfigurieren** oder den Menüeintrag **Gerät** / **Konfigurieren** liest die aktuellen Einstellungen aus dem Gerät aus und zeigt die allgemeinen Geräteinformationen an.

Die eingebaute Hilfe-Funktion

Die weitere Bedienung des Programms erklärt sich selbst bzw. über die Online-Hilfe. Mit einem Klick auf das Fragezeichen oben rechts in jedem Fenster bzw. mit einem rechten Mausklick auf einen unklaren Begriff können Sie jederzeit die kontextsensitive Hilfe aufrufen.

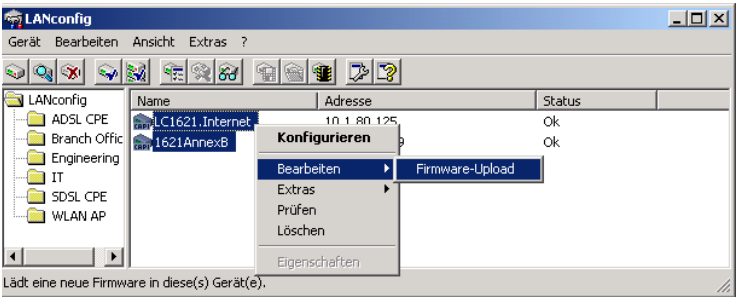
DE

Verwaltung mehrerer Geräte gleichzeitig

Mit *LANconfig* können mehrere Geräte gleichzeitig komfortabel (fern-) gewartet werden. Dazu einfach alle gewünschten Geräte selektieren, *LANconfig* führt dann alle Aktionen für alle ausgewählten Geräte nacheinander durch. Einzige Bedingung ist, dass es sich um Geräte gleichen Typs handelt.

Zur bequemen Verwaltung lassen sich Geräte zu Gruppen zusammenfassung. Dazu muss die Ansicht 'Verzeichnisbaum' aktiviert sein, dann können die Geräte durch einfaches Verschieben per 'drag und drop' in die gewünschten Ordner gruppiert werden.

In der Mehrgeräte-Konfiguration zeigt LANconfig nur die für die Mehrgeräte-Konfiguration geeigneten Eingabefelder an, z.B. bei LANCOM Wireless LAN Access-Points die MAC Access-Control-Liste.



1.2.2 Konfiguration mit *WEBconfig*

Sie können die Einstellungen des Gerätes über einen beliebigen (auch textbasierten) Web-Browser vornehmen. Im *LANCOM* ist die Konfigurationssoftware *WEBconfig* integriert. Sie benötigen lediglich einen Web-Browser, um auf *WEBconfig* zuzugreifen.

Funktioniert mit beliebigem Web-Browser

WEBconfig bietet ähnliche Setup-Assistenten wie *LANconfig* an und bietet damit optimale Voraussetzungen für eine komfortable Konfiguration des *LANCOM* – im Unterschied zu *LANconfig*, aber unter allen Betriebssystemen, für die es einen Web-Browser gibt.

Für die Verwendung von *WEBconfig* muss eine TCP/IP-Verbindung zum LAN- oder WAN-Anschluss aufgebaut sein. Der Zugriff auf *WEBconfig* erfolgt mit Hilfe eines Web-Browsers entweder über die IP-Adresse des *LANCOM*, über

den Namen des Gerätes (sofern bereits zugewiesen) bzw. sogar über einen beliebigen Namen, falls das Gerät noch nicht konfiguriert wurde.

```
http://<IP-Adresse oder Gerätename>
```

Sicher mit HTTPS

WEBconfig bietet zur sicheren (Fern-) Konfiguration die Möglichkeit der verschlüsselten Übertragung der Konfigurationsdaten über HTTPS.

```
https://<IP-Adresse oder Gerätename>
```

Für maximale Sicherheit sollten Sie stets die neueste Version Ihres Internet-Browsers verwenden. Unter Windows 2000 empfiehlt LANCOM Systems die Installation des sog. "High Encryption Pack" oder den Internet Explorer Version 5.5 mit Service Pack 2 oder besser.

1.2.3 Konfiguration über Telnet

Über Telnet starten Sie die Konfiguration z.B. aus der Windows-Kommandozeile mit dem Befehl:

```
C:\>telnet 10.0.0.1
```

Telnet baut dann eine Verbindung zum Gerät mit der eingegebenen IP-Adresse auf.

Nach der Eingabe des Passworts (sofern Sie eines zum Schutz der Konfiguration vereinbart haben) stehen Ihnen alle Konfigurationsbefehle zur Verfügung.

Die Sprache der Konsole auf Deutsch ändern

Der Terminalmodus steht in den Sprachen Deutsch und Englisch zur Verfügung. *LANCOM* werden werkseitig auf Englisch als Konsolensprache eingestellt. Im weiteren Verlauf dieser Dokumentation werden alle Konfigurationsbefehle in ihrer deutschen Form angegeben. Zur Änderung der Konsolensprache auf Deutsch verwenden Sie folgende Befehle:

Konfigurationstool	Aufruf (bei Englisch als eingestellter Konsolensprache)
WEBconfig	Expertenkonfiguration / Config-Module / Language
Telnet	`set /Setup/Config-Module/Language Deutsch`

DE

TFTP

Bestimmte Funktionen lassen sich über Telnet nicht oder nicht befriedigend ausführen. Dazu gehören alle Funktionen, bei denen komplette Dateien übertragen werden, etwa der Upload von Firmware oder die Speicherung und Wiederherstellung von Konfigurationsdaten. In diesen Fällen wird TFTP eingesetzt.

TFTP steht standardmäßig unter den Betriebssystemen Windows 2000 und Windows NT zu Verfügung. Es ermöglicht den einfachen Dateitransfer von Dateien mit anderen Geräten über das Netzwerk.

Die Syntax des TFTP-Aufrufs ist abhängig vom Betriebssystem. Bei Windows 2000 und Windows NT lautet die Syntax:

```
tftp -i <IP-Adresse Host> [get|put] Quelle [Ziel]
```

Bei zahlreichen TFTP-Clients ist das ASCII-Format voreingestellt. Für die Übertragung binärer Daten (z.B. Firmware) muss daher meist die binäre Übertragung explizit gewählt werden. In diesem Beispiel für Windows 2000 und Windows NT erreichen Sie das durch den Parameter '-i'.

1.2.4 Konfiguration über SNMP

Das Simple Network Management Protocol (SNMP V.1 nach RFC 1157) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus.

Es gibt eine ganze Reihe von Konfigurations- und Management-Programmen, die über SNMP laufen. Kommerzielle Beispiele sind Tivoli, OpenView von Hewlett-Packard, SunNet Manager und CiscoWorks. Daneben existieren auch zahlreiche Programme auf Freeware- und Shareware-Basis.

Ihr *LANCOM* kann für die Verwendung in SNMP-Programmen sogenannte Geräte-MIB-Datei (**M**anagement **I**nformation **B**ase) exportieren.

Konfigurationstool	Aufruf
WEBconfig	SNMP-Geräte-MIB abrufen (im Hauptmenü)
TFTP	`tftp 10.0.0.1 get readmib file1`

1.3 Die Fernkonfiguration über das DFÜ-Netzwerk

Der komplette Abschnitt zur Fernkonfiguration gilt nur für LANCOM mit ISDN-Schnittstelle.

Besonders einfach wird die Einstellung von Routern an entfernten Standorten mit der Fernkonfiguration über das DFÜ-Netzwerk von Windows. Das Gerät ist nach dem Einschalten und der Verbindung mit dem WAN-Anschluss ohne eine einzige Einstellung sofort vom Administrator zu erreichen. Damit sparen Sie beim Anschluss von anderen Netzwerken an Ihr eigenes LAN viel Zeit und Geld für die Reise zum anderen Netzwerk oder für die Einweisung der Mitarbeiter vor Ort in die Konfiguration der Router.

Außerdem können Sie eine spezielle Rufnummer für die Fernkonfiguration reservieren. Damit kann ein Service-Techniker immer auf den Router zugreifen, auch wenn das Gerät durch fehlerhafte Einstellungen eigentlich nicht mehr ansprechbar ist.

1.3.1 Das brauchen Sie für die ISDN-Fernkonfiguration

- Einen *LANCOM* mit ISDN-Anschluss
- Einen Rechner mit PPP-Client, z.B. Windows DFÜ-Netzwerk
- Ein Programm für die Inband-Konfiguration, z.B. *LANconfig* oder Telnet
- Einen Konfigurations-PC mit ISDN-Adapter oder Zugriff über *LANCAPI* auf einen *LANCOM* mit ISDN-Anschluss

1.3.2 Die erste Fernverbindung mit DFÜ-Netzwerk

a Wählen Sie im *LANconfig* **Gerät** / **Neu**, aktivieren Sie die 'DFÜ-Verbindung' als Anschlusstyp und geben Sie die Rufnummer des WAN-Anschlusses ein, an dem der *LANCOM* angeschlossen ist. Stellen Sie dazu ggf. die Zeit ein, nach der eine Verbindung ohne Datentransfer automatisch getrennt werden soll.

b *LANconfig* legt nun automatisch einen neuen Eintrag im DFÜ-Netzwerk an. Wählen Sie ein PPP-fähiges Gerät (z.B. den NDIS-WAN-Treiber aus dem Lieferumfang der *LANCAPI*) für die Verbindung aus, und bestätigen Sie mit **OK**.

c Anschließend zeigt *LANconfig* in der Geräteliste ein neues Gerät mit dem Namen 'Unbekannt' und der Rufnummer über DFÜ als Adresse an.

Mit dem Löschen eines Eintrags in der Geräteliste wird auch die zugehörige Verbindung im Windows-DFÜ-Netzwerk gelöscht.

DE

d Sie können das Gerät über die Fernverbindung nun genauso einstellen wie alle anderen Geräte. Zum Auslesen der Konfiguration baut *LANconfig* eine Verbindung über das DFÜ-Netzwerk auf.

1.3.3 Die erste Fernverbindung mit PPP-Client und Telnet

a Stellen Sie mit Ihrem PPP-Client eine Verbindung zum *LANCOM* her, verwenden Sie dabei folgende Angaben:

- Benutzername 'ADMIN'
- Passwort wie beim *LANCOM* eingestellt
- eine IP-Adresse für die Verbindung, nur wenn erforderlich

b Starten Sie eine Telnet-Verbindung zum *LANCOM*. Verwenden Sie dazu die folgende IP-Adresse:

- '172.17.17.18', wenn Sie keine IP-Adresse für den PPP-Client festgelegt haben. Diese Adresse verwendet der *LANCOM* automatisch, falls nichts anderes vereinbart ist. Der anrufende PC reagiert dann auf die IP '172.17.17.17'.
- Erhöhen Sie die IP-Adresse des PCs um eins, wenn Sie eine Adresse festgelegt haben. Beispiel: Sie haben für den PPP-Client die IP '10.0.200.123' festgelegt, dann hört der *LANCOM* auf die '10.0.200.124'. Ausnahme: Bei einer '254' am Ende der IP reagiert der Router auf die 'x.x.x.1'.

c Sie können den *LANCOM* über die Fernverbindung nun genauso einstellen wie alle anderen Geräte.

Der Default-Layer für die Ferninbetriebnahme

Die PPP-Verbindung von einer beliebigen ISDN-Gegenstelle zum Router gelingt natürlich nur dann, wenn das Gerät jeden Ruf mit den entsprechenden Einstellungen für den PPP-Betrieb annimmt. Im Auslieferungszustand geht das auch, da das Standard-Protokoll (Default-Layer) auf PPP eingestellt ist.

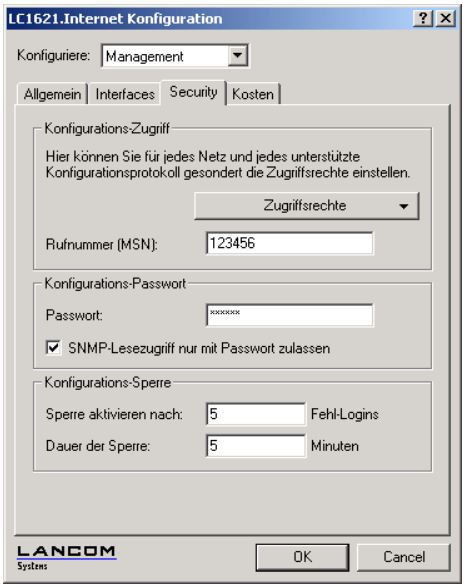
Aber vielleicht möchten Sie ja nach der ersten Konfiguration den Default-Layer z.B. für LAN-LAN-Verbindungen auf ein anderes Protokoll einstellen? Dann nimmt das Gerät die Rufe über die DFÜ-Verbindung nicht mehr mit den PPP-Einstellungen an. Abhilfe schafft hier die Vereinbarung einer speziellen Rufnummer für den Konfigurationszugriff:

DE

Der ISDN-Administrationszugang für die Fernwartung

Empfängt das Gerät einen Ruf auf dieser Nummer, wird immer die Einstellung für PPP verwendet - unabhängig von der weiteren Konfiguration des Routers! Dabei wird nur ein spezieller Benutzername während der PPP-Verhandlung akzeptiert, der beim Verbindungsaufbau über *LANconfig* automatisch eingetragen wird ('ADMIN').

a Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Security'.



b Geben Sie als Rufnummer im Bereich 'Konfigurationszugriff' eine Rufnummer Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.

Geben Sie alternativ den folgenden Befehl ein:

```
set /setup/config-modul/Fernconfig 123456
```

Schützen Sie die Einstellungen des Geräts immer durch die Vergabe eines Passworts! Geben Sie bei einer Telnet- oder Terminalverbindung alternativ den folgenden Befehl ein:

```
passwd
```

DE

Damit werden Sie zur Eingabe eines neuen Passworts mit Bestätigung aufgefordert.

1.4 *LANmonitor* – wissen, was läuft

Mit dem Überwachungstool *LANmonitor* können Sie sich unter Windows-Betriebssystemen die wichtigsten Informationen über den Status Ihrer Router auf dem Bildschirm anzeigen lassen. Und zwar den Status aller *LANCOM* im Netz.

Viele der internen Meldungen der Geräte werden dabei in Klartext umgewandelt, zeigen Ihnen den aktuellen Zustand des Gerätes und helfen Ihnen bei der Fehlersuche.

Sie können mit *LANmonitor* auch den Datenverkehr auf den verschiedenen Schnittstellen der Router beobachten und erhalten so wichtige Hinweise darüber, mit welchen Einstellungen Sie den Datenverkehr optimieren können.

Neben den Statistiken des Geräts, die Sie zum Beispiel auch in einer Telnet- oder Terminalsitzung oder mit *WEBconfig* auslesen können, stehen Ihnen im *LANmonitor* noch weitere nützliche Funktionen zur Verfügung, wie beispielsweise die Freischaltung eines zusätzlichen Gebührenlimits.

Sie können mit LANmonitor nur solche Geräte überwachen, die Sie über IP erreichen (lokal oder remote). Über die serielle Schnittstelle können Sie einen Router mit diesem Programm nicht ansprechen.

1.4.1 Erweiterte Anzeige-Optionen

Unter **Ansicht** / **Anzeigen** können Sie folgende Anzeige-Optionen ein- und ausschalten:

- Fehlermeldungen
- Diagnosemeldungen
- System-Informationen

Viele wichtige Details zum Status des LANCOM werden erst angezeigt, wenn die Anzeige der System-Informationen aktiviert ist. Dazu gehören beispielsweise die Schnittstellen und das Gebührenmanagement. Wir empfehlen daher interessierten Benutzern, die Anzeige der System-Informationen einzuschalten.

DE

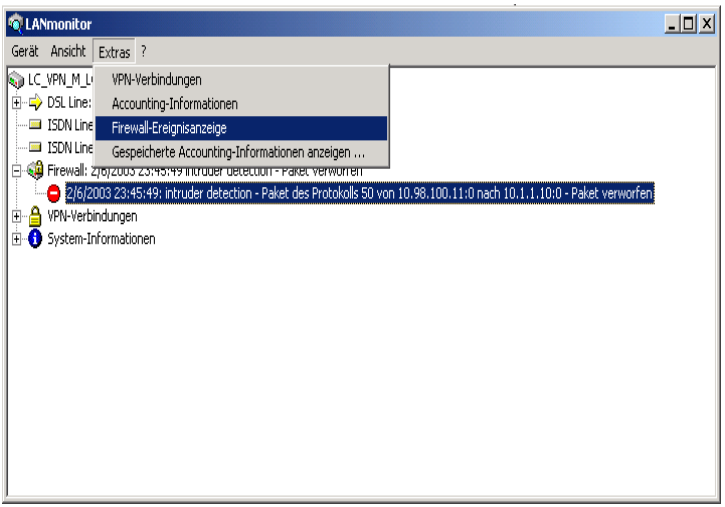
1.4.2 Internet-Verbindung kontrollieren

Als Beispiel für die Funktionen von *LANmonitor* zeigen wir Ihnen zuerst einmal, welche Informationen *LANmonitor* über den Verbindungsaufbau zu Ihrem Internet-Provider bereitstellt.

a Starten Sie *LANmonitor* mit **Start** / **Programme** / **LANCOM** / **LANmonitor**. Legen Sie mit **Gerät** / **Neu** ein neues Gerät an und geben im folgenden Fenster die IP-Adresse für den Router an, den Sie überwachen wollen. Falls die Konfiguration des Gerätes mit einem Passwort gesichert ist, geben Sie dieses gleich mit ein.

Alternativ können Sie über *LANconfig* das Gerät auswählen und mit **Extras** / **Gerät überwachen** die Überwachung für ein Gerät starten.

b *LANmonitor* legt automatisch einen neuen Eintrag in der Geräteliste an und zeigt zunächst den Zustand der Übertragungskanäle. Starten Sie Ihren Web-Browser, und geben Sie eine beliebige Webseite ein. *LANmonitor* zeigt nun an, wie auf einem Kanal eine Verbindung aufgebaut wird und welche Gegenstelle dabei gerufen wird. Sobald die Verbindung hergestellt ist, zeigt der Kommunikationskanal durch das Pluszeichen vor dem Eintrag an, dass zu diesem Kanal weitere Informationen vorliegen. Durch Klicken auf das Pluszeichen oder Doppelklick auf einen entsprechenden Eintrag öffnen Sie eine baumartige Struktur, in der Sie verschiedene Informationen ablesen können.



DE

In diesem Beispiel können Sie aus den Protokoll-Informationen zum PPP ablesen, welche IP-Adresse der Provider Ihrem Router für die Dauer der Verbindung zugewiesen hat und welche Adressen für DNS- und NBNS-Server übermittelt wurden.

Unter den allgemeinen Informationen können Sie beobachten, mit welchen Übertragungsraten aktuell Daten mit dem Internet ausgetauscht werden.

c Durch einen Klick mit der rechten Maustaste auf den aktiven Kanal können Sie die Verbindung manuell trennen. Dazu benötigen Sie ggf. das Konfigurationspasswort.

d Wenn Sie ein Protokoll der *LANmonitor*-Ausgaben in Form einer Datei wünschen, wählen Sie unter **Gerät** / **Eigenschaften** die Registerkarte 'Protokoll'. Aktivieren Sie die Protokollierung und stellen Sie ein, ob *LANmonitor* täglich, monatlich oder fortlaufend eine Protokolldatei erstellt.

1.5 Trace-Ausgaben – Infos für Profis

Zur Kontrolle der internen Abläufe im Router während oder nach der Konfiguration bieten sich die Trace-Ausgaben an. Durch einen solchen Trace werden z.B. die einzelnen Schritte bei der Verhandlung des PPPs angezeigt. Erfahrene Anwender können durch die Interpretation dieser Ausgaben evtl. Fehler beim Verbindungsaufbau aufspüren. Besonders positiv: Die aufzuspürenden Fehler können sowohl in der Konfiguration eigener Router als auch bei der Gegenseite zu finden sein.

Die Trace-Ausgaben sind leicht zeitverzögert zum tatsächlichen Ereignis, jedoch immer in der richtigen Reihenfolge. Das stört im Regelfall die Interpretation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.

1.5.1 So starten Sie einen Trace

Trace-Ausgaben starten Sie z.B. in einer Telnet-Sitzung. Der Trace-Aufruf folgt dieser Syntax:

```
trace [Schlüssel] [Parameter]
```

Der Befehl Trace, der Schlüssel, die Parameter und die Kombinationsbefehle werden jeweils durch Leerzeichen voneinander getrennt. Und was steckt hinter Schlüssel und Parameter?

1.5.2 Übersicht der Schlüssel

Dieser Schlüssel ...	... ruft in Verbindung mit Trace die folgende Reaktion hervor:
?	zeigt einen Hilfetext an
+	schaltet eine Trace-Ausgabe ein
-	schaltet eine Trace-Ausgabe aus
#	schaltet zwischen verschiedenen Trace-Ausgaben um (Toggle)
kein Schlüssel	zeigt den aktuellen Zustand des Traces an

1.5.3 Übersicht der Parameter

Die jeweils für ein bestimmtes Modell verfügbaren Traces können über die Eingabe von `trace` *ohne Argumente auf der Kommandozeile angezeigt werden.*

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
Status	Status-Meldungen der Verbindungen
Fehler	Fehler-Meldungen der Verbindungen
LANCOM	Verhandlung des LANCOM-Protokolls
IPX-Router	IPX-Routing
PPP	Verhandlung des PPP-Protokolls
SAP	IPX Service Advertising Protocol
IPX-Watchdog	IPX-Watchdog-Spoofing
SPX-Watchdog	SPX-Watchdog-Spoofing
LCR	Least-Cost-Router
Script	Script-Verhandlung
RIP	IPX Routing Information Protocol
IP-Router	IP-Routing
IP-RIP	IP Routing Information Protocol
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
IP-Masquerading	Vorgänge im Masquerading-Modul
DHCP	Dynamic Host Configuration Protocol

DE

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
NetBIOS	NetBIOS-Verwaltung
DNS	Domain Name Service Protocol
Paket-Dump	Anzeige der ersten 64 Bytes eines Pakets in hexadezimaler Darstellung
D-Kanal-Dump	Trace des D-Kanals des angeschlossenen ISDN-Busses
ATM	Spoofing auf ATM-Paketebene
ADSL	ADSL-Verbindungsstatus
VPN-Status	IPSec und IKE Verhandlungen
VPN-Packet	IPSec und IKE Pakete
SMTP-Client	E-Mail-Verarbeitung des integrierten Mail-Clients
SNTP	Simple Network Time Protokoll

1.5.4 Kombinationsbefehle

Dieser Kombinations-Befehl ...	... ruft beim Trace die folgende Anzeige hervor:
All	alle Trace-Ausgaben
Display	Status- und Error-Ausgaben
Protocol	LANCOM- und PPP-Ausgaben
TCP-IP	IP-Rt.-, IP-RIP-, ICMP- und ARP-Ausgaben
IPX-SPX	IPX-Rt.-, RIP-, SAP-, IPX-Wd.-, SPX-Wd.-, und NetBIOS-Ausgaben
Time	zeigt vor der eigentlichen Trace-Ausgabe auch die Systemzeit an
Source	zeigt vor der eigentlichen Trace-Ausgabe auch das Protokoll an, das die Ausgabe veranlasst hat

Die angehängten Parameter werden dabei von links nach rechts abgearbeitet. Dadurch kann ein zunächst aufgerufener Parameter anschließend auch wieder eingeschränkt werden.

1.5.5 Beispiele

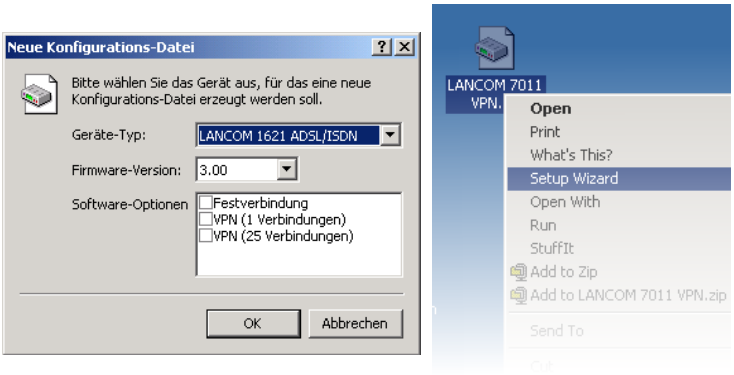
Dieser Schlüssel ...	... ruft in Verbindung mit Trace die folgende Reaktion hervor:
trace	zeigt alle Protokolle an, die während der Konfiguration Ausgaben erzeugen können, und den Zustand der jeweiligen Ausgaben (ON oder OFF)
trace + all	schaltet alle Trace-Ausgaben ein
trace + protocol display	schaltet die Ausgabe aller Verbindungsprotokolle und der Status- und Fehlermeldungen ein
trace + all - icmp	schaltet alle Trace-Ausgaben mit Ausnahme des ICMP-Protokolls ein
trace ppp	zeigt den Zustand des PPPs an
trace # ipx-rt display	schaltet die Trace-Ausgaben des IPX-Routers und der Display-Ausgaben um
trace - time	schaltet die Ausgabe der Systemzeit vor der eigentlichen Trace-Ausgabe ab

1.6 Abspeichern, Wiederherstellen und Erzeugen von Konfigurationsdateien

Die aktuelle Konfiguration eines *LANCOM* kann als Datei abgespeichert und bei Bedarf wieder in das Gerät (oder in ein anderes Gerät desselben Typs) geladen werden.

Zusätzlich können mit *LANconfig* Konfigurationsdateien auch "offline" erzeugt und editiert werden - für alle unterstützten Gerätetypen, Firmware-Versionen und Software-Optionen.

DE



Sicherheitskopien der Konfiguration

Mit dieser Funktion können Sie Sicherungskopien der Konfiguration Ihres *LANCOM* erstellen. Sollte Ihr *LANCOM* (z.B. durch einen Defekt) seine Konfigurationsdaten verlieren, spielen Sie einfach die Sicherungskopie ein.

Komfortable Serienkonfiguration

Aber auch wenn Sie vor der Aufgabe stehen, mehrere gleichartige *LANCOM* konfigurieren zu müssen, werden Sie die Funktion des Abspeicherns und Wiederherstellens von Konfigurationen schätzen lernen. Sie können sich in diesem Fall einen großen Teil der Arbeit sparen, indem Sie in alle Geräte zunächst übereinstimmende Parameter als Grundkonfiguration einspielen und nur noch die individuellen Einstellungen an den einzelnen Geräten vornehmen.

Funktionsaufruf:

Konfigurationstool	Aufruf
LANconfig	Bearbeiten / Konfiguration als Datei sichern Bearbeiten / Konfiguration aus Datei wiederherstellen Bearbeiten / Neue Konfigurations-Datei Bearbeiten / Konfigurations-Datei bearbeiten Bearbeiten / Konfigurations-Datei drucken
WEBconfig	Konfiguration speichern / Konfiguration laden (im Hauptmenü)
TFTP	`tftp 10.0.0.1 get readconfig file1` `tftp 10.0.0.1 put file1 writeconfig`

DE

1.7 Neue Firmware mit LANCOM FirmSafe

Die Software für die Geräte von LANCOM Systems wird ständig weiterentwickelt. Damit Sie auch in den Genuss von neuen Features und Funktionen kommen, haben wir die Geräte mit einem Flash-ROM-Speicher ausgerüstet, der das nachträgliche Ändern der Betriebssoftware zum Kinderspiel macht. Kein EPROM tauschen, kein Gehäuse öffnen: Einfach die neue Version einspielen und fertig!

1.7.1 So funktioniert LANCOM FirmSafe

LANCOM FirmSafe macht das Einspielen der neuen Software zur sicheren Sache: Die gerade verwendete Firmware wird dabei nicht einfach überschrieben, sondern es wird eine zweite Firmware zusätzlich im Gerät gespeichert.

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firmware überschrieben. Sie können selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll:

- 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
  - Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
  - Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit neu.
- 'Login': Um den Problemen eines fehlerhaften Uploads zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
  - Im Unterschied zur ersten Variante wartet das Gerät anschließend fünf Minuten lang auf einen erfolgreichen Login. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.
  - Wenn das Gerät nicht mehr ansprechbar ist und ein Login somit unmöglich ist, aktiviert es automatisch wieder die bisherige Firmware und startet damit neu.
- 'Manuell': Bei der dritten Möglichkeit können Sie vorher selbst eine Zeit bestimmen, in der Sie die neue Firmware testen wollen. Das Gerät startet

DE

mit der neuen Firmware und wartet in der eingestellten Zeit darauf, dass die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird.

1.7.2 So spielen Sie eine neue Software ein

Beim Firmware-Upload (so heisst das Einspielen der Software) führen verschiedene Wege zum Ziel:

- *LANconfig*
- *WEBconfig*
- Terminalprogramm
- TFTP

Beim Firmware-Upload bleiben alle Einstellungen erhalten! Trotzdem sollten Sie sicherheitshalber die Konfiguration vorher speichern (bei *LANconfig* z.B. mit **Bearbeiten** / **Konfiguration sichern**).

Enthält die neu eingespielte Version Parameter, die in der aktuellen Firmware des Gerätes nicht vorhanden sind, werden die fehlenden Werte mit den Default-Einstellungen ergänzt.

LANconfig

Beim *LANconfig* markieren Sie das gewünschte Gerät in der Auswahlliste und klicken auf **Bearbeiten** / **Firmware-Verwaltung** / **Neue Firmware hochladen** oder direkt auf die Schaltfläche **Firmware-Upload**. Dann wählen Sie das Verzeichnis, in dem sich die neue Version befindet, und markieren die entsprechende Datei.

LANconfig informiert Sie dann in der Beschreibung über Versions-Nummer und Datum der Firmware und bietet den Upload an. Mit **Öffnen** ersetzen Sie die vorhandene Firmware durch die ausgewählte Version.

Wählen Sie außerdem aus, ob die Firmware sofort nach dem Laden dauerhaft aktiviert werden soll, oder stellen Sie eine Testzeit ein, in der Sie die Firmware selbst freischalten. Um anschließend die Firmware während der eingestellten Testzeit zu aktivieren, klicken Sie auf **Bearbeiten** / **Firmware-Verwaltung** / **Firmware im Test freischalten**.

WEBconfig

Starten Sie *WEBconfig* in Ihrem Web-Browser. Auf der Startseite finden Sie den Link **Eine neue Firmware hochladen**. Im nächsten Fenster können Sie

die Firmware-Datei im Verzeichnissystem suchen und anschließend auf die Schaltfläche **Upload** klicken.

Terminalprogramm (z.B. Hyperterminal von Windows)

Stellen Sie bei Terminalprogrammen im Menü 'Firmware' mit dem Befehl 'set Modus-Firmsafe' zunächst ein, in welchem Modus Sie die neue Firmware laden wollen (unmittelbar, login oder manuell). Stellen Sie ggf. zusätzlich mit 'set Timeout-Firmsafe' die Zeit für den Firmwaretest ein.

Mit dem Befehl 'Firmware-Upload' wird der Router anschließend in Empfangsbereitschaft versetzt. Starten Sie anschließend den Upload-Vorgang von Ihrem Terminalprogramm aus:

- Bei Telix klicken Sie auf die Schaltfläche **Upload**, stellen 'XModem' für die Übertragung ein und wählen die gewünschte Datei zum Upload aus.
- Bei Hyperterminal klicken Sie auf **Übertragung** / **Datei senden**, wählen die Datei aus, stellen 'XModem' als Protokoll ein und starten mit **OK**.

TFTP

Auf *LANCOM* kann mit TFTP eine neue Firmware aufgespielt werden. Dazu wird der Befehl (bzw. das Ziel) **writeflash** angegeben. Um eine neue Firmware in einen *LANCOM* mit der IP-Adresse 10.0.0.1 zu übertragen, geben Sie z.B. unter Windows 2000 oder Windows NT folgenden Befehl ein:

```
tftp -i 10.0.0.1 put Lc_16xxu.282 writeflash
```

1.8 Das Kommandozeilen-Interface

Das *LANCOM* Kommandozeilen-Interface ist stets wie folgt strukturiert:

- Status
  Enhält die Zustände und Statistiken aller internen Module des Gerätes
- Setup
  Beinhaltet alle einstellbaren Parameter aller internen Module des Gerätes
- Firmware
  Beinhaltet das Firmware-Management
- Sonstiges
  Enthält Aktionen für Verbindungsauf- und abbau, Reset, Reboot und Upload

DE

1.8.1 Kommandozeilen-Referenz

Das *LANCOM* Kommandozeilen-Interface kann mit den folgenden DOS- oder UNIX-ähnlichen Befehlen bedient werden:

Command	Description
cd <Verzeichnis>	Wechselt das aktuelle Verzeichnis. Verschiedene Kurzformen werden unterstützt, z.B. "cd ../.." kann verkürzt werden zu "cd ..." etc.
del <Name> rm <Name>	Löscht den Tabelleneintrag mit dem Index <Name>
dir [<Verzeichnis>] list[<Verzeichnis>] ls [<Verzeichnis>] ll [<Verzeichnis>]	Zeigt den Inhalt des aktuellen Verzeichnisses an
do <Name> [<Parameter>]	Führt die Aktion <Name> im aktuellen Verzeichnis aus. Zusätzl. Paramter können mit angegeben werden
exit/quit/x	Beendet die Kommandozeilen-Sitzung
feature <code>	Freischaltung eines SW-Features mit dem angegebenen Feature-Code
passwd	Ändern des Passworts
ping [IP-Addresse]	Sendet einen ICMP echo request and die angegebene IP-Adresse
readconfig	Anzeige der kompletten Konfiguration in der Geräte-Syntax
readmib	Anzeige der SNMP Management Information Base
repeat <INTERVAL> <Kommando>	Wiederholt das Kommando alle INTERVAL Sekunden, bis der Vorgang durch neue Eingaben beendet wird
stop	Beendet den PING-Befehl
set <Name> <Wert(e)>	Setzt einen Konfigurationsparameter auf einen bestimmten Wert. Handelt es sich beim Konfigurationsparameter um einen Tabellenwert, so muss für jede Spalte der ein Wert angegeben werden. Dabei übernimmt das Zeichen * als Eingabewert einen vorhandenen Tabelleneintrag unverändert.

DE

Command	Description
set [<Name>] ?	Auflistung der möglichen Eingabewerte für einen Konfigurationsparameter. Wird kein Name angegeben, so werden die möglichen Eingabewerte für alle Konfigurationsparameter im aktuellen Verzeichnis angegeben
show <Optionen>	Anzeige spezieller interner Daten. show ? zeigt alle verfügbaren Informationen an, z.B. letzte Boot-Vorgänge ('bootlog'), Firewall Filterregeln ('filter'), VPN-Regeln ('VPN') und Speicherauslastung ('mem' und 'heap')
sysinfo	Anzeige der Systeminformationen (z.B. Hardware/Softwareversion etc.)
trace […]	Konfiguration der Diagnose-Ausgaben. Siehe 'So starten Sie einen Trace' auf Seite 20
writeconfig	Laden eines neuen Konfigurationsfiles in der Geräte-Syntax. Alle folgenden Zeilen werden als Konfigurationswerte interpretiert, solange bis zwei Leerzeilen auftreten
writeflash	Laden einer neuen Firmware-Datei (via TFTP)

- Alle Befehle, Verzeichnis- und Parameternamen können verkürzt eingegeben werden - solange sie eindeutig sind. Zum Beispiel kann der Befehl "`sysinfo`" zu "`sys`" verkürzt werden, oder aber "`cd Management`" zu "`c ma`". Die Eingabe "`cd /s`" dagegen ist ungültig, da dieser Eingabe sowohl "`cd /Setup`" als auch "`cd /Status`" entspräche.
- Namen, die Leerzeichen enthalten, müssen in Anführungszeichen ("") eingeschlossen werden.
- Für Aktionen und Befehle steht eine kommandospezifische Hilfefunktion zur Verfügung, indem die Funktion mit einem Fragezeichen als Parameter aufgerufen wird. Zum Beispiel zeigt der Aufruf '`ping ?`' die Optionen des eingebauten ping Kommandos an.
- Eine vollständige Auflistung der zur Verfügfung stehenden Konsolen-Kommandos erhalten Sie durch die Eingabe von '`?`' auf der der Kommandozeile.

DE

1.9 Scheduled Events

Automatische, zeitgesteuerte Ausführung von Kommandozeilen-Befehlen

Dieses Feature erlaubt dem Gerät bestimmte Befehle zu bestimmten, benutzerdefinierten Zeitpunkten auszuführen. Die Funktionalität entspricht dabei dem unter UNIX bekannten *cron*-Dienst. Ausgeführt werden kann dabei jede beliebige *LANCOM* Kommandozeilenfunktion. Es können damit also alle *LANCOM* Features mit einer zeitlichen Steuerung versehen werden.

Anwendungsbeispiele:

- Verbindungsauf- und -abbauten zu bestimmten Zeiten
- zeitgesteuerte Firewall-Regeln
- Durchführung reglmäßiger Firmware- oder Konfigurationsupdates

Die Parameter werden dabei wie folgt abgelegt:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration / Setup / Config--Modul / Cron-Tabelle
Terminal/Telnet	`/Setup/Config-Modul/Cron-Tabelle`

DE

Eintrag	Beschreibung
Index	Eindeutige Kennzeichnung des Tabelleneintrages
Base	Das Feld `Base` bestimmt ob die zeitliche Steuerung gegen Echtzeit oder gegen die Betriebszeit des Gerätes ausgeführt werden soll. Echtzeit-basierte Regel können nur ausgeführt werden sofern das Gerät über einen gültigen Zeitbezug verfügt, also z.B. via NTP. Echtzeit-basierte Regeln werten alle Zeit-/Datumsangaben aus, während Betriebszeit-basierte Regeln nur die Minuten- und Stundenangaben auswerten.
Minute Hour DayOfWeek Day Month	Die Werte `Minute` bis `Month` definieren die Zeitpunkte, an denen ein Kommando ausgeführt werden soll. Wird ein Wert nicht angegeben, so wird er auch nicht in die Steuerung einbezogen. Pro Parameter kann auch eine Komma-separierte Liste von Werten, oder aber ein Bereich (angegeben als "Minimalwert-Maximalwert") eingegeben werden. Die Syntax des `DayOfWeek`-Feldes entspricht dabei der üblichen *cron*-Interpretation: 0 Sonntag 1 Montag 2 Dienstag 3 Mittwoch 4 Donnerstag 5 Freitag 6 Samstag
Command	Das auszuführende Kommando oder eine Komma-separierte Kommando-Liste

Das folgende Beispiel baut an jedem Werktag automatisch um 18.00h eine Verbindung zur Gegenstelle 'ZENTRALE' auf:

Base	Realtime
Minute Hour DayOfWeek Day Month	 18 1,2,3,4,5,
Command	do /sonst/man/aufbau ZENTRALE

Zeitgesteuerte Regeln werden mit einer Genauigkeit von einer Minute ausgeührt.

DE

2 Sicherheit

Sie mögen es sicher nicht, wenn jeder Aussenstehende einfach die Daten auf Ihren Rechnern einsehen oder verändern kann. Dieses Kapitel widmet sich daher einem sehr wichtigen Thema: der Sicherheit. Die Beschreibung der Sicherheitseinstellungen ist in folgende Abschnitte unterteilt:

- Schutz für die Konfiguration
  - Passwortschutz
  - Login-Sperre
  - Zugangskontrolle
- Die Stateful-Inspection Firewall
  - Filterung von Datenpaketen
  - Stateful-Inspection im Detail
  - Alarmierungsfunktionen
  - Tipps zur Einstellung der Firewall
  - Firewall-Diagnose
- Abwehr von Einbruchsversuchen: Intrusion-Detection
- Schutz vor Denial-of-Service-Angriffen
- 'Unsichtbar' machen
- Absichern des ISDN-Einwahlzugangs

Zum Ende des Kapitels finden Sie die wichtigsten Sicherheitseinstellungen in Form einer Checkliste. Damit Sie ganz sicher sein können, dass Ihr *LANCOM* bestens abgesichert ist.

2.1 Schutz für die Konfiguration

Mit der Konfiguration des Gerätes legen Sie eine Reihe von wichtigen Parametern für den Datenaustausch fest: Die Sicherheit des eigenen Netzes, die Kontrolle der Kosten und die Berechtigung einzelner Netzteilnehmer gehören z.B. dazu.

Die von Ihnen einmal eingestellten Parameter sollen natürlich nicht durch Unbefugte verändert werden. Daher bietet ein *LANCOM* die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

DE

2.1.1 Passwortschutz

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Passworts.

Solange Sie kein Passwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Beispielsweise könnten Ihre Internerzugangsdaten gestohlen werden, oder der Router so umkonfiguriert werden, dass alle Schutzmechanismen für lokale Netz ausser Kraft gesetzt werden.

Hinweis: Ein nicht gesetztes Passwort wird auf allen LANCOM durch eine blinkende Power-LED signalisiert, sofern die Geräte in Betrieb genommen worden sind (lokale Intranet-Adresse vorhanden).

Tipps für den richtigen Umgang mit Passwörtern

Für den Umgang mit Passwörtern möchten wir Ihnen an dieser Stelle einige Tipps ans Herz legen:

- **Halten Sie ein Passwort so geheim wie möglich.**
  Notieren Sie niemals ein Passwort. Beliebt aber völlig ungeeignet sind beispielsweise: Notizbücher, Brieftaschen und Textdateien im Computer. Es klingt trivial, kann aber nicht häufig genug wiederholt werden: verraten Sie Ihr Passwort nicht weiter. Die sichersten Systeme kapitulieren vor der Geschwätzigkeit.
- **Passwörter nur sicher übertragen.**
  Ein gewähltes Passwort muss der Gegenseite mitgeteilt werden. Wählen Sie dazu ein möglichst sicheres Verfahren. Meiden Sie: Ungeschütztes E-Mail, Brief, Fax. Besser ist die persönliche Übermittlung unter vier Augen. Die höchste Sicherheit erreichen Sie, wenn Sie das Passwort auf beiden Seiten persönlich eingeben.
- **Wählen Sie ein sicheres Passwort.**
  Verwenden Sie zufällige Buchstaben- und Ziffernfolgen. Passwörter aus dem allgemeinen Sprachgebrauch sind unsicher. Auch Sonderzeichen wie '&"?#-*+_:;,!°' erschweren es Angreifern, Ihr Passwort zu erraten und erhöhen so die Sicherheit des Passworts.
- **Verwenden Sie ein Passwort niemals doppelt.**
  Wenn Sie dasselbe Passwort für mehrere Zwecke verwenden, mindern Sie seine Sicherheitswirkung. Wenn eine Gegenseite unsicher wird, gefährden Sie mit einem Schlag auch alle anderen Verbindungen, für die Sie dieses Passwort verwenden.

- **Wechseln Sie das Passwort regelmässig.**
  Passwörter sollen möglichst häufig gewechselt werden. Das ist mit Mühe verbunden, erhöht aber die Sicherheit des Passwortes beträchtlich.
- **Wechseln Sie das Passwort sofort bei Verdacht.**
  Wenn ein Mitarbeiter mit Zugriff auf ein Passwort Ihr Unternehmen verlässt, wird es höchste Zeit, dieses Passwort zu wechseln. Ein Passwort sollte auch immer dann gewechselt werden, wenn der geringste Verdacht einer undichten Stelle auftritt.

Wenn Sie diese einfachen Regeln einhalten, erreichen Sie ein hohes Maß an Sicherheit.

Eingabe des Passwortes

Das Feld zur Eingabe des Passworts finden Sie in *LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Unter *WEBconfig* rufen Sie den Assistenten **Sicherheitseinstellungen** auf. In einer Terminal- bzw. einer Telnet-Sitzung setzen oder ändern Sie das Passwort mit dem Befehl `passwd`.

Konfigurationstool	Aufruf
LANconfig	Management / Security / Passwort
WEBconfig	Sicherheitseinstellungen
Terminal/Telnet	`passwd`

Den SNMP-Zugang schützen

Im gleichen Zug sollten Sie auch den SNMP-Lesezugriff mit Passwort schützen. Für SNMP wird das allgemeine Konfigurations-Passwort verwendet.

Konfigurationstool	Aufruf
LANconfig	Management / Security / SNMP-Lesezugriff nur mit Passwort zulassen
WEBconfig	Experten-Konfiguration / Setup / SNMP-Modul / Passw.Zwang-fuer-SNMP-Lesezugriff
Terminal/Telnet	`Setup/SNMP-Modul/Passw.Zwang`

DE

2.1.2 Die Login-Sperre

Die Konfiguration im *LANCOM* ist durch eine Login-Sperre gegen „Brute-Force-Angriffe" geschützt. Bei einem Brute-Force-Angriff versucht ein unberechtigter Benutzer, ein Passwort zu knacken, und so Zugang zu einem Netzwerk, einem Rechner oder einem anderen Gerät zu erlangen. Dazu spielt z.B. ein Rechner automatisch alle möglichen Kombinationen aus Buchstaben und Zahlen durch, bis das richtige Passwort gefunden wurde.

Zum Schutz gegen solche Versuche kann die maximal zulässige Anzahl von fehlerhaften Login-Versuchen eingegeben werden. Wird diese Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt.

Tritt auf einem Zugang die Sperre in Kraft, so sind auch alle anderen Zugänge automatisch gesperrt.

Zur Konfiguration der Login-Sperre stehen in den Konfigurationstools folgende Einträge zur Verfügung:

- Sperre aktivieren nach (`Login-Fehler`)
- Dauer der Sperre (`Sperr-Minuten`)

Konfigurationstool	Aufruf
LANconfig	Management / Security
WEBconfig	Experten-Konfiguration / Setup / Config-Modul
Terminal/Telnet	`Setup/Config-Modul`

2.1.3 Einschränkung der Zugriffsrechte auf die Konfiguration

Der Zugriff auf die internen Funktionen kann wie folgt getrennt nach Zugangarten getrennt konfiguriert werden:

- ISDN-Administrationzugang
- Netzwerk
  - LAN
  - WAN

Bei den Netzwerk-Konfigurationszugriffen können weitere Einschränkungen vorgenommen, z.B. dass nur die Konfiguration von bestimmten IP-Adressen oder LANCAPI-Clients vorgenommen werden darf. Ferner sind alle internen Funktionen getrennt schaltbar

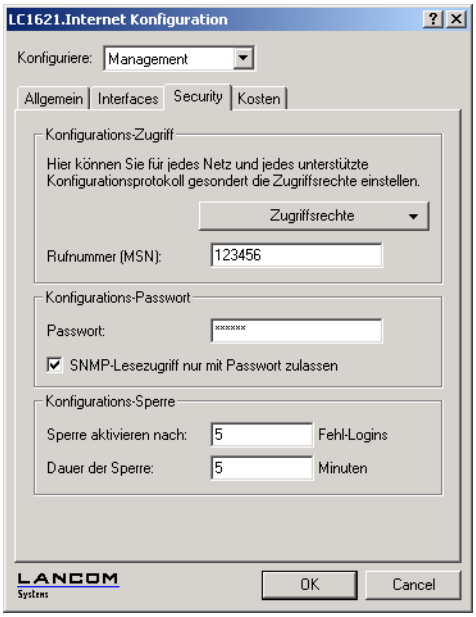
DE

Mit den internen Funktionen werden hierbei Konfigurationssitzungen über *LANconfig* (TFTP), *WEBconfig* (HTTP, HTTPS), SNMP oder Terminal/Telnet bezeichnet.

Den ISDN-Administrationszugang einschränken

Dieser Absatz gilt nur für Modelle mit ISDN-Schnittstelle.

a Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Security'.



b Geben Sie als Rufnummer im Bereich 'Konfigurationszugriff' eine Rufnummer Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.

Geben Sie alternativ den folgenden Befehl ein:

```
set /setup/config-modul/Fernconfig 123456
```

Der ISDN-Administrationszugang ist als einzige Konfigurationsmethode von den im folgenden beschriebene Netzwerk-Zugangsbeschränkungen ausgenommen. D.h. alle auf der ADMIN-MSN eingehenden Verbindungen

DE

werden nicht über die Zugriffssteuerung von entfernten Netzen eingeschränkt.

Wenn Sie die ISDN-Fernwartung ganz abschalten wollen, lassen Sie das Feld mit der ADMIN-MSN leer.

Den Netzwerk-Konfigurationszugriff einschränken

Der Zugriff auf die internen Funktionen kann -getrennt für Zugriffe aus dem lokalen oder aus entfernten Netzen - für alle Konfigurationsdienste getrennt gesteuert werden.

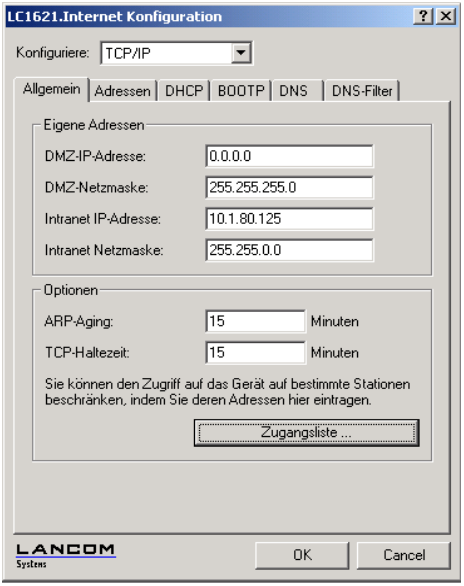
Dabei kann der Konfigurationszugriff generell erlaubt oder verboten werden, als reiner Lesezugriff oder - falls Ihr Modell mit VPN ausgerüstet ist - auch nur über VPN erlaubt werden.

Wenn Sie den Netzwerkzugriff auf den Router über das WAN ganz sperren wollen, stellen Sie den Konfigurationszugriff von entfernten Netzen für alle Methoden auf 'nicht erlaubt'.

DE

Einschränkung des Netzwerk-Konfigurationszugriffs auf bestimmte IP-Adressen

Mit einer speziellen Filterliste kann der Zugriff auf die internen Funktionen der Geräte auf bestimmte IP-Adressen eingeschränkt werden.



Standardmässig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP ein Zugriff auf den Router gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen.

Konfigurationstool	Aufruf
LANconfig	TCP/IP / Allgemein / Zugangsliste
WEBconfig	Experten-Konfiguration / Setup / TCP-IP-Modul / Zugangs-Liste
Terminal/Telnet	`/Setup/TCP-IP-Modul/Zugangsliste`

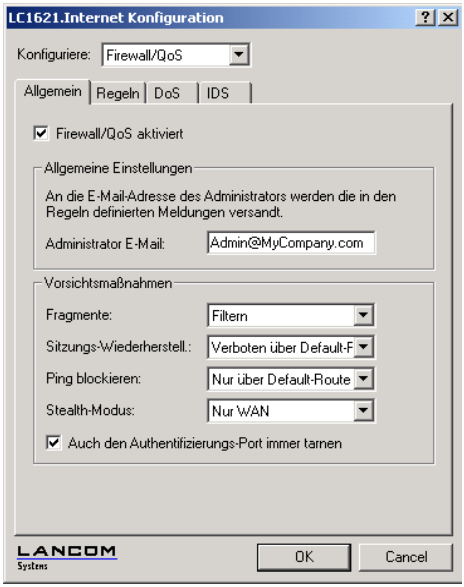
DE

2.2 Die Stateful-Inspection Firewall

Hautpanforderung an moderne Breitbandanschlüsse ist eine Sicherheitsfunktionalität, die einen sicheren "Always-On"-Betrieb ganzer Netze gewährleistet. Dieses wird durch die im *LANCOM* integrierte Firewall erreicht.

Die Filter-Regeln einer Stateful-Inspection Firewall sind - anders als bei klassische Portfilter-Firewalls - richtungsabängig: Ein Verbindung kann immer von nur der Quelle zum Ziel aufgebaut werden; es sei denn, für die Rückrichtung wäre ein expliziter Eintrag vorhanden. Ist eine Verbindung aufgebaut, so werden nur die zu dieser Verbindung gehörenden Datenpakete - in beide Richtungen natürlich - übertragen. Damit lassen sich z.B. alle Zugriffe, die unaufgefordert und nicht aus dem lokalen Netz heraus erfolgen, zuverlässig abblocken.

Im Gegensatz zu einfachen Portfilter-Firewalls lassen sich mit der Stateful-Inspection auch dynamische ausgehandelte Ports (wie z.B. bei FTP oder H.323) überwachen: Anstatt dass alle Ports zum Funktionieren solcher Protokolle freigeben werden müssten, überwacht die Stateful-Inspection Firewall diese Protokolle im Detail, und öffnet dynamisch nur die jeweils ausgehandelten Ports.



Von der Firewall betroffen ist stets nur "durchgehender" Datentransfer durch das LANCOM. Zugangseinschränkungen für die internen Dienste zur Konfiguration des LANCOM (z.B. HTTP, HTTPS, TFTP und Telnet) wurden im vorherigen Abschnitt vorgestellt.

2.2.1 Filterung von Datenpaketen

Die Firewall-Filter des *LANCOM* bieten Filterfunktionen für einzelne Rechner und auch ganze Netze. Sie ermöglichen einen effektiven Schutz gegen unerwünschte Eindringlinge in Ihr Netzwerk.

Was kann gefiltert werden?

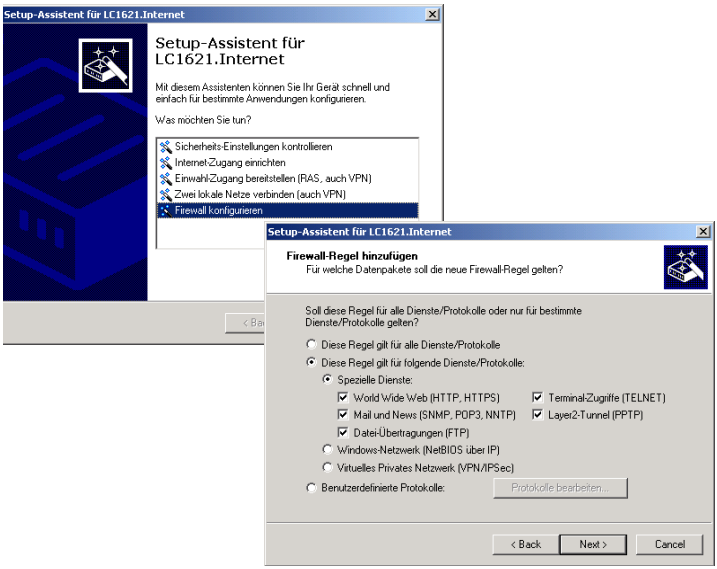
Wichtig sind die Quell- und Zielfilter für einzelne Ports oder auch Portbereiche. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (TCP/UDP/ICMP) gefiltert werden. Auch IP-Adressbereiche oder komplette IP-Netzwerke sind geeignete Objekte, ebenso wie bestimmte Stationen oder Gegenstellen.

Neben diesen Objekten auf IP-Ebene können Stationen im LAN auch über ihre MAC-Adresse ausgewählt werden. „MAC" steht für **M**edia **A**ccess **C**ontrol und ist Dreh- und Angelpunkt für die Kommunikation innerhalb eines LAN. Jedem Netzwerkadapter ist eine MAC-Adresse fest eingespeichert. MAC-Adressen sind weltweit eindeutig und unverwechselbar, ähnlich zu Seriennummern von Geräten. Über die MAC-Adressen lassen sich die PCs im LAN zuverlässig auswählen, um ihnen gezielt Rechte auf IP-Paketebene zu gewähren oder zu versagen. MAC-Adressen werden häufig aussen auf den Netzwerkgeräten in hexadezimaler Darstellung (z.B. 00:A0:57:01:02:03) angebracht.

DE

Einrichten der Filter

Die schnellste Methode zur Konfiguration der Firewall steht mit dem Firewall-Assistenten in LANconfig zur Verfügung:



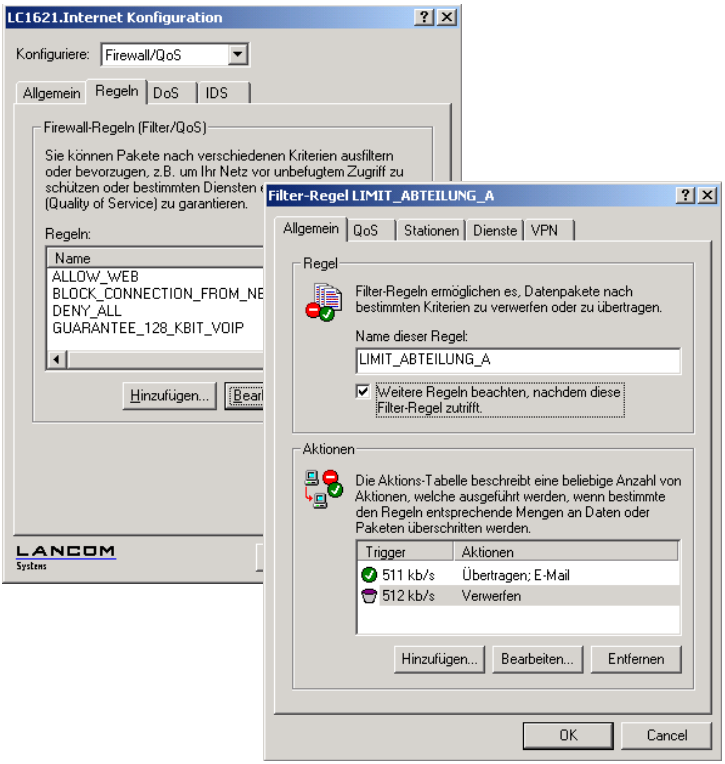
Mit den anderen Konfigurationstools werden die Firewall-Filter in folgenden Menüs und Listen konfiguriert:

Konfigurationstool	Aufruf
LANconfig	Firewall/QoS / Regeln / Hinzufügen
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / Firewall / Regel-Tabelle
Terminal/Telnet	`/Setup/IP-Router-Modul/Firewall/Regel-Tabelle`

DE

Einrichten der Filter unter *LANconfig*

Die Einrichtung der Filter mit Hilfe von *LANconfig* ist besonders komfortabel. Unter 'Firewall/QoS / Regeln' finden Sie die folgenden Karteikarten, mit deren Hilfe Filterregeln definiert werden können.



Ausgehend von der Übersichtsseite "Firewall/QoS / Regeln" gelangen Sie duch "Hinzufügen" oder "Bearbeiten" auf den Dialog zur Definition von Filterregeln:

- 'Regel'
  Hier wird der Name des Filterdienstes festgelegt, und ob weitere Regeln beachtet werden sollen, nachdem diese Regel zutrifft.
- 'Aktionen'
  Hier legen Sie die Auslösebeding für die zu erstellende Firewall-Regel und die bei Eintritt des Ereignisses stattfindenden Aktionen fest (siehe 'Aktions-Objekte' auf Seite 49)

DE

- 'QoS'
  Hier können Sie Mindestbandbreiten für die Datenpakete zur Verfügung stellen, die durch die betreffende Firewall-Regel spezifiziert sind (siehe 'Quality-of-Service Objekte' auf Seite 53 und 'Quality-of-Service' auf Seite 93).
- 'Stationen'
  Hier werden die Stationen – als Absender oder Adressat der Pakete – festgelegt, für die die Filterregel gelten soll (siehe 'Quell- und Zielobjekte' auf Seite 47).
- 'Dienste'
  Hier wird festgelegt, für welche IP-Protokolle, Quell- und Zielports die Filterregel gelten soll. Beispielsweise können Sie hier angeben, dass nur der Zugriff auf Internetseiten und E-Mail gestattet sein soll.
- 'VPN'
  Hier können Sie Regeln für die Behandlung von verschlüsselten Paketen definieren, sofern Ihr Router VPN unterstützt, z.B. ob nur die Übertragung von verschlüsselten Datenpaketen gestattet sein soll.

Einrichten der Filter mit *WEBconfig* oder über Terminal/Telnet

Etwas schwieriger als in *LANconfig* gestaltet sich die Konfiguration über *WEBconfig* oder über eine Terminal- oder Telnet-Verbindung. Gleichzeitig stehen mit diesen Konfigurationsmethoden die detailliertesten Einstellmöglichkeiten für erfahrene Benutzer zur Verfügung.

Hier wird die Filterfunktion mit der Filterliste beschrieben, die ihrerseits auf drei Tabellen basiert: Der Objekttabelle, der Aktionstabelle und der Regeltabelle. Die Objekttabelle definiert u.a. Rechner, Netze und Protokolle. In der Aktionstabelle werden z.B. Limitierungen, Mindestbandbreiten und Meldungen definiert. Die Regeltabelle fasst Objekte und Aktionen zu Firewall-Regeln zusammen. Die Filterliste wird automatisch aus der Regeltabelle erzeugt und zeigt die daraus resultierenden Filtereinstellungen an.

2.2.2 Stateful-Inspection im Detail

In diesem Abschnitt werden detaillierte Hintergrundinformationen über die Funktionsweise und Möglichkeiten der LANCOM Firewall vorgestellt.

Wenn Sie diese Informationen zunächst überspringen wollen können Sie direkt zum Kapitel 'Tipps zur Einstellung der Firewall' auf Seite 63 übergehen.

Hauptaufgabe einer Stateful-Inspection Firewall ist die Überwachung erlaubter Verbindungen.

Die Stateful-Inspection Firewall benutzt für ihre Arbeit zwei Datenbanken. Diese ist zum einen die Portfilterdatenbank, und zum anderen die Zustandsdatenbank (die eigentliche "Stateful-Inspection"), in der alle aktiven Verbindungen sowie gesperrte Ports, Hosts, etc. abgelegt sind.

Wird ein Paket empfangen, so wird zuerst nachgeschaut, ob ein für dieses Paket ein Verbindungseintrag in der Zustandsdatenbank existiert. Existiert ein solcher Eintrag, dann wird mit dem Paket so verfahren, wie in der Datenbank vermerkt ist. Wird für das Paket kein Eintrag gefunden, dann wird die Portfilterdatenbank durchsucht, ob ein passender Eintrag vorhanden ist und die dort angegebene Aktion ausgeführt. Wenn die Aktion besagt, dass das Paket akzeptiert werden soll, so wird ein Eintrag in der Zustandsdatenbank vorgenommen und etwaige weitere Aktionen dort vermerkt.

Existiert für ein Datenpaket keine explizite Firewall-Regel, so wird das Paket akzeptiert ('Allow-All'). Damit ist eine Abwärtskompatibilität zu bestehenden Installationen gegeben. Für einen maximalen Schutz durch die Stateful-Inspection beachten Sie bitte den Abschnitt 'Aufbau einer expliziten "Deny-All"-Strategie' auf Seite 64.

Objekt-Tabelle

In der Objekt-Tabelle werden diejenigen Elemente bzw. Objekte definiert, die in der Regel-Tabelle der Firewall verwendet werden sollen. Objekte können sein:

- Protokolle
- einzelne Rechner (MAC- oder IP-Adresse, Host-Name)
- ganze Netze
- Dienste (Ports oder Port-Bereiche, z.B. HTTP, Mail&News, FTP, ...)
- Auslösebedingungen (Trigger) - global oder pro Verbindung
- Benachrichtigungen (Email/SYSLOG/SNMP/Log)
- Host- und Verbindungsaktionen (close port, disconnect)

Diese Elemente lassen sich auch beliebig kombinieren. Zudem können Objekte hierarchisch definiert werden. So könnten zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kämen dann Objekte z.B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP +

Port 53) hinzu. Diese könnten dann wiederum zu einem Objekt zusammengefasst werden, das alle Definitionen der Einzelobjekte enthält.

Auf die direkten Beschreibungen, die Sie hier mit angeben können, wird im Abschnitt zum Thema Regel-Tabelle näher eingegangen.

Regel-Tabelle

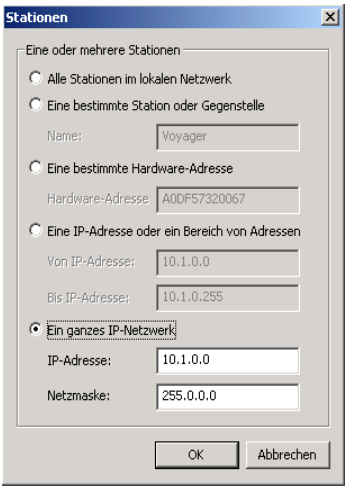
In der Regel-Tabelle werden die Objekte zu Filterregeln verknüpft. Die Regel-Tabelle enthält das zu filternde Protokoll (das sie in der Objekt-Tabelle definiert haben), die Quell-Objekte, die Ziel-Objekte sowie die auszuführende Filteraktion.

Das Protokoll sowie die Quell- bzw. Ziel-Objekte können sowohl aus zusammengestellten Objekten bestehen, als auch direkte Beschreibungen (z.B. %P6 für TCP) beinhalten, die durch '+' oder Leerzeichen getrennt werden. Eine direkte Beschreibung wird durch '%' gekennzeichnet. Mögliche Beschreibungen sind:

DE

Quell- und Zielobjekte

Beschreibung	Objekt-ID
lokales Netz	%L
Hostname	%H
MAC-Adresse	%E
IP-Adresse	%A
Netzmaske	%M
Protokoll (TCP/UDP/ICMP etc.)	%P
Dienst (Port)	%S



Gleichartige Beschreibungen können durch Komma getrennte Listen, wie z.B. Host-Listen/Adresslisten (%A10.0.0.1, 10.0.0.2) oder durch Bindestrich getrennte Bereiche wie z.B. Portlisten (%S20-25) erzeugen. Die Angabe einer '0' oder eines Leerstrings bezeichnet das Any-Objekt:

alle Rechner:	%A0.0.0.0
alle Dienste:	%S0
alle Protokolle:	%P0

DE

Hostnamen können nur dann verwendet werden, wenn das *LANCOM* die Namen in IP-Adressen auflösen kann. Dafür muss das *LANCOM* die Namen über DHCP oder NetBIOS gelernt haben, oder die Zuordnung muss statisch in der DNS- oder IP-Routing-Tabelle eingetragen sein. Ein Eintrag in der IP-Routing-Tabelle kann dabei einem Hostnamen ein ganzes Netz zuordnen.

Bei der Konfiguration über die Konsole (Telnet oder Terminalprogramm) müssen die kombinierten Parameter (Port, Destination, Source) jeweils in Anführungszeichen (Zollzeichen: ") eingeschlossen werden.

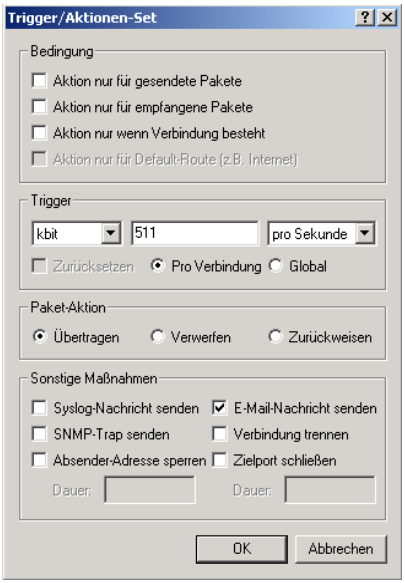
Vorgefertigte Protokollobjekte

In LANconfig stehen ein Reihe von Preset-Objekten zur einfachen Filtererstellung zur Verfügung:

- HTTP / HTTPS
- FTP
- MAIL/NEWS
- TELNET
- TFTP
- NETBIOS
- PPTP
- IPSEC
- DNS

DE

Aktions-Objekte



Als Aktionen, die ausgeführt werden können, wenn es einen Eintrag für das Paket in einer der beiden Datenbanken gibt kann eine beliebige Kombination aus der nachfolgenden Tabelle angegeben werden:

Aktion	Beschreibung	Objekt-ID
Accept	Das Paket wird angenommen	%a
Reject	Das Paket wird mit einer passenden Fehlermeldung zurückgewiesen	%r
Drop	Das Paket wird stillschweigend verworfen	%d
Connect-Filter	Der Filter ist aktiv, wenn keine logische Verbindung zum Ziel des Pakets besteht	%c
Internet-Filter	Der Filter ist aktiv, wenn das Paket über die Defaultroute empfangen wurde oder gesendet werden soll	%i
Syslog	Gibt eine detailierte Meldung über Syslog aus	%s
Mail	Schickt eine E-Mail an den Administrator	%m
SNMP	Sendet einen SNMP-Trap	%n

DE

Aktion	Beschreibung	Objekt-ID
Close-Port	Schliesst den Zielport des Pakets für eine vorgebbare Zeit	%p
Deny-Host	Sperrt die Absender-Adresse des Pakets für eine vorgebbare Zeit	%h
Disconnect	Trennt die Verbindung zur Gegenstelle, über die das Paket empfangen wurde oder gesendet werden sollte	%t
Zero-Limit	Setzt den Limit-Counter (s.u.) bei überschreiten der Trigger-Schwelle wieder auf 0	%z

Diese Aktionen sind beliebig miteinander kombinierbar, wobei bei widersinningen Aktionen (z.B.: Accept + Drop) die sicherere, d.h. im Beispiel "Drop" genommen wird. Wenn zum "Connect-" oder "Internet-" Filter keine weitere Aktion angegeben wird, dann wird implizit eine Kombination dieser Filter mit der "Reject" Aktion angenommen.

Wenn die "Close-Port" Aktion ausgeführt wird, wird ein Eintrag in einer Sperrliste vorgenommen, durch den alle Pakete, die an den jeweiligen Rechner und Port gesendet werden, verworfen werden. Für das "Close-Port"-Objekt kann eine Sperrzeit in Sekunden, Minuten oder Stunden angegeben werden, die direkt hinter der Objekt-ID vermerkt wird. Diese Zeitangabe baut sich zusammen aus dem Bezeichner für die Zeiteinheit (h, m, s für Stunde, minute und sekunde) sowie der eigentlichen Zeitangabe. So sperrt z.B. %pm10 den Port für 10 Minuten. Wird keine Zeiteinheit angegeben, so wird "Minuten" als Einheit angenommen. (damit ist %p10 gleichbedeutend mit %pm10)

Wird die "Deny-Host" Aktion ausgeführt, so wird der Absender des Pakets in eine Sperrliste eingetragen. Ab diesem Moment werden alle Pakete, die von dem gesperrten Rechner empfangen werden verforfen. Auch das "Deny-Host"-Objekt kann mit einer Sperrzeit versehen werden, die wie bei der "Close-Port" Option beschrieben gebildet wird.

Jede dieser Aktionen kann mit einem Limit verknüpft werden, dessen Überschreitung zur Auslösung der Aktion führt. Über mehrere Limits für einen Filter sind dadurch auch Aktionsketten möglich. Es stehen folgende Limitierungen zur Verfügung

DE

Trigger-Objekte:

Limit	Beschreibung	Objekt -ID
Data (abs)	Absolute Anzahl von Kilobytes auf der Verbindung nach denen die Aktion ausgeführt wird	%lcd
Data (rel)	Anzahl von Kilobytes/Sekunde, Minute , Stunde auf der Verbindung nach denen die Aktion ausgeführt wird	%lcds %lcdm %lcdh
Packet (abs)	Absolute Anzahl von Paketen auf der Verbindung nach denen die Aktion ausgeführt wird	%lcp
Packet (rel)	Anzahl von Paketen/Sekunde Minute, Stunde oder absolut auf der Verbindung nach denen die Aktion ausgeführt wird	%lcps %lcpm %lcph
global Data (abs)	Absolute Anzahl von Kilobytes, die an den Zielrechner gesendet oder von diesem empfangen wurde, nach denen die Aktion ausgeführt wird	%lgd
global Data (rel)	Anzahl von Kilobytes/Sekunde, Minute oder Stunde, die an den Zielrechner gesendet oder von diesem empfangen wurde, nach denen die Aktion ausgeführt wird	%lgds %lgdm %lgdh
global Packet (abs)	Absolute Anzahl von Paketen, die an den Zielrechner gesendet oder von diesem empfangen wurde, nach denen die Aktion ausgeführt wird	%lgp
global Packet (rel)	Anzahl von Paketen/Sekunde Minute oder Stunde, die an den Zielrechner gesendet oder von diesem empfangen wurden, nach denen die Aktion ausgeführt wird	%lgps %lgpm %lgph
receive Option	Beschränkung des Limits auf die Empfangsrichtung (dies wirkt im Zusammenhang mit obigen Limitierungen). In der Object-ID Spalte sind Beispiele angegeben	%lgdsr %lcdsr
transmit Option	Beschränkung des Limits auf die Senderichtung (dies wirkt im Zusammenhang mit obigen Limitierungen). In der Object-ID Spalte sind Beispiele angegeben	%lgdst %lcdst

DE

Wird eine Aktion ohne Limit angegeben, so wird implizit ein Paket-Limit angenommen, welches sofort beim ersten Paket überschritten wird.

Eigenschaften von Aktions- und Trigger-Objekten

Aktionen und Limitierungen werden wie Protokolle, Adressen und Dienste als Objekte abgelegt, die beliebig miteinander kombiniert werden können. Damit die Objekte nicht zu unübersichtlich werden, werden diese Objekte in einer eigenen Objektliste verwaltet.

Limit-Objekte werden dabei allgemein mit %l eingeleitet, gefolgt von

- Bezug
  - verbindungsbezogen (c)
  - global (g)
- Art
  - Datenrate (d)
  - Anzahl der Pakete (p)
  - Paketrate (b)
- Wert des Limits
- Weitere Parameter (z.B. Zeitraum und Größe)

So wird z.B. das mit `%lcds8` beschriebene Limit überschritten, wenn innerhalb einer Sekunde mehr als 8 kBit über die Verbindung übertragen wurden. In diesem Moment werden die mit dem Limit verbundenen Aktionen ausgelöst. Alle nach einer Limitierung folgenden Aktionen sind mit dem Limit verknüpft. Ein neues Limit in der jeweiligen Objektbeschreibung startet eine neue Aktionsliste.

Will man z.B. die Datenrate, die für eine Verbindung zulässig ist, auf 8 KBit/s limitieren, und bei einem Flooding-Versuch den Angreifer ausperren sowie eine Email an den Administrator senden, dann lautet die Objektbeschreibung für die Aktion wie folgt:

```
%a %lcds8%d %lgbs100%h10%m
```

Diese Beschreibung erlaubt zunächst den Verkehr (`%a`). Ein einfaches `%a` am Anfang der Beschreibung ist im übrigen gleichbedeutend mit einem `%lp0%a` (= Akzeptiere, wenn das Limit von Null Paketen überschritten wurde, d.h. beim ersten Paket)

Wenn über die aktuelle Verbindung in einer Sekunde nun 8 kBit (`%lcds8`) übertragen wurden, dann werden alle weiteren Pakete bis zum Ablauf der

Sekunde stillschweigend verworfen (`%d`), wodurch sich automatisch ein Traffic-Shaping ergibt.

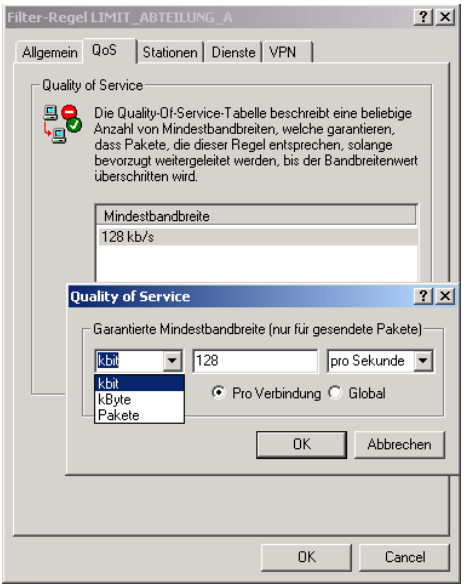
Treffen aber in einer Sekunde 100 Pakete für den Server (Zieladresse der Verbindung) ein (`%lgbs100`), so wird der entfernte Host (Quelladresse) für 10 Minuten gesperrt (`%h10`) und eine E-Mail an den Administrator geschickt (`%m`)

Die Aktionsobjekte können wie bereits die Protokoll-, Adress- und Diesntobjekte der Portfilter Firewall mit einem Namen versehen und beliebig rekursiv miteinander kombiniert werden, wobei die maximale Rekursionstiefe auf 16 Rekursionen beschränkt ist. Sie können aber auch direkt in das Aktionsfeld der Regeltabelle eingetragen werden. Beim Aufbau der eigentlichen Filter-Tabelle werden die Aktionsobjekte dann genau so wie Protokoll-, Adress- und Diesntobjekte auf die kleinste notwendige Anzahl reduziert, d.h. Mehrfachdefinitionen einer Aktion werden eliminiert und bei widersprüchlichen Aktionen wird die "sicherste" ausgewählt. So wird z.B. aus `%a` (Accept) und `%d` (Drop) nur `%d` und aus `%r` (Reject) und `%d` wird `%r`.

Quality-of-Service Objekte

Eine weiteres Limit-Objekt ist das "Quality-of-Service-Objekt" oder QoS-Objekt, das es erlaubt, einen minimalen Durchsatz bzw. eine Minimale Bandbreite für eine Verbindung oder global zu definieren. Es können sämtliche Begrenzungen angegeben werden, die auch bei normalen Limit-Objekten möglich sind, also verbindungsorientierte oder globale Minima, absolute oder zeitabhängige (relative) Minima, paket- oder datenbezogene Minima. Es gelten die gleichen Konventionen wie bei den Limit-Objekten.

DE



QoS-Objekte werden durch das Token `%q` eingeleitet und unterscheiden sich von Limit-Objekten nur dadurch, dass sie zunächst eine implizite "Accept" Aktion besitzen, d.h. nach überschreiten der Schwelle werden die folgenden Pakete weiterhin akzeptiert. Alle Pakete, die einen mit einem QoS-Objekt belegten Filter durchlaufen, werden vom Router bevorzugt versendet (das entspricht einem gesetzten "Low Delay" Flag im TOS-Feld des IP-Headers), solange die Anzahl der übertragenen Pakete oder Daten unterhalb der angegebenen Schwelle liegt. Wird die Schwelle überschritten, so werden die hinter dem QoS-Objekt angegebenen Aktionen ausgeführt. So kann für einen Dienst durch Kombination von QoS- und Limit-Objekt eine minimale und maximale Bandbreite vorgegeben werden. So ergibt z.B. aus einer minimalen Bandbreite von 32 kBit/s pro Verbindung und einer maximalen Bandbreite von 256 kBit/s für alle Verbindungen die folgende Beschreibung:

```
%a %qcds32%a %lgds256%d
```

Hier kann die explizite Angabe der Accept-Aktion, sowohl als Haupt-Aktion, als auch als getriggerte Aktion unterbleiben und die Beschreibung entsprechend abgekürzt werden:

```
%qcds32 %lgds256%d
```

Wenn die minimale und maximale Bandbreite eines Kanals gleich sein soll, so kann an die Drop-Aktion auch direkt im QoS-Objekt angegeben werden (direkt in abgekürzter Schreibweise):

```
%qcds32%d
```

Hier wird eine minimale Bandbreite von 32 kBit/s reserviert und gleichzeitig alle Pakete, die über diese Bandbreite hinaus übertragen werden sollen, verworfen. Diese Formulierung ist somit gleichbedeutend mit

```
%a %qcds32%a %lgds32%d
```

Es können beim Überschreiten der Schwelle wie bei den Limit-Objekten auch Log-Aktionen (E-Mail, Syslog etc.) ausgeführt werden

Besondere Protokolle

Ein wichtiger Punkt bei der Verbindungsüberwachung ist die Behandlung von Protokollen, die dynamisch Ports und / oder Adressen aushandeln, über die die weitere Kommunikation passiert. Beispiele für diese Protokolle sind FTP, H.323 oder auch viele UDP-basierte Protokolle. Hier ist es nötig, dass zusätzlich zu der ersten Verbindung ggf. weitere Verbindungen geöffnet werden.

UDP-Verbindungen

UDP ist eigentlich ein zustandsloses Protokoll, trotzdem kann man auch bei UDP-basierten Protokollen von einer nur kurzfristigen Verbidnung sprechen, da es sich meistens um Request/Response-basierte Protokolle handelt, bei denen ein Client seinen Request an den Well-Known Port des Servers (z.B. 53 für DNS) richtet, und dieser darauf den Response wieder an den vom Client gewählten Quellport sendet:

```
Client                Server
Request
12345 ----------------> 53
Response
12345 <---------------- 53
```

Wenn der Server hingegen größere Datenmengen senden (z.B. TFTP) will und auf dem Well-Known Port nicht zwischen Requests und Acknowledges unterscheiden möchte oder kann, so schickt er das Response-Pake an den Quellport des Absenders des ursprünglichen Requests, setzt aber als eigenen Quellport einen freien Port ein, auf dem er nun nur noch auf Pakete, die zur Datenübertragung gehören, reagiert:

DE

```
Client                  Server
Request
12345 ----------------> 69
Response
12345 <---------------- 54321
Ack/Data
12345 ----------------> 54321
Data/Ack
12345 <---------------- 54321
```

Während sich die Datenübertragung nun über die Ports 12345 und 54321 abspielt, kann der Server auf dem Well-Known Port (69) weitere Requests annehmen. Wenn das *LANCOM* wie unter 'Aufbau einer expliziten "Deny-All"-Strategie' auf Seite 64 beschrieben eine Deny-All Stategie verfolgt, würden bei einem Eintrag in der Portfilter-Firewall, der nur den Aufbau zu Port 69 zulässt, die Antwortpakte des Servers einfach verworfen. Um dies zu verhindern, wird beim Anlegen des Eintrags in der Zustandsdatenbank der Zielport der Verbindung zunächst freigehalten, und erst beim Eintreffen des ersten Antwortpakets gesetzt, wodurch beide möglichen Fälle einer UDP Verbindung abgedeckt werden.

TCP-Verbindungen

TCP-Verbindungen können nicht einfach nur durch die Prüfung der Ports nachgehalten werden. Bei einigen Protokollen wie z.B. FTP, PPTP oder H.323 sind Prüfungen der Nutzdaten nötig, um alle später ausgehandelten Verbindungen zu öffnen, und nur die wirklich zu den Verbindungen gehörenden Pakete zu akzeptieren. Dies entspricht einer vereinfachten Version dessen, was auch beim IP-Masquerading gemacht werden muss, nur, dass hier keine Adressen oder Ports umgemappt werden brauchen. Es reicht aus, die Verhandlung nachzuverfolgen, die entsprechenden Ports zu öffnen und mit der Hauptverbindung zu verknüpfen, so dass diese Ports einerseits mit dem Schliessen der Hauptverbindung ebenfalls geschlossen werden, und andererseits Traffic auf den Nebenverbindungen auch die Hauptverbindung weiter offen hält.

ICMP-Verbindungen

Für ICMP werden zwei Fälle unterschieden: Das sind zum einen die ICMP-Request/Reply-Verbindungen, wie sie z.B. beim "ping" verwendet werden, zum anderen die ICMP-Fehlermeldungen, die als Antwort auf ein beliebiges IP-Paket empfangen werden können.

ICMP Request/Reply-Verbidnungen können eindeutig durch den vom Initiator verwendeten Identifier zugeordnet werden, d.h. in der Zustandsdatenbank

wird beim Senden eines ICMP-Requests ein Eintrag erstellt, der nur ICMP-Replies mit dem korrekten Identifier durchlässt. Alle anderen ICMP-Replies werden stillschweigend verworfen.

Bei ICMP-Fehlermeldungen steht der IP-Header und die ersten 8 Bytes des IP-Pakets (i.A. UDP- oder TCP-Header) innerhalb des ICMP-Pakets. Anhand dieser Information wird beim Empfang einer ICMP-Fehlermeldung der zugehörige Eintrag in der Zustandsdatenbank gesucht. Das Paket wird nur weitergeleitet, wenn ein solcher Eintrag existiert, ansonsten wird es stillschweigend verworfen. Zusätzlich dazu werden potentiell gefährliche ICMP-Fehlermeldungen (Redirect-Route) herausgefiltert.

Verbindungen sonstiger Protokolle

Bei allen anderen Protokollen können keine verwandten Verbindungen nachgehalten werden, d.h. bei ihnen kann nur eine Verbindung zwischen den beteiligten Hosts in der Zustandsdatenbank aufgenommen werden. Diese können auch nur von einer Seite aus initiiert werden, es sei denn, in der Portfilter-Firewall ist ein dedizierter Eintrag für die "Gegenrichtung" vorhanden.

Verkettete Regeln

Es gibt Konfigurationen, die mit einer einzelnen "First Match"-Regel nicht abgedeckt werden können. Zum Beispiel eine Alarmierung bei 90%iger Überschreitung eines Transfervolumens könnte nicht gefolgt werden von einer Sperrung ab Erreichen von 100% des gestatteten Transfervolumens.

Als weiteres Beispiel sei hier eine generelle Limitierung verbunden mit verschiedenen Teillimitierungen einzelner User beschrieben. Ein solcher Regelsatz könnte wie folgt formuliert werden:

- Für alle User gilt eine globales Limit von 1 MBit/s
  - Usergruppe A darf jeweils 64 kBit/s davon verwenden
  - Usergruppe B darf jeweils 128 kBit/s davon verwenden
  - Usergruppe C ist innerhalb des globalen Limits unbeschränkt

Richtet man nun für alle Usergruppen einen Filter ein, der zum einen das Gruppenspezifische Limit enthält, zum anderen auch das globale, so erzielt man nicht den gewünschten Erfolg, sondern erhält 3 Gruppen, die in sich einen maximalen Durchsatz von 1 MBit/s besitzen, ansonsten aber völlig unabhängig voneinander sind und somit genaugenommen das globale Limit indirekt auf 3 MBit erhöht wurde.

DE

Auch eine Splittung des globalen Limits auf die einzelnen Gruppen würde nicht zum Erfolg führen, was die Usergruppe C sofort merken würde, da sie niemals die "versprochene" Bandbreite zugeteilt bekäme.

Die einzig mögliche Lösung dieses Problems ist die Verkettung mehrerer Regeln, die nacheinander abgearbeitet werden. Hierzu besitzt jede Regel ein "Continue"- bzw. "Link"-Flag, welches angibt, dass diese Regel mit einer weiteren verknüpft ist. Diese Verknüpfung besteht darin, dass in der Filter-Tabelle der nächste Filter, der ebenfalls auf das aktuelle Paket zutrifft, zur Ermittlung der auszuführenden Aktionen herangezogen wird. Dies geschieht in der Form, dass diese Limits mit ihren Aktionen einfach dem aus dem ersten Filter erzeugten Eintrag in der Verbindungsdatenbank zugeschlagen werden. Der verknüpfte Filter kann seinerseits mit weiteren Regeln verknüpft sein, so dass sich eine Filterkette hin zur allgemeinsten der verküpften Regeln ergibt.

Obiges Beispiel kann nun z.B. für FTP wie folgt definiert werden:

Name	Prot	Src	Dst	Aktion	Linked
USERGROUP_A	TCP	%a10.1.1.0 %m255.255.255.0	anyhost %s20	%a %lcds64 %d	ja
USERGROUP_B	TCP	%a10.1.2.0 %m255.255.255.0	anyhost %s20	%a %lcds128 %d	ja
USERGROUP_C	TCP	%a10.1.3.0 %m255.255.255.0	anyhost %s20	%a	ja
FTP_GLOBAL_LIMIT	TCP	%a10.1.0.0 %m255.255.252.0	anyhost %s20	%a %lgds1024 %d	nein
DENY_ALL	TCP	anyhost	anyhost %s20	%r	nein

In diesem Beispiel sind die Usergruppen durch eigene Subnetze voneinander getrennt. Kommt nun ein Paket von einem Rechner aus der Usergruppe A, so wird zunächst ein Eintrag in der Verbindungs-Datenbank für diese Verbindung aufgenommen und das in der Regel angegebene Limit mit diesem Eintrag verknüpft. Da in dieser Regel nun das Verknüpfungs-Flag ("Linked"-Spalte) gesetzt ist, wird nach der nächsten passenden Regel gesucht. Dies ist die FTP-GLOBAL Regel. In dieser Regel wird ein globales Limit definiert, das nun zusätzlich mit dem Verbindungseintrag verknüpft wird. Das gleiche geschieht mit Paketen aus den anderen Usergruppen.

Da die drei Usergruppen einen kleineren Adressbereich abdecken als der, der mit der FTP-GLOBAL Regel erfasst wird, muss noch eine weitere Regel

aufgenommen werden, die für den restlichen Adressbereich alle FTP-Zugriffe abblockt. Damit ergibt sich der komplette Regelsatz zu:

Name	Prot	Src	Dst	Aktion	Linked
FTP-BLOCK	TCP	%a10.1.0.0 %m255.255.255.0	anyhost %s20	%r	nein
USERGROUP_A	TCP	%a10.1.1.0 %m255.255.255.0	anyhost %s20	%a %lcds64 %d	ja
USERGROUP_B	TCP	%a10.1.2.0 %m255.255.255.0	anyhost %s20	%a %lcds128 %d	ja
USERGROUP_C	TCP	%a10.1.3.0 %m255.255.255.0	anyhost %s20	%a	ja
FTP_GLOBAL_LIMIT	TCP	%a10.1.0.0 %m255.255.252.0	anyhost %s20	%a %lgds1024 %d	nein
DENY_ALL	TCP	anyhost	anyhost %s20	%r	nein

Beachten Sie bitte, dass Filter bei einer Fehlangabe nicht erzeugt und auch keine Fehlermeldungen ausgegeben werden. Wenn Sie die Filter manuell konfigurieren, sollten Sie in jedem Fall überprüfen, ob die gewünschten Filter erzeugt wurden (siehe 'Die Filterliste' auf Seite 68).

2.2.3 Alarmierungsfunktionen

In diesem Abschnitt werden die Meldungen, die die Firewall bei sicherheitsrelevanten Ereignissen verschickt, im Detail beschrieben. Es stehen die folgenden Meldungstypen zur Verfügung:

- E-Mail Benachrichtigung
- SYSLOLG-Meldung
- SNMP-Trap

Benachrichtigungen können dabei jeweils getrennt entweder durch die Intrusion Detection, die Denial-of-Service Protection oder durch frei einstellbare Triggerbedingungen in der Firewall ausgelöst werden. Die spezifischen Parameter für die verschiedenen Benachrichtigungssarten (wie

DE

z.B. das zu benutzende E-Mail-Konto) können Sie an folgenden Stellen angeben:

Konfigurationstool	Aufruf
LANconfig	Meldungen / SMTP-Konto / SNMP / SYSLOG
WEBconfig	Experten-Konfiguration / Setup / SMTP / SNMP-Modul / SYS-LOG-Modul
Terminal/Telnet	`/Setup/SMTP bzw. SNMP-Modul oder SYSLOG-Modul`

Ein Beispiel:

Es sei ein Filter namens 'BLOCKHTTP' definiert, der den Zugriff auf einen HTTP-Server (192.168.200.10) abblockt, und für den Fall, dass doch jemand auf den Server zugreifen wollte, jeden Traffic von und zu diesem Rechner unterbindet und den Administrator über SYSLOG informiert.

Benachrichtigung per SYSLOG

Wenn die Portfilter-Firewall ein entsprechendes Paket verwirft, wird über Syslog (siehe auch 'Einrichten des SYSLOG-Moduls' auf Seite 114) eine Meldung ausgegeben, z.B.:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {}
(TCP): port filter
```

Die Ports werden dabei nur bei portbehafteten Protokollen ausgegeben. Zusätzlich werden Rechnernamen dann ausgegeben, wenn das *LANCOM* diese direkt (d.h. ohne weitere DNS-Anfrage) auflösen kann.

Werden für einen Filter die Syslog-Meldungen aktiviert (`%s`-Aktion), so wird diese Meldung ausführlicher. Dann werden Name des Filters, überschrittenes Limit, sowie ausgeführte Aktionen zusätzlich mit ausgegeben. Für das obige Beispiel könnte die Meldung dann so aussehen:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {}
(TCP): port filter

PACKET_INFO:
matched filter: BLOCKHTTP
exceeded limit: more than 0 packets transmitted or received on a
connection
actions: drop; block source address for 1 minutes; send syslog
message;
```

DE

Benachrichtigung per E-Mail

Ist das E-Mail-System des *LANCOM* aktiviert, so können Sie die bequeme Benachrichtigung per E-Mail nutzen:

```
FROM: LANCOM_Firewall@MyCompany.com
TO: Administrator@MyCompany.com
SUBJECT: packet filtered
Date: 9/24/2002 15:06:46

The packet below

Src: 10.0.0.37:4353 {cs2} Dst: 192.168.200.10:80 {ntserver} (TCP)

45 00 00 2c ed 50 40 00 80 06 7a a3 0a 00 00 25 | E..,.P@. ..z....%
c0 a8 c8 0a 11 01 00 50 00 77 5e d4 00 00 00 00 | .......P .w^.....
60 02 20 00 74 b2 00 00 02 04 05 b4 | `. .t... ....

matched this filter rule: BLOCKHTTP
and exceeded this limit: more than 0 packets transmitted or received
on a connection

because of this the actions below were performed:
drop
block source address for 1 minutes
send syslog message
send SNMP trap
send email to administrator
```

Benachrichtigung per SNMP-Trap

Wenn als Benachrichtigungsmethode das Versenden von SNMP-Traps aktiviert wurde (siehe auch 'Konfiguration über SNMP' auf Seite 14), so wird die erste Zeile der Logging-Tabelle als Enterprise-Specific Trap 26 verschickt. Dieser Trap enthält zusätzlich noch den System-Descriptor und den System-Namen aus der MIB-2.

Für das Beispiel wird also der folgende Trap erzeugt:

```
SNMP: SNMPv1; community = public; SNMPv1 Trap; Length = 443 (0x1BB)
SNMP: Message type = SNMPv1
SNMP: Version = 1 (0x0)
SNMP: Community = public
SNMP: PDU type = SNMPv1 Trap
SNMP: Enterprise = 1.3.6.1.4.1.2356.400.1.6021
```

Trap wurde von einem LANCOM 6021 erzeugt

```
SNMP: Agent IP address = 10.0.0.43
SNMP: Generic trap = enterpriseSpecific (6)
SNMP: Specific trap = 26 (0x1A)
SNMP: Time stamp = 1442 (0x5A2)
```

LANCOM Firewall Trap

DE

```
SNMP: OID = 1.3.6.1.2.1.1.1.0 1.
SNMP: String Value = LANCOM Business 6021 2.80.0001 / 23.09.2002
8699.000.036
```

System-Descriptor

```
SNMP: OID = 1.3.6.1.2.1.1.5.0 2. System-Name
SNMP: String Value = LANCOM Business 6021
```

Device-String

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.2.1 3.
SNMP: String Value = 9/23/2002 17:56:57
```

Time-Stamp

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.3.1 3.
SNMP: IP Address = 10.0.0.37
```

Quell-Adresse

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.4.1 4.
SNMP: IP Address = 192.168.200.10
```

Ziel-Adresse

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.5.1 5.
SNMP: Integer Value = 6 (0x6) TCP
```

Protokoll (6 = TCP)

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.6.1 6.
SNMP: Integer Value = 4353 (0x1101)
```

Quell-Port

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.7.1 7.
SNMP: Integer Value = 80 (0x50)
```

Ziel-Port (80 = HTTP)

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.8.1 8.
SNMP: String Value = BLOCKHTTP
```

Name der Filterregel

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.9.1 9.
SNMP: Integer Value = 1 (0x1)
```

Limit (1 = absolute Anzahl von Paketen)

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.10.1 10.
SNMP: Integer Value = 0 (0x0)
```

Trigger (0 = ab dem erten Paket)

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.11.1 11. Aktion
SNMP: Integer Value = 3758114816 (0xE0004800)
```

Aktion: (0xE0004800 = Drop, Quelladresse sperren, SYSLOG, SNMP-Trap, E-Mail)

Dieser Trap und alle anderen im *LANCOM* generierten Traps werden sowohl an alle manuell konfigurierten Trap-Empfänger gesendet, ebenso wie auch an jeden angemeldeten *LANmonitor*, welcher diesen und u.U. auch alle anderen Traps auswerten kann

2.2.4 Tipps zur Einstellung der Firewall

Mit der *LANCOM* Firewall steht ein extrem flexibles und mächtiges Werkzeug zur Verfügung. Um Ihnen bei der Erstellung individuell angepasster Firewall-Regeln behilflich zu sein, finden Sie im folgenden Hinweise zur optimalen Einstellung für Ihre spezifische Anwendung.

Die Default-Einstellung der Firewall

Im Auslieferungszustand befindet sich genau ein Eintrag in der Firewall-Regeltabelle:

- WINS
  Diese Regel verhindert unerwünschte Verbindungsaufbauten auf der Default-Route (i.d.R. zum Internet) durch das NetBIOS-Protokoll.
  Windows Netzwerke senden in regelmässigen Intervallen Anfragen in das Netzwerk um herauszufinden, ob die bekannten Stationen noch verfügbar sind. Dies führt bei zeitbasierter Abrechnung einer Netzwerkkopplung zu unerwünschten Verbindungsaufbauten.

Das LANCOM kann durch den integrierten NetBIOS-Proxy auch für Netzwerkkopplungen diese unerwünschten Vebindungsaufbauten verhinden, indem es selbst solange eine Antwort für die betreffende Ressource vortäuscht, bis ein tatsächlicher Zugriff erfolgt.

Sicherheit durch NAT und Stateful-Inspection

Sofern keine weitere Firewall-Regel eingetragen wird, wird das lokales Netz durch das Zusammenspiel von Network Address Translation und Stateful-Inspection geschützt: Nur Verbindungen aus dem lokalen Netz heraus erzeugen einen Eintrag in der NAT-Tabelle, woraufhin das *LANCOM* einen Kommunikationsport öffnet. Die Kommunikation über diesen Port wird durch die Stateful-Inspection überwacht: Nur Pakete, die genau zu dieser Verbindung gehören, dürfen über diesen Port kommunizieren. Für Zugriff von

DE

aussen auf das lokale Netzwerk ergibt sich somit eine implizite "Deny-All"-Strategie.

Sofern Sie einen z.B. Web-Server betreiben (siehe 'Unmaskierter Internet-Zugang für Server in der DMZ' auf Seite 84), sind zunächst alle Zugriffe von aussen auf diesen Dienst gestattet.

Aufbau einer expliziten "Deny-All"-Strategie

Für einen maximalen Schutz und bestmögliche Kontrolle über den Datenverkehr wird empfohlen, zunächst einmal jeglichen Datentransfer durch die Firewall zu unterbinden. Danach werden dann selektiv nur genau die benötigten Funktionen und Kommunikationspfade freigeschaltet. Dies bietet z.B. Schutz vor sog. 'Trojanern' bzw. E-Mail-Viren, die aktiv eine abgehende Verbindung auf bestimmten Ports aufbauen.

Einige typische Anwendungsfälle sind im folgenden aufgezeigt.

Tipp: Alle hier beschriebenen Filter können sehr komfortabel mit dem Firewall-Assistenten eingerichtet werden, um danach bei Bedarf mit z.B. LANconfig weiter verfeinert zu werden.

- Beispielkonfiguration "Basic Internet"

Regel	Quelle	Ziel	Aktion	Dienst (Zielport)
DENY_ALL	Alle Stationen	Alle Stationen	Zurückweisen	ANY
ALLOW_HTTP	Lokales Netzwerk	Alle Stationen	Übertragen	HTTP, HTTPS
ALLOW_FTP	Lokales Netzwerk	Alle Stationen	Übertragen	FTP
ALLOW_EMAIL	Lokales Netzwerk	Alle Stationen	Übertragen	MAIL, NEWS
ALLOW_DNS_ FORWARDING	Lokales Netzwerk	IP-Adresse des LANOM (alternativ: Lokales Netzwerk)	Übertragen	DNS

- Sofern Sie VPN-Einwahl auf ein *LANCOM* als VPN-Gateway gestatten wollen, so brauchen Sie keine explizite Firewall-Regel, da die Firewall nur für 'durchgehenden' Datentransfer benötigt wird.

- Für dem Fall, dass ein VPN nicht vom *LANCOM* selbst terminiert wird (z.B. VPN-Client im lokalen Netz, oder *LANCOM* als Firewall vor einem zusätzlichem VPN-Gateway), so müssen Sie zusätzlich IPSec bzw. PPTP (für das 'IPSec over PPTP' des LANCOM VPN Clients) freischalten:

Regel	Quelle	Ziel	Aktion	Dienst (Zielport)
ALLOW_VPN	VPN-Client	VPN-Server	Übertragen	IPSEC, PPTP

- Sofern Sie ISDN-Einwahl oder V.110-Einwahl (z.B. per HSCSD-Handy) gestatten, müssen Sie die betreffende Gegenstelle freischalten (siehe auch 'Die Konfiguration von Gegenstellen' auf Seite 136) :

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_DIAL_IN	Gegenstellenname	Lokales Netzwerk	Übertragen	ANY

- Für eine Netzwerkkopplung gestatten Sie zusätzlich die Kommunikation zwischen den beteiligten Netzwerken:

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	Übertragen	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	Übertragen	ANY

- Zusätzlich bei VPN-Netzwerkkopplung: Nachdem Sie die zu koppelnden Netze eingegeben haben, modifizieren Sie im Anschluss die DENY_ALL-Regel sowie die beiden Regeln zur LAN-LAN-Kopplung so, dass die Regeln keine Auswirkung auf IPSec haben ('Keine VPN-Sicherheitsrichtlinie erzeugen' auf den 'VPN'-Registerkarten der Regeln).
- Wenn Sie einen z.B. einen eigenen Webserver betreiben, so schalten Sie selektiv den Server frei:

Regel	Quelle	Ziel	Aktion	Dienst(Zielport)
ALLOW_WEBSERVER	ANY	Webserver	Übertragen	HTTP, HTTPS

DE

- Für Diagnosezwecke empfiehlt sich ferner die Freischaltung des ICMP-Protokolls (z.B. ping):

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_PING	Lokales Netzwerk	Alle Stationen	Übertragen	ICMP

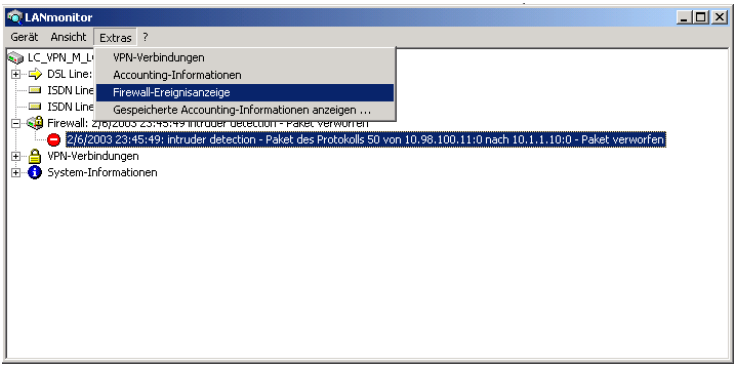
Diese Regeln können jetzt beliebig verfeinert werden - z.B. durch die Angabe von Mindest- und Maximalbandbreiten für den Serverzugriff, oder aber durch die feinere Einschränkung auf bestimmte Dienste, Stationen oder Gegenstellen.

Das LANCOM nimmt beim Aufbau der Filterliste eine automatische Sortierung der Firewall-Regeln vor. Dies geschieht dadurch, dass die Regeln anhand ihres Detaillierungsgrades sortiert in die Filterliste eingetragen werden. Zunächst werden alle spezifischen Regeln beachtet, danach die allgemein (z.B. Deny-All). Prüfen Sie bei komplexen Regelwerken die Filterliste, wie im nachfolgenden Abschnitt beschrieben.

2.2.5 Firewall-Diagnose

Alle Ereignisse, Zustände und Verbindungen der Firewall können detailliert protokolliert und überwacht werden.

Die komfortabelste Überwachung ergibt sich mit der Anzeige der Logging-Tabelle (s. u.) durch den LANmonitor. Dazu muss für die zu betrachteten Fireall-, DoS- oder IDS-Ereignisse die Signalisierung für 'SNMP (LANmonitor)' aktiviert sein.



Alle in diesem Abschnitt beschriebenen Listen und Tabellen finden Sie unter folgenden Menüpunkten:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration / Status / IP-Router-Statistik
Terminal/Telnet	`/Status/IP-Router-Statistik`

Die Logging-Tabelle

Wenn ein zu loggendes Ereignis eingetreten ist, d.h. als auszuführende Aktion beim Empfang eines Paketes ist eine Mitteilung per E-Mail, Syslog oder SNMP gefordert, so wird dieses Ereignis in einer Logging-Tabelle festgehalten. Diese Tabelle enthält die folgenden Werte:

Element	Bedeutung
Idx.	laufender Index (damit die Tabelle auch über SNMP abgefragt werden kann)
System-time	System-Zeit in UTC kodiereung (wird bei der Ausgabe der Tabelle in Klartext umgewandelt)
Src-address	Quelladresse des gefilterten Pakets
Dst-address	Zieladresse des gefilterten Pakets
Prot.	Protokoll (TCP, UDP etc.) des gefilterten Pakets
Src-p	Quellport des gefilterten Pakets (nur bei portbehafteten Protokollen)
Dst-p	Zielport des gefilterten Pakets (nur bei portbehafteten Protokollen)
Filter-Rule	Name der Regel, die den Eintrag erzeugt hat.

DE

Element	Bedeutung
Limit	Bitfeld, das das überschrittene Limit beschreibt, durch welches das Paket gefiltert wurde. Es sind z.Zt folgende Werte definiert: 0x01 Absolute Anzahl, 0x02 Anzahl pro Sekunde, 0x04 Anzahl pro Minute, 0x08 Anzahl pro stunde, 0x10 globales Limit, 0x20 Bytelimit (wenn nicht gesetzt, handelt es sich um ein Paket-Limit), 0x40 limit gilt nur in Empfangsrichtung, 0x80 limit gilt nur in Senderichtung
Threshold	überschrittener Grenzwert des auslösenden Limits
Action	Bitfeld, das alle ausgeführten Aktionen aufführt. Es sind z.Zt folgende Werte definiert: 0x00000001 Accept 0x00000100 Reject 0x00000200 Aufbaufilter 0x00000400 Internet- (Defaultrouten-) Filter 0x00000800 Drop 0x00001000 Disconnect 0x00004000 Quelladresse sperren 0x00020000 Zieladresse und -port sperren 0x20000000 Sende Syslog-Benachrichtigung 0x40000000 Sende SNMP-Trap 0x80000000 Sende E-Mail

Alle Firewall-Aktionen werden ebenfalls im IP-Router-Trace angezeigt ('So starten Sie einen Trace' auf Seite 20). Einige LANCOM-Modelle verfügen ferner über eine Firewall-LED, welche jedes gefilterte Paket signalisiert.

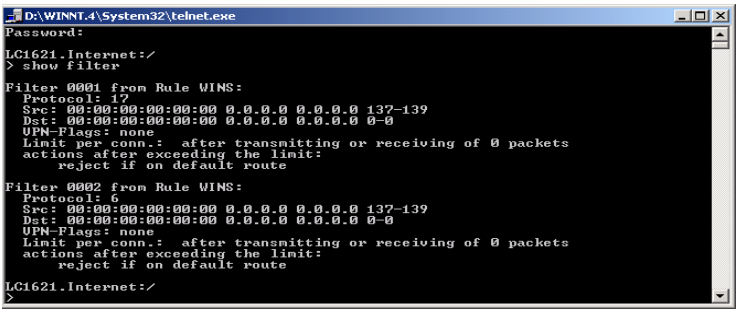
Die Filterliste

Über die Filterliste können die aus den in der Aktions-, Objekt- und Regeltabelle definierten Regeln erzeugten Filter ermittelt werden.

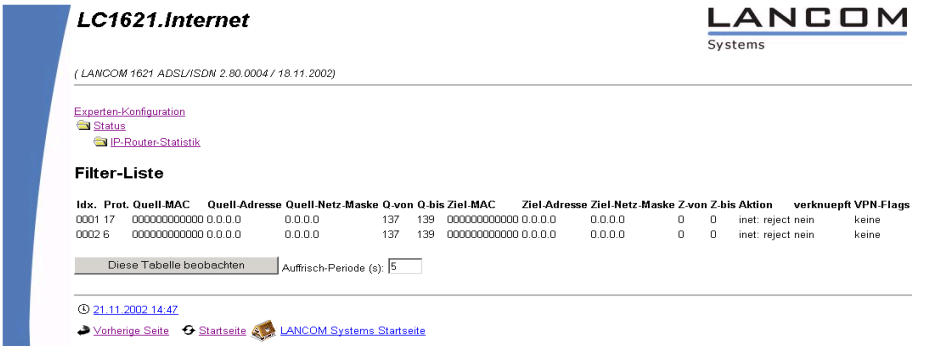
Beachten Sie bitte, dass Filter bei einer manuellen Fehlangabe nicht erzeugt und auch keine Fehlermeldungen ausgegeben werden. Wenn Sie die Filter manuell konfigurieren, sollten Sie in jedem Fall anhand der Filterliste überprüfen, ob die gewünschten Filter erzeugt wurden.

DE

Auf Telnet-Ebene kann der Inhalt der Filterliste auch mit dem Kommando `show filter` *anzeigt werden:*



Die Filterliste hat den folgenden Aufbau (incl. der per Default eingerichteten NetBIOS-Filter):



Die einzelnen Felder in der Filterliste haben folgende Bedeutung:

Eintrag	Beschreibung
Idx.	laufender Index
Prot	zu filterndes Protkoll, also z.B. 6 für TCP oder 17 für UDP
Quell-MAC	Ethernet-Quelladresse des zu filternden Pakets oder 000000000000, wenn der Filter für alle Pakete gelten soll
Quell-Adress	Quell-IP-Adresse oder 0.0.0.0, wenn der Filter für alle Pakete gelten soll
Quell-Netzmaske	Quell-Netzmaske, die zusammen mit der Quell-IP-Adresse das Quell-Netz bestimmt, oder 0.0.0.0, wenn der Filter für Pakete aus allen Netzen gelten soll

DE

Eintrag	Beschreibung
Q-von	Start-Quellport der zu filternden Pakete.
Q-bis	End-Quellport der zu filternden Pakete. Spannt zusammen mit dem Start-Quellport einen Portbereich auf, in dem der Filter wirksam ist. Sind Start und Endport 0, so gilt der Filter für alle Quellports
Ziel-MAC	Ethernet-Zieladresse des zu filternden Pakets oder 000000000000, wenn der Filter für alle Pakete gelten soll
Ziel-Adresse	Ziel-IP-Adresse oder 0.0.0.0, wenn der Filter für alle Pakete gelten soll
Ziel-Netzmaske	Ziel-Netzmaske, die zusammen mit der Ziel-IP-Adresse das Ziel-Netz bestimmt, oder 0.0.0.0, wenn der Filter für Pakete zu allen Netzen gelten soll
Z-von	Start-Zielport der zu filternden Pakete.
Z-bis	End-Zielport der zu filternden Pakete. Spannt zusammen mit dem Start-Zielport einen Portbereich auf, in dem der Filter wirksam ist. Sind Start und Endport 0, so gilt der Filter für alle Zielports
Aktion	In dieserSpalte wird die "Haupaktion", also die Aktion textuell ausgegeben, die bei überschreiten des ersten Limits ausgeführt wird. Das erste Limit kann auch ein implizietes Limit sein, so z.B. wenn nur ein Limit zur Beschränkung des Durchsatzes konfiguriert wurde, so wird ein implizites Limit, das mit einer "accept" Aktion verknüpft ist eingefügt. Als Hauptaktion wird in diesem Fall "accept" ausgegeben. Die vollständigen Aktionen lassen sich über das Kommando `show filter` anzeigen
verknuepft	Gibt an, ob es sich bei dieser Regel um eine "First Match"-Regel handelt (verknuepft = Nein). Nur bei verknuepften Regeln werden im Falle des Zutreffens dieser Regel auch weitere Regeln ausgewertet.
VPN-Flags	Die in der Regelliste definierten VPN-Flags (VPN-Only, ignore)

Die Verbindungsliste

In der Verbindungstabelle werden Quelladresse, Zieladresse, Protokoll, Quellport, Zielport, etc. einer Verbindung nachgehalten sowie mögliche Aktionen gespeichert. Diese Tabelle ist sortiert nach Quelladresse,

Zieladresse, Protokoll, Quellport und Zielport des Pakets, das den Eintrag in der Tabelle hervorgerufen hat. Die Tabelle enthält die folgenden Elemente:

Element	Bedeutung
Src-Addr.	Quell-Adresse der Verbindung
Dst-Addr.	Ziel-Adresse der Verbindung
Protocol	verwendetes Protokoll (TCP/UDP etc.) Das Protokoll wird dezimal angegeben
Src.-Port	Quellport der Verbindung. Der Port wird nur bei portbehafteten Protokollen (TCP/UDP) oder Protokollen, die ein vergleichbares Feld besitzen (ICMP/ GRE) angegeben
Dst.-Port	Zielport der Verbindung (bei UDP-Verrbidnungen wird dieser erst mit der ersten Antwort besetzt)
Timeout	Jeder Eintrag altert mit der Zeit aus dieser Tabelle heraus, damit die Tabelle bei "gestorbenen" Verbindungen nicht überläuft
Flags	In den Flags wird der Zustand der Verbindung und weitere (interne) Informationen in einem Bitfeld gespeichert. Als Zustände sind folgende Werte möglich: **new**, **establish**, **open**, **closing**, **closed**, **rejected** (enstsprechend der TCP-Flags: SYN, SYN ACK, ACK, FIN, FIN ACK und RST) UDP-Verbindungen kennen nun die Zustände **new**, **open** und **closing** (letzteren nur, wenn die UDP-Verbindung mit einem zustandsbehafteten Steuerkanal verknüpft ist. Dies ist z.B. beim Protokoll H.323 der Fall)
Rule	Name der Regel, die den Eintrag erzeugt hat (diese bestimmt auch die auszuführenden Aktionen), wenn ein passendes Paket empfangen wird.

Portsperrliste

Wenn als Aktion die Sperrung des Zielports auf dem Zielrechner ausgewählt wurde, so werden Adresse, Protokoll und Port des Zielrechners in der Portsperrtabelle abgelegt. Diese Tabelle ist ebenfalls eine sortierte

halbdynamische Tabelle. Die Sortierung erfolgt nach Adresse, Protokoll und Port. Die Tabelle enthält die folgenden Elemente:

Element	Bedeutung
Address	Adresse des Rechners, für den die Sperre gelten soll
Protocol	verwendetes Protokoll (TCP/UDP etc.) Das Protokoll wird dezimal angegeben
Port	zu sperrender Port auf dem Rechner. Wenn das jeweilige Protokoll nicht Portbehaftet ist, dann wird das gesamte Protokoll für diesen rechner gesperrt
Timeout	Dauer der Sperre in Minuten
Filter-Rule	Name der Regel, die den Eintrag erzeugt hat (diese bestimmt auch die auszuführenden Aktionen), wenn ein passendes Paket empfangen wird.

Hostsperrliste

Wenn als Aktion eines Filters die Sperrung des Absenders ausgewählt wurde, so werden Adresse des Rechners in der Hostsperrtabelle abgelegt. Diese Tabelle ist eine nach der Absenderadresse sortierte halbdynamische Tabelle und enthält die folgenden Elemente:

Element	Bedeutung
Address	Adresse des Rechners, der gesperrt werden soll
Timeout	Dauer der Sperre in Minuten
Filter-Rule	Name der Regel, die den Eintrag erzeugt hat (diese bestimmt auch die auszuführenden Aktionen), wenn ein passendes Paket empfangen wird.

DE

2.3 Abwehr von Einbruchsversuchen: Intrusion Detection

Einbruchsversuche in das lokale Netzwerk oder auf die zentrale Firewall werden über das Intrusion-Detection-System (IDS) des *LANCOM* erkannt, abgewehrt und protokolliert. Dabei kann zwischen Protokollierung im Gerät (Logging), E-Mail-Benachrichtigung, SNMP-Traps oder SYSLOG-Alarmen gewählt werden.

Als typische Einbruchsversuche kann man gefälschte Absender-Adressen ("IP-Spoofing") und Portscans ansehen, sowie den Missbrauch spezieller Protokolle wie z.B. FTP, um einen Port im angegriffenen Rechner und der davor hängenden Firewall zu öffnen.

Die Verhaltensweise des *LANCOM* Intrusion Detection Systems können Sie hier konfigurieren:

Konfigurationstool	Aufruf
LANconfig	Firewall/QoS / IDS
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / Firewall
Terminal/Telnet	`/Setup/IP-Router-Modul/Firewall`

IP-Spoofing

Beim IP-Spoofing gibt sich der Absender eines Pakets als ein anderer Rechner aus. Dies geschieht entweder, um Firewalls überlisten, die Paketen aus dem eigenen Netz mehr Vertrauen schenken als Paketen aus fremden Netzen, oder um den Urheber eines Angriffs (z.B. Smurf) zu verschleiern.

Die *LANCOM* Firewall schützt sich davor durch Routenprüfung, d.h. sie überprüft, ob das Paket überhaupt über das Interface empfangen werden durfte, von dem es empfangen wurde.

Portscan-Erkennung

Das Intrusion-Detection System des *LANCOM* versucht Portscans zu erkennen, zu melden und geeignet auf den Angriff zu reagieren. Dies geschieht ähnlich der Erkennung eines ‘SYN Flooding’-Angriffs (siehe 'SYN Flooding' auf Seite 75): Es werden auch hier die "halboffenen" Verbindungen gezählt, wobei ein TCP-Reset, das vom gescannten Rechner gesendet wird, die "halboffene" Verbindung weiterhin offen lässt.

DE

Wenn eine bestimmte Anzahl von halboffenen Verbindungen zwischen dem gescannten und dem scannenden Rechner existiert, so wird dies als Portscan gemeldet.

Ebenso wird der Empfang von leeren UDP-Paketen als versuchter Portscan interpretiert

2.4 Schutz vor "Denial-of-Service"-Angriffen

Angriffe aus dem Internet können neben Einbruchsversuchen auch Angriffe mit dem Ziel sein, die Erreichbarkeit und Funktionstüchtigkeit einzelner Dienste zu blockieren. Daher sind *LANCOM* Geräte mit entsprechenden Schutzmechanismen ausgestattet, die bekannte Hacker-Angriffe erkennen und die Funktionstüchtigkeit garantieren.

2.4.1 Abblocken von DoS-Attacken

Um die Anfälligkeit des Netzes vor DoS-Attacken schon im Vorfeld drastisch zu reduzieren, dürfen Pakete aus entfernten Netzen nur dann angenommen werden, wenn entweder eine Verbindung vom internen Netz aus initiiert wurde, oder die einkommenden Pakete durch einen expliziten Filtereintrag (Quelle: entferntes Netz, Ziel: lokales Netz) zugelassen werden. Diese Maßnahme blockiert bereits eine Vielzahl von Angriffen.

Für alle erlaubten Zugriffe werden im *LANCOM* explizit Verbindungszustand, Quelladressen und Korrektheit von Fragmenten überprüft. Dies geschieht sowohl für einkommende als auch für ausgehende Pakete, da ein Angriff auch aus dem lokalen Netz heraus gestartet werden kann.

Um nicht durch fehlerhafte Konfiguration der Firewall ein Tor für DoS-Angriffe zu öffnen, wird dieser Teil zentral konfiguriert. Konfigurierbar ist dabei:

- die maximale Anzahl von halboffenen Verbindungen zu einem Host (gegen SYN-Flooding)
- ob Fragmente verworfen werden sollen, oder sie vom *LANCOM* reassembliert und geprüft werden sollen

- wie der Administrator bei DoS-Attacken informiert werden soll (Syslog/ E-Mail) :

Konfigurationstool	Aufruf
LANconfig	Firewall/QoS / DoS
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / Firewall
Terminal/Telnet	`/Setup/IP-Router-Modul/Firewall`

Immer aktiv hingegen sind folgende Schutzmechanismen:

- Adressüberprüfung (gegen IP-Spoofing)
- Abblocken von Broadcasts in lokale Netz (gegen Smurf und Co).

2.4.2 Denial-of-Service-Angriffe im Detail

Denial-Of-Service-Angriffe nutzen prinzipielle Schwächen der TCP/IP-Protokolle sowie fehlerhafte Implementationen von TCP/IP-Protokollstacks aus. Zu den Angriffen, die prinzipiellen Schwächen ausnutzen, gehören z.B. SYN-Flood und Smurf, zu den Angriffen, die fehlerhafte Implementationen zum Ziel haben, gehören alle Angriffe, die mit fehlerhaft fragmentierten Paketen operieren (z.B. Teardrop), oder die mit gefälschten Absenderadressen arbeiten (z.B.Land). Im folgenden werden einige dieser Attacken, deren Auswirkungen und mögliche Gegenmaßnahmen beschrieben.

SYN Flooding

Beim SYN-Flooding schickt der Angreifer in kurzen zeitlichen Abständen TCP-Pakete, mit gesetztem SYN-Flag und sich ständig ändernden Quellports auf offene Ports seines Opfers. Der angegriffene Rechner richtet darauf hin eine TCP-Verbindung ein, sendet dem Angreifer ein Paket mit gesetzten SYN- und ACK-Flags und wartet nun vergeblich auf die Bestätigung des Verbindungsaufbaus. Dadurch bleiben dann hunderte "halboffener" TCP-Verbindungen zurück, und verbrauchen Ressourcen (z.B. Speicher) des angegriffenen Rechners. Das ganze kann letztendlich so weit gehen, dass das Opfer keine TCP-Verbindung mehr annehmen kann oder gar aufgrund von Speichermangel abstürzt.

Als Gegenmaßnahme in einer Firewall hilft nur, die Anzahl "halboffener" TCP-Verbindungen, die zwischen zwei Rechnern bestehen zu überwachen und zu

beschränken, d.h. falls weitere TCP-Verbindungen zwischen diesen Rechnern aufgebaut werden, dann müssen diese von der Firewall abgeblockt werden.

Smurf

Der Smurf-Angriff arbeitet zweistufig und legt gleich zwei Netze lahm. Im ersten Schritt wird mit gefälscher Absenderadresse ein Ping (ICMP Echo-Request) an die Broadcastadresse des erste Netzes gesendet, worauf alle Rechner in diesem Netz mit einem ICMP-Echo-Reply and die gefälschte Absenderadresse (die im zweiten Netz liegt) antworten. Wenn die Rate der einkommenden Echo-Requests sowie die Anzahl der antwortenden Rechner hoch genug ist, dann wird zum einen der gesamte einkommende Traffic des zweiten Netzes für die Dauer der Attacke blockiert, zum anderen kann der Besitzer der gefälschten Adresse für die Dauer der Attake keine normalen Daten mehr annehmen. Ist die gefälschte Absenderadresse die Broadcastadresse des zweiten Netzes, so sind sogar alle Rechner in diesem Netz blockiert.

In diesem Fall blockiert die DoS-Erkennung des *LANCOM* das Weiterleiten von Paketen, die an die lokale Broadcastadresse gerichtet sind.

LAND

Beim LAND-Angriff handelt es sich um ein TCP-Paket, dass mit gesetztem SYN-Flag und gefälscher Absender-Adresse an den Opferrechner geschickt wird. Das Pikante dabei ist, dass die gefälschte Absenderadresse gleich der Adresse des Opfers ist. Bei einer unglücklichen Implementierung des TCP wird das auf dieses Paket gesendete SYN-ACK vom Opfer wieder als "SYN" interpretiert und ein neues SYN-ACK gesendet. Dies führt zu einer Endlosschleife, die den Rechner einfrieren lässt.

Ping of Death

Der Ping of Death gehört zu den Angriffen, die Fehler bei der Reassemblierung von fragmentierten Paketen ausnutzen. Dies funktioniert wie folgt:

Im IP-Header befindet sich das Feld "Fragment-Offset" das Angibt, an welcher Stelle das empfangene Fragment in das IP-Paket eingebaut werden soll. Dieses Feld ist 13 Bit lang und gibt den offset in 8 Byte schritten an, und kann somit einen Offset von 0 bis 65528 bilden. Bei einer MTU auf dem Ethernet von 1500 Bytes kann somit ein biz zu 65528 + 1500 - 20 = 67008 Byte großes IP-Paket erzeugt werden, was zu Überläufen von internen Zählern führen kann oder gar Pufferüberläufe provozieren kann und es somit dem Angreifer

gar die Möglichkeit eröffnet, eigenen Code auf dem Opferrechner auszuführen.

Hier bieten sich der Firewall zwei Möglichkeiten:

Entweder, die Firewall reassembliert das gesamte einkommende Paket und prüft dessen Integrität, oder aber es wird nur das Fragment, das über die maximale Paketgröße hinaus geht, verworfen. Im ersten Fall kann die Firewall bei einer fehlerhaften Implementation selbst zum Opfer werden, im zweiten Fall sammeln sich beim Opfer "halb" reassemblierte Pakete an, die erst nach einer gewissen Zeit verworfen werden, wodurch sich ein neuer Denial-Of-Service Angriff ergeben kann, wenn dem Opfer dadurch der Speicher ausgeht.

Teardrop

Der Teardrop-Angriff arbeitet mit überlappenden Fragmenten. Dabei wird nach dem ersten Fragment ein weiteres geschickt, das komplett innerhalb des ersten liegt, d.h. das Ende des zweiten Fragments liegt vor dem Ende des ersten. Wird nun aus Bequemlichkeit des Programmierers des IP-Stack bei der Ermittlung der Länge der zur Reassemblierung zu kopierenden Bytes einfach "neues Ende" - "altes Ende" gerechnet, so ergibt sich ein negativer Wert, bzw. ein sehr großer positiver wert, durch den bei der kopieroperation Teile des Speichers des Opfers überschrieben werden und der Rechner daraufhin abstürzt.

Auch hier hat die Firewall wieder zwei Möglichkeiten:

Entweder sie reassembliert selbst und verwirft ggf. das gesamte Paket, oder sie hält nur minimalen Offset und maximales Ende des Pakets nach und verwirft alle Fragmente, deren Offset oder Ende in diesen Bereich fallen. Im ersten Fall muss die Implementation innerhalb der Firewall korrekt sein, damit diese nicht selbst Opfer wird, im anderen Fall sammeln sich wieder "halb" reassemblierte Pakete beim Opfer.

Bonk/Fragrouter

Bonk ist eine Variante des Teardrop-Angriffs, die jedoch nicht zum Ziel hat den angegriffenen Rechner zum Absturz zu bringen, sondern einfache Portfilter Firewalls, die auch Fragmentierte Pakete akzeptieren auszutricksen und somit in das zu schützende Netz einzudringen. Bei diesem Angriff wird nämlich durch geschickte Wahl des Fragment-Offsets der UDP- oder TCP-Header des ersten Fragments überschrieben. Hierdurch akzeptieren einfache Portfilter-Firewalls das erste Paket und die dazugehörenden Fragmente.

DE

Durch das Überschreiben des Headers im zweiten Fragment, wird so ganz plötzlich aus einem erlaubten Paket ein Paket, das eigentlich in der Firewall geblockt werden sollte.

Auch hier gilt, die Firewall kann entweder selbst Reassemblieren, oder nur das falsche Fragment (und alle nachfolgenden) filtern, mit den bereits oben angedeuteten Problemen der einen oder anderen Lösung.

In der Default-Einstellung sind alle Einstellungen auf "sicher" konfiguriert, d.h. maximal 100 zulässige halboffene Verbindungen von verschiedenen Rechnern (vgl. SYN-Flooding), maximal 50 halboffene Verbindungen von einem Rechner (vgl. Portscan) fragmentierte Pakete werden reassembliert.

2.5 Unsichtbar machen

Eine - nicht unumstrittene - Methode die Sicherheit zu erhöhen, ist das Verstecken des Routers; frei nach der Methode: "Wer mich nicht sieht, wird auch nicht versuchen mich anzugreifen...".

Die entsprechenden Einstellungen (Erklärung siehe unten) können Sie an der folgenden Stellen vornehmen:.

Konfigurationstool	Aufruf
LANconfig	Firewall/QoS / Allgemein
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / Firewall
Terminal/Telnet	`/Setup/IP-Router-Modul/Firewall`

2.5.1 Ping-Blocking

Um dies zu erreichen, kann das *LANCOM* angewiesen werden, ICMP-Echo-Requests nicht mehr zu beantworten. Gleichzeitig werden auch die bei einem "traceroute" benutzten TTL-Exceeded Meldungen unterdrückt, so dass das *LANCOM* weder durch ein "ping" noch ein "traceroute" gefunden werden kann.

Mögliche Einstelungen sind

- Aus
  ICMP Anworten werden nicht blockiert
- Immer
  ICMP Anworten werden immer blockiert

- WAN
  ICMP Anworten werden auf allen WAN-Verbindungen blockiert
- Default Route
  ICMP Anworten werden auf der Default-Router (i.d.R. Internet) blockiert

2.5.2 TCP-Stealth-Modus

Neben ICMP-Meldungen verrät auch das Verhalten bei TCP- und UDP-Verbindungen, ob sich an der angesprochenen Adresse ein Rechner befindet. Je nach umgebendem Netzwerk kann es sinnvoll sein, wenn TCP- und UDP-Pakete einfach verworfen werden, anstatt mit einem TCP-Reset bzw. einer ICMP-Meldung (port unreachable) zu antworten, wenn kein Listener für dem jeweiligen Port existiert. Das jeweils gewünschte Verhalten kann im *LANCOM* eingestellt werden.

Werden Ports ohne Listener versteckt, so ergibt sich auf maskierten Verbindungen das Problem, dass der "authenticate"- bzw. "ident"-Dienst nicht mehr funktioniert (bzw. nicht mehr korrekt abgelehnt wird).

Ein Mail- oder News-Server, der mit Hilfe dieses Dienstes etwaige zusätzliche Informationen vom User anfordert, läuft dann zunächst in einen störenden Timeout, bevor er beginnt, die Mails auszuliefern. Dieser Dienst benötigt also einen eigenen Schalter um ihn zu verstecken bzw. "konform" zu halten.

Die Problematik dabei ist nun allerdings, dass eine Einstellung, die alle Ports versteckt, den ident-Port aber zurückweist, unsinnig ist - denn allein dadurch, dass der ident-Port zurückgewiesen wird, wäre das *LANCOM* zu sehen.

Das *LANCOM* bietet zur Lösung dieses Problems an, ident-Anfragen nur von den Mail und News-Servern abzulehnen, und bei Anfragen von allen anderen Rechnern diese einfach zu verwerfen. Hierzu werden bei der Abfrage eines Mail- (SMTP, POP3 IMAP2) oder Newsservers (NNTP) für eine Kurze Zeit (20 Sekunden) ident-Anfragen von den jeweiligen Servern abgelehnt.

Ist die Zeit abgelaufen, so wird der Port wieder versteckt.

Mögliche Einstellungen sind:

- off
  Alle Ports sind geschlossen und TCP-Pakete werden mit einem TCP-Reset beantwortet

DE

- allways
  Alle Ports sind versteckt und TCP-Pakete werden stillschweigend verworfen.
- WAN
  Auf der WAN-Seite sind alle Ports versteckt und auf der LAN-Seite geschlossen
- Default-Route
  Die Ports sind auf der Default-Route (i.d.R. Internet) versteckt und auf allen anderen Routen geschlossen

Einstellungen zur Sonderbehandlung von ident-Anfragen (nur bei 'Stealth'):

- closed
  Anfragen and den authenticate bzw. ident Port werden mit einem TCP-Reset beantwortet, wenn sie vom kurz zuvor abgefragten Mail- oder News-Server kommen, ansonsten werden sie verworfen.
- stealth
  Pakete an den authenticate bzw. ident Port werden immer stillschweigend verworfen

2.6 Das Versteck – IP-Masquerading (NAT, PAT)

Eine der häufigsten Aufgaben für Router ist heute die Anbindung vieler Arbeitsplätze in einem LAN an das Netz der Netze, das Internet. Jeder soll nach Möglichkeit direkt von seinem Arbeitsplatz aus z.B. auf das Internet zugreifen und sich brandaktuelle Informationen für seine Arbeit holen können.

Damit nicht jeder Arbeitsplatzrechner im gesamten Internet bekannt sein muss: IP-Masquerading heisst das Versteck für alle Rechner im Intranet. Dabei wird nur das Routermodul des *LANCOM* mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt dabei Internet und Intranet.

Wie funktioniert IP-Masquerading?

Das Masquerading nutzt die Eigenschaft der Datenübertragung über TCP/IP aus, dass neben der Quell- und Ziel-Adresse auch Portnummer für Quelle und Ziel verwendet werden. Bekommt der Router nun ein Datenpaket zur Übertragung, merkt er sich die IP-Adresse und den Port des Absenders in

einer internen Tabelle. Dann gibt er dem Paket seine eigene IP-Adresse und eine beliebige neue Portnummer. Diesen neuen Port trägt er ebenfalls in der Tabelle ein und leitet das Paket mit den neuen Angaben weiter.

Die Antwort auf dieses Paket geht nun an die IP-Adresse des Routers mit der neuen Absender-Portnummer. Mit dem Eintrag in der internen Tabelle kann der Router diese Antwort nun wieder dem ursprünglichen Absender zuordnen.

Welche Protokolle können mit IP-Masquerading übertragen werden?

Das IP-Masquerading funktioniert problemlos für all jene IP-Protokolle, die auf TCP, UDP oder ICMP basieren und dabei ausschliesslich über Ports kommunizieren. Zu diesen unproblematischen Protokollen zählt beispielsweise das Basis-Protokoll des World Wide Web: HTTP.

Einzelne IP-Protokolle verwenden zwar TCP oder UDP, kommunizieren allerdings nicht ausschliesslich über Ports. Derartige Protokolle verlangen beim IP-Masquerading eine entsprechende Sonderbehandlung. Zu den vom IP-Masquerading im *LANCOM* unterstützten Protokollen mit Sonderbehandlung gehören:

- FTP (über die Standardports)
- H.323 (im Umfang, wie ihn Microsoft Netmeeting verwendet)
- PPTP
- IPSec
- IRC

Konfiguration des IP-Masquerading

Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle erreichen Sie wie folgt:

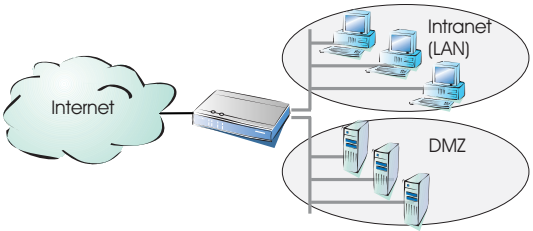
Konfigurationstool	Aufruf
LANconfig	IP-Router / Routing / Routing-Tabelle
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / IP-Routing-Tab
Terminal/Telnet	`/Setup/IP-Router-Modul/IP-Routing-Tab`

DE

Mehrere Adressen für den Router

Bei Masquerading treffen zwei gegensätzliche Forderungen an den Router aufeinander: Zum einen soll er eine im lokalen Netz gültige Intranet-IP-Adresse haben, damit er aus dem LAN erreichbar ist, zum anderen soll er eine im Internet gültige Adresse haben. Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, hilft hier nur eins: Zwei IP-Adressen müssen her. Dazu wird die Internet-IP-Adresse bei den meisten Standard-Internetzugängen dem Router im Zuge der PPP-Verhandlung dynamisch zugewiesen.

Auf der lokalen Seite kann der Router zwei unterschiedliche IP-Adresskreise verwalten: Das Intranet (LAN) und die DMZ ('De-Militarized Zone'). Die DMZ bezeichnen einen eigenen Bereich, welcher in der Regel für aus dem Internet erreichbare Server verwendet wird:



Mit der Option **Maskierung** in der Routing-Tabelle informieren Sie den Router darüber, ob die lokalen Intranet- oder DMZ-Adressen hinter der Internet-IP-Adresse des Routers versteckt werden sollen:

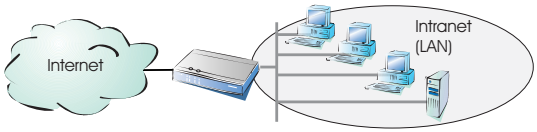
- 'IP-Masquerading abgeschaltet': Es wird keine Maskierung durchgeführt. Diese Variante ist für Internetzugänge mit mehreren statischen IP-Adressen (einzutragen unter DMZ-Adresse und DMZ-Netzmaske) vorgesehen, mit denen ausschließlich Server an das Internet gekoppelt werden, oder aber um z.B. zwei Intranet-Subnetze via VPN zu koppeln.
- 'Intranet und DMZ maskieren (Standard)':
  In dieser Einstellung werden alle lokalen Adressen maskiert. Neben dem Intranet (LAN) kann zusätzlich noch ein zweites lokales Netz mit privaten Adressen an das Internet angebunden werden.
- 'Nur Intranet maskieren':
  Diese Einstellung ist insbesondere für Internetzugänge mit mehreren statischen IP-Adressen geeignet. Anders als beim Fall 'IP-Masquerading abgeschaltet' steht jedoch neben der DMZ noch der Intranet-Adresskreis mit maskierten, privaten IP-Adressen für ein LAN zur Verfügung.

Die Zuweisung der DMZ und der Intranet Adressen des *LANCOM* kann wie folgt vorgenomen werden:

Konfigurationstool	Aufruf
LANconfig	TCP/IP / Allgemein
WEBconfig	Experten-Konfiguration / Setup / TCP-IP--Modul
Terminal/Telnet	`/Setup/TCP-IP-Modul`

Einfaches und inverses Masquerading

Maskierung funktioniert in beide Richtungen: Wenn ein Rechner aus dem LAN ein Paket ins Internet schickt, wird das lokale Netz hinter der IP-Adresse des Routers maskiert (einfaches Masquerading).



Schickt umgekehrt ein Rechner aus dem Internet ein Paket z.B. an einen FTP-Server im LAN ('exposed host'), so sieht es für diesen Rechner so aus, als wäre der Router der FTP-Server. Der Router liest aus dem Eintrag in der Service-Tabelle die IP-Adresse des FTP-Servers im LAN. Das Paket wird an diesen Rechner weitergeleitet. Alle Pakete, die vom FTP-Server im LAN kommen (Antworten des Servers), werden hinter der IP-Adresse des Routers versteckt.

Der kleine Unterschied:

- Der Zugriff von aussen auf einen Dienst (Port) im Intranet muss vorher durch Angabe einer Port-Nummer definiert werden. In einer Service-Tabelle wird dazu der Ziel-Port mit der Intranet-Adresse z.B. des FTP-Servers angegeben.

DE

- Beim Zugriff aus dem LAN auf das Internet hingegen wird der Eintrag in der Tabelle mit Port- und IP-Adress-Informationen durch den Router selbst vorgenommen.

  Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also **gleichzeitig** 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

  Nach einer einstellbaren Zeit geht der Router jedoch davon aus, dass der Eintrag nicht mehr benötigt wird, und löscht ihn selbständig wieder aus der Tabelle.

Konfiguration des inversen Masqueradings

Konfigurationstool	Aufruf
LANconfig	IP-Router / Masq. / Service-Tabelle
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / Masquerading / Service-Tabelle
Terminal/Telnet	`/Setup/IP-Router-Modul/Masquerading/Service-Tabelle`

Stateful-Inspection und inverses Maquerading

Wenn im Masquerading-Modul ein Port freigeschaltet wird (d.h. alle auf diesem Port empfangenen Pakete sollen an einen Rechner im lokalen Netz weitergeleitet werden), so erfordert dies bei einer Deny-All Firewall-Strategie einen zusätzlichen Eintrag in der Stateful-Inspection Firewall, der den Zugriff aller Rechner auf den jeweiligen Server ermöglicht.

2.6.1 Unmaskierter Internet-Zugang für Server in der DMZ

Das im vorangegangenen Abschnitt beschriebene inverse Maskieren erlaubt zwar, jeweils einen bestimmten Dienst zu exponieren (z.B. je ein Web-, Mail- und FTP-Server), hat aber z.T. weitere Einschränkungen:

- Der betreffende Dienst des 'exposed host' muss vom Maskierungsmodul unterstützt und verstanden werden. Zum Beispiel benutzen einige VoIP-Server nicht-standarisierte, proprietäre Ports für eine erweiterte Signalisierung. Dadurch können solche Server-Dienste nur an Verbindungen ohne Maskierung betrieben werden.
- Vom Sicherheitsstandpunkt muss beachtet werden, dass sich der 'exposed host' im lokalen Netz befindet. Falls der Rechner unter die

Kontrolle eines Angreifers gebracht wird, so kann dieser Rechner als Ausgangsbasis für Angriffe gegen weitere Maschinen im lokalen Netz missbraucht werden.

Um Angriffe von 'geknackten' Servern auf das lokale Netz zu verhindern, verfügen einige LANCOM über ein dediziertes DMZ-Interface (LANCOM 7011 VPN), oder können die LAN-Ports per Hardware auf Ethernet-Ebene voneinander trennen (LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN beim Betrieb des Switches im 'Private Mode').

Zwei lokale Netze - Betrieb von Servern in der DMZ

Hierfür ist ein Internetzugang mit mehreren statischen IP-Adressen notwendig. Bitte kontaktieren Sie Ihren ISP ggfs. für ein entsprechendes Angebot.

Ein Beispiel: Sie erhalten die Internet IP-Netzadresse 123.45.67.0 mit der Netzmaske 255.255.255.248 vom Provider zugewiesen. Dann könnten Sie die IP-Adressen wie folgt verteilen:

DMZ IP-Adresse	Bedeutung/Verwendung
123.45.67.0	Netzadresse
123.45.67.1	*LANCOM* als Gateway für das **Intranet**
123.45.67.2	Gerät im lokalen Netzwerk, das unmaskierten Zugang ins Internet erhalten soll, beispielsweise ein Web-Server am **DMZ**-Port
123.45.67.3	Broadcast-Adresse

Alle Rechner und Geräte im Intranet haben keine öffentliche IP-Adresse und treten daher mit der IP-Adresse des *LANCOM* (123.45.67.1) im Internet auf.

Trennung von Intranet und DMZ

Obwohl Intranet und DMZ vielleicht bereits schon auf Ethernet-Ebene durch dedizierte Interfaces voneinander getrennt sind, so muss in jedem Fall noch eine Firewall-Regel zur Trennung auf IP-Ebene eingerichtet werden!
Dabei soll der Server-Dienst vom Internet und aus dem Intranet heraus erreichbar sein, aber jeglicher IP-Traffic aus der DMZ Richtung Intranet soll unterbunden werden. Für das obige Beispiel ergäbe sich folgendes:

- Bei einer "Allow-All"-Strategie (default): Zugriff von "123.45.67.2" auf "Alle Stationen im lokalen Netz" verbieten

DE

- Bei einer "Deny-All"-Strategie (siehe 'Aufbau einer expliziten "Deny-All"-Strategie' auf Seite 64): Zugriff von "Alle Stationen im lokalen Netz" auf "123.45.67.2" erlauben

2.7 Den ISDN-Einwahlzugang absichern

Bei einem Gerät mit ISDN-Anschluss kann sich prinzipiell jeder Teilnehmer in Ihren *LANCOM* einwählen. Um unerwünschte Eindringlinge zu vermeiden, müssen Sie deshalb einen besonderen Augenmerk auf die Absicherung des ISDN-Zugangs legen.

Die Absicherungsfunktionen des ISDN-Zugangs können in zwei Gruppen eingeteilt werden:

- Identifikationskontrolle
  - Zugangsschutz mit Name und Passwort
  - Zugangsschutz über die Anruferkennung
- Rückruf an festgelegte Rufnummern

2.7.1 Die Identifikationskontrolle

Zur Identifikationskontrolle kann entweder der Name der Gegenstelle oder die sogenannte Anruferkennung herangezogen werden. Die Anruferkennung ist die Telefonnummer des Anrufers, die bei ISDN normalerweise mit dem Anruf an die Gegenstelle übermittelt wird.

Welcher „Identifier" zur Erkennung des Anrufers verwendet werden soll, wird im folgender Liste eingestellt:

Konfigurationstool	Aufruf
LANconfig	Kommunikation / Rufannahme
WEBconfig	Experten-Konfiguration / Setup / WAN-Modul / Schutz
Terminal/Telnet	`/Setup/WAN-Modul/Schutz`

Zur Auswahl stehen die folgenden Möglichkeiten:

- kein Schutz: Anrufe aller Gegenstellen werden angenommen.
- nach Nummer: Es werden nur Anrufe angenommen, deren Anschlusskennungen (CLIP) in der Nummernliste eingetragen sind.

- nach geprüfter Nummer: Es werden nur Anrufe angenommen, deren Anschlusskennungen (CLIP) einerseits in der Nummernliste eingetragen sind, sowie andererseits von der Vermittlungsstelle für korrekt befunden wurden.

Die Identifizierung setzt natürlich voraus, dass die entsprechende Information vom Anrufer auch übermittelt wird.

Überprüfung des Benutzernamens und des Kennwortes

Bei einer PPP-Einwahl wird zunächst ein Benutzername (und in Verbindung mit PAP, CHAP oder MS-CHAP auch ein Passwort) beim Verbindungsaufbau an die Gegenstelle übertragen. Wählt sich ein Computer in den *LANCOM* ein, so fragt die verwendete Verbindungssoftware, beispielsweise das DFÜ-Netzwerk unter Windows, den zu übermittelnden Benutzernamen und das Passwort in einem Eingabefenster ab.

Baut der Router selber eine Verbindung auf, etwa zu einem Internet Service Provider, so verwendet er seinerseits Benutzername und Passwort aus der PPP-Liste. Ist dort kein Benutzername eingetragen, wird stattdessen der Gerätename verwendet.

Die PPP-Liste finden Sie wie folgt:

Konfigurationstool	Aufruf
LANconfig	Kommunikation / Protokolle / PPP-Liste
WEBconfig	Experten-Konfiguration / Setup / WAN-Modul / PPP-Liste
Terminal/Telnet	`/Setup/WAN-Modul/PPP-Liste`

Ausserdem kann beim PPP-Protokoll auch der Anrufer von der Gegenstelle eine Authentifizierung verlangen. Er fordert dann die Gegenstelle zur Übermittlung eines Benutzer- bzw. Gerätenamens und eines Passwortes auf.

Die Sicherungsverfahren PAP, CHAP oder MS-CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem LANCOM z.B. einen Internet Service Provider anwählen. Sie werden den ISP wahrscheinlich nicht dazu bewegen können, eine Anfrage an ihn nach einem Passwort zu beantworten …

Überprüfung der Nummer

Beim Anruf über eine ISDN-Leitung wird in den meisten Fällen über den D-Kanal die Rufnummer des Anrufers übertragen, schon bevor eine Verbindung zustande kommt (CLI – **C**alling **L**ine **I**dentifier).

DE

Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen. Ist ein Schutz im *LANCOM* über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekannten Rufnummern abgelehnt.

Der Schutz mit Hilfe der Rufnummer kann mit allen B-Kanal-Protokollen (Layern) verwendet werden.

2.7.2 Der Rückruf

Eine besondere Variante des Zugriffsschutzes wird mit der Rückruffunktion erreicht: Dazu wird in der Namenliste für den gewünschten Anrufer die Option 'Rückruf' aktiviert und ggf. die Rufnummer angegeben.

Konfigurationstool	Aufruf
LANconfig	Kommunikation / Gegenstellen / Namenliste
WEBconfig	Experten-Konfiguration / Setup / WAN-Modul / Namenliste
Terminal/Telnet	`/Setup/WAN-Modul/Namenliste`

Mit den Einstellungen in Namen- und Nummernliste können Sie das Rückrufverhalten Ihres Routers steuern:

- Der Router kann den Rückruf ablehnen.
- Er kann eine voreingestellte Rufnummer zurückrufen.
- Er kann zunächst den Namen überprüfen und dann eine voreingestellte Rufnummer zurückrufen.
- Die Rufnummer für den Rückruf kann vom Anrufer frei eingegeben werden.

Und ganz nebenbei steuern Sie über die Einstellungen die Verteilung der Kosten für die Verbindung. Ist in der Namenliste ein Rückruf 'Nach Name' vereinbart, übernimmt der rückrufende Router alle Gebühren bis auf eine, die für die Namensübermittlung benötigt wird. Ebenfalls eine Einheit fällt für den Anrufer an, wenn der Anrufer nicht über CLIP (**C**alling **L**ine **I**dentifier **P**rotocol) identifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg (Rückruf über den D-Kanal).

Eine besonders effektive Methode des Rückrufs ist das Fast-Call-Back-Verfahren (zum Patent angemeldet). Dieses Verfahren beschleunigt die Rückrufprozedur beträchtlich. Das Verfahren funktioniert nur dann, wenn es von beiden Gegenstellen unterstützt wird. Alle aktuellen *LANCOM*-Router beherrschen das Fast-Call-Back-Verfahren.

Weitere Informationen zum Rückruf finden Sie im Abschnitt 'Rückruf-Funktionen' auf Seite 145.

2.8 Die Sicherheits-Checkliste

In der folgenden Checkliste finden Sie die wichtigsten Sicherheitsfunktionen im Überblick. Damit Sie ganz sicher sein können, nichts Wesentliches bei der Sicherheitskonfiguration Ihres *LANCOM* übersehen zu haben.

- **Haben Sie ein Passwort für die Konfiguration vergeben?**

  Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Passworts. Solange Sie kein Passwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Das Feld zur Eingabe des Passworts finden Sie in *LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Es ist insbesondere dann ratsam, ein Passwort zur Konfiguration zu vergeben, wenn Sie die Fernkonfiguration erlauben wollen!

- **Haben Sie die Fernkonfiguration zugelassen?**

  Wenn Sie die Fernkonfiguration nicht benötigen, so schalten Sie sie ab. Wenn Sie die Fernkonfiguration benötigen, so vergeben Sie unbedingt einen Passwortschutz für die Konfiguration (siehe vorhergehender Abschnitt). Das Feld zur Abschaltung der Fernkonfiguration finden Sie ebenfalls in *LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'.

- **Haben Sie die SNMP-Konfiguration mit einem Passwort versehen?**

  Schützen Sie auch die SNMP-Konfiguration mit einem Passwort. Das Feld zum Schutz der SNMP-Konfiguration mit einem Passwort finden Sie ebenfalls in *LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'.

- **Haben Sie den Remote Access erlaubt?**

  Wenn Sie keinen Remote Access benötigen, schalten Sie die Rufannahme aus, indem Sie in *LANconfig* im Konfigurationsbereich

DE

'Kommunikation' auf der Registerkarte 'Rufannahme' eine Rufannahme nach Nummer wählen und die Nummernliste leer lassen.

- **Haben Sie die Rückrufoptionen für den Remote Access aktiviert, und ist CLI eingeschaltet?**

  Beim Anruf über eine ISDN-Leitung wird in den meisten Fällen über den D-Kanal die Rufnummer des Anrufers übertragen, schon bevor eine Verbindung zu Stande kommt (CLI – **C**alling **L**ine **I**dentifier). Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen (dieser Rückruf über den D-Kanal wird vom Windows-DFÜ-Netzwerk nicht unterstützt). Ist ein Schutz im *LANCOM* über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekannten Rufnummern abgelehnt.

- **Haben Sie die Firwall aktiviert?**

  Die Stateful-Inspection Firewall der *LANCOM* Router sorgt dafür, dass Ihr lokales Netzwerk von aussen nicht angegriffen werden kann. Die Firewall können Sie in *LANconfig* unter 'Firewall/Qos' auf der Registerkarte 'Allgemein' einschalten.

- **Haben Sie IP-Masquerading aktiviert?**

  IP-Masquerading heisst das Versteck für alle lokalen Rechner beim Zugang ins Internet. Dabei wird nur das Router-Modul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle finden Sie in *LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router'.

- **Verwenden Sie eine 'Deny-All' Firewall-Strategie?**

  Für maximale Sicherheit und Kontrolle unterbinden Sie zunächst jeglichen Datentransfer durch die Firewall. Nur die Verbindungen, die explizit gestattet sein sollen, sind in die Firewall einzutragen. Damit wird 'Trojanern' und bestimmten E-Mail-Viren der Kommunikations-Rückweg entzogen. Die Firewall-Regeln finden Sie in *LANconfig* unter 'Firewall/ Qos' auf der Registerkarte 'Regeln' zusammengefasst. Eine Anleitung dazu findet sich unter 'Aufbau einer expliziten "Deny-All"-Strategie' auf Seite 64.

- **Haben Sie bestimmte Stationen von dem Zugriff auf den Router ausgeschlossen?**

  Mit einer speziellen Filter-Liste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfigurationssitzungen über *LANconfig*, *WEBconfig*, Telnet oder TFTP bezeichnet. Standardmässig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf den Router gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen. Die Zugangsliste finden Sie in *LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein'.

- **Lagern Sie Ihre abgespeicherte *LANCOM*-Konfiguration an einem sicheren Ort?**

  Schützen Sie abgespeicherte Konfigurationen an einem sicheren Ort vor unberechtigtem Zugriff. Eine abgespeicherte Konfiguration könnte sonst von einer unberechtigten Person in ein anderes Gerät geladen werden, wodurch z.B. Ihre Internet-Zugänge auf Ihre Kosten benutzt werden können.

DE

3 Quality-of-Service

Dieses Kapitel widmet sich dem Thema Qualität: Unter dem Oberbegriff Quality-of-Service (kurz: QoS) sind die Funktionen des *LANCOM* zusammengefasst, die sich mit der Sicherstellung von bestimmten Dienstegüten befassen. Dieser Funktionen werden - wie im vorausgehenden Kapitel beschrieben - durch die Firewall bereitgestellt (siehe 'Quality-of-Service Objekte' auf Seite 53).

Das hat den Vorteil, dass die QoS-Funktionen mit den vorhandenen, mächtigen Klassifizierungsmethoden der Firewall (z.B. Einschränkung auf Subnetze, einzelne Arbeitsstationen oder bestimmte Dienste) erfolgen kann. Somit können QoS-Features auch für Anwendungen zum Einsatz kommen, in denen die Applikationen von sich aus keine QoS-Methoden bereitstellen.

In den folgenden Abschnitten werden die zugrundeliegenden Konzepte genauer erläutert.

3.1 Überblick

Einige LANCOM Modelle bieten QoS zusätzlich zum Layer 3 der IP QoS auch auf anderen Netzwerkschichten an, z.B. auf ATM-Ebene. Die Beschreibung dieser speziellen Features entnehmen Sie bitte den entsprechenden Benutzerhandbüchern dieser Modelle.

Folgende QoS-Funktionen stehen im *LANCOM* zur Verfügung. Damit können entsprechende Qualitätsregeln ("QoS-Policies") zum Management der Bandbreiten erstellt werden ("Traffic-Engineering").

3.1.1 Garantierte Mindestbandbreiten

Hiermit geben Sie Vorfahrt für unternehmenskritische Applikationen, VoIP-TK-Anlagen oder bestimmte Benutzergruppen.

Volldynamisches Bandbreitenmanagement.

Das Bandbreitenmanagement erfolgt dynamisch. Dies bedeutet, dass z.B. eine garantierte Mindestbandbreite nur solange zur Verfügung stellt wird, wie auch tatsächlich entsprechender Datentransfer anliegt.

Ein Beispiel:

DE

Zur Übertragung von VoIP-Daten eines entsprechenden VoIP-Gateways immer soll eine Bandbreite von 256 kBit/s garantiert werden. Ein einzelne VoIP-Verbindung benötige 32 kBit/s.

Solange niemand telefoniert, steht die gesamte Bandbreite anderen Diensten zur Verfügung. Pro VoIP-Verbindung stehen den anderen Anwendungen jeweils 32 kBit/s weniger zur Verfügung, bis 8 VoIP-Verbindungen aktiv sind. Sobald eine VoIP-Verbindung beendet ist, steht die entsprechende Bandbreite wieder allen anderen Anwendungen zur Verfügung.

Für das korrekte Funktionieren dieses Mechanismus darf die Summe der konfigurierten Mindestbandbreiten die effektiv zur Verfügung stehende Sendebandbreite nicht übersteigen.

3.1.2 Limitierte Maximalbandbreiten

Hiermit schränken Sie z.B. die gesamte oder verbindungsbezogene Maximalbandbreite für Serverzugriffe ein.

Ein Beispiel:

Sie betreiben einen Webserver und ein lokales Netzwerk an einem gemeinsamen Internetzugang.

Um zu verhinden, dass Ihr Produktivnetz (LAN) von vielen Internetzugriffen auf Ihren Webserver lahmgelegt wird, limitieren Sie alle Serverzugriffe auf die Hälfte der Ihnen zur Verfügung stehenden Bandbreite. Um ferner sicherzustellen, dass Ihre Serverdienste vielen Usern gleichzeitig und gleichberechtigt zugute kommen, setzen Sie pro Verbindung zum Server eine bestimmte Maximalbandbreite.

Kombination möglich

Minimal- und Maximalbandbreiten können kombiniert zusammen verwendet werden. Somit kann die zur Verfügung stehende Bandbreite speziell nach Ihren Erfordernissen z.B. auf bestimmte Benutzergruppen oder Anwendungen verteilen werden.

DE

3.1.3 Type-of-Service (TOS) bzw. DiffServ-Unterstützung

Applikationen werden bevorzugt, die bestimmte Flags im IP-Header setzen. Dazu gehören:

- TOS "Low Delay"
- DiffServ "Expedited Forwarding"
- TOS "High Reliability"

Die IP-Header-Bits des TOS-bzw. DiffServ-Feldes werden im Falle einer VPN-Strecke auch in den umgebenden IP-Header des IPSec-VPN-Paketes kopiert. Somit steht QoS auch für VPN-Strecken über das Internet zur Verfügung, sofern Ihr Provider entsprechende Pakete auch im WAN bevorzugt behandelt.

3.2 IP Quality-of-Service im Detail

Quality-of-Service wird im *LANCOM* dadurch erzeugt, dass verschiedene Warteschlangen mit unterschiedlichen Bearbeitungsprioritäten zur Verfügung stehen.

Die QoS-Features stehen nur für die Senderichtung zur Verfügung, da in der Regel das lokale Netzwerk (LAN) ein deutlich höhere Bandbreite als der Weitverkehrszugang (WAN) hat.

Folgende Warteschlangen stehen zur Verfügung:

- Urgent-Queue I

  Hier landen alle Pakete mit gesetztem TOS "Low Delay"- bzw. DiffServ "Expedited Forwarding"-Attribut. Diese Queue wird immer vor allen anderen abgearbeitet. Ebenfalls werden alle Pakete, die eine bestimme Mindestbandbreite zugewiesen bekommen haben in dieser Queue - allerdings nur solange, wie die garantierte Minimalbandbreite nicht überschritten wird. Ferner können TCP-Steuerungspakete ebenfalls durch diese Queue bevorzugt versendet werden (siehe 'SYN/ACK-Speedup' auf Seite 135).

- Urgent Queue II

  Hier landen alle Pakete, die eine garantierte Mindestbandbreite zugewiesen bekommen haben, deren Verbindung diese aber überschritten hat.

  Solange das Intervall für die Mindestbandbreite läuft (d.h. bis zum Ende der laufenden Sekunde) werden alle Pakete in dieser Queue ohne weitere besondere Priorität behandelt. Alle Pakete in dieser Queue, der

"gesicherten Queue" und der "Standard-Queue" teilen sich von nun an die vorhandene Bandbreite. Die Pakete werden beim Senden in der Reihenfolge aus den Queues geholt, in der sie auch in die Queues gestellt wurden. Läuft das Intervall ab, werden alle Blöcke, die sich zu diesem Zeitpunkt noch in der "Urgent-Queue II" befinden, bis zum Überschreiten der jeweils zugeteilten Mindestbandbreite wieder in die "Urgent-Queue I" gestellt, der Rest verbleibt in der "Urgent-Queue II".

Mit diesem Verfahren wird sichergestellt, dass priorisierte Verbindungen den restlichenDatenverkehr nicht erdrücken.

- gesicherte Queue

  Diese Warteschlange hat keine gesonderte Priorität. Jedoch werden Pakete in dieser Queue niemals verworfen (garantierte Übertragung). Diese Queue wird benutzt für Pakete, die das TOS-Attribut "High Reliability" gesetzt haben.

- Standard-Queue

  Die Standard-Warteschlange enthält allen nicht gesondert klassifizierte Datenverkehr. Pakete in dieser Queue werden zuerst verworfen, sofern die Datenpakete nicht schnell genug abgeliefert werden können.

DE

4 Server-Dienste

Ein *LANCOM* bietet eine Reihe von Dienstleistungen für die PCs im LAN an. Es handelt sich dabei um zentrale Funktionen, die von den Arbeitsplatzrechnern genutzt werden können. Im Einzelnen handelt es sich um:

- Automatische Adressverwaltung mit DHCP
- Namenverwaltung von Rechnern und Netzwerken mit DNS
- Protokollierung von Netzverkehr mit SYSLOG
- Gebührenerfassung
- Bürokommunikations-Funktionen mit *LANCAPI*
- Zeit-Server

4.1 Automatische IP-Adressverwaltung mit DHCP

Für einen reibungslosen Betrieb in einem TCP/IP-Netzwerk benötigen alle Geräte in einem lokalen Netzwerk eindeutige IP-Adressen.

Zusätzlich brauchen sie noch die Adressen von DNS- und NBNS-Servern sowie eines Standard-Gateways, über das Datenpakete von lokal nicht erreichbaren Adressen geroutet werden sollen.

Bei einem kleinen Netzwerk ist es durchaus noch denkbar, allen Rechnern im Netz „von Hand" diese Adressen einzutragen. Bei einem großen Netz mit vielen Arbeitsplatzrechnern wird das jedoch leicht zu einer unüberschaubaren Aufgabe.

In solchen Fällen bietet sich die Verwendung des DHCP (Dynamic Host Configuration Protocol) an. Über dieses Protokoll kann ein DHCP-Server in einem TCP/IP-basierten LAN den einzelnen Stationen die benötigten Adressen dynamisch zuweisen.

4.1.1 Der DHCP-Server

LANCOM kann als DHCP-Server die IP-Adressen in seinem TCP/IP-Netz verwalten. Dabei teilt er den Arbeitsplatzrechnern die folgenden Parameter mit:

- IP-Adresse
- Netzmaske
- Broadcast-Adresse

DE

- Standard-Gateway
- DNS-Server
- NBNS-Server
- Gültigkeitsdauer der zugewiesenen Parameter

Der DHCP-Server entnimmt die IP-Adressen entweder aus einem frei definierten Adress-Pool oder ermittelt die Adressen selbstständig aus der eigenen IP-Adresse (oder Intranet-Adresse).

Ein völlig unkonfiguriertes Gerät kann sogar im DHCP-Automodus die IP-Adressen für sich selbst und für die Rechner im Netz selbstständig festlegen.

Im einfachsten Fall müssen Sie daher nur das neue Gerät im Auslieferungszustand in einem Netz ohne andere DHCP-Server anschließen und einschalten. Der DHCP-Server regelt im Zusammenspiel mit *LANconfig* über einen Assistenten dann alle weiteren Adresszuweisungen im lokalen Netz selbst.

4.1.2 DHCP – 'Ein', 'Aus' oder 'Auto'?

Der DHCP-Server kann drei verschiedene Zustände annehmen:

- 'Ein': Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adress-Pools) überprüft.
  - Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an.
  - Bei einer fehlerhaften Konfiguration (z.B. ungültige Pool-Grenzen) wird der DHCP-Server wieder abgeschaltet und wechselt in den Zustand 'Aus'.
- 'Aus': Der DHCP-Server ist dauerhaft abgeschaltet.
- 'Auto': In diesem Zustand sucht das Gerät nach dem Einschalten im lokalen Netz automatisch nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LAN-Rx/Tx-LED.
  - Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Damit wird u.a. verhindert, dass ein unkonfiguriertes Gerät nach dem Einschalten im Netz Adressen vergibt, die nicht im lokalen Netz liegen.

- Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein.

Ob der DHCP-Server letztendlich ein- oder ausgeschaltet ist, kann den DHCP-Statistiken entnommen werden.

Die Default-Einstellung für den Zustand ist 'Auto'.

4.1.3 So werden die Adressen zugewiesen

Zuweisung von IP-Adressen

Damit der DHCP-Server den Rechnern im Netz IP-Adressen zuweisen kann, muss er zunächst einmal wissen, welche Adressen er für diese Zuweisung verwenden darf. Für die Auswahl der möglichen Adressen gibt es drei verschiedene Optionen:

- Die IP-Adresse kann aus dem eingestellten Adress-Pool genommen werden (Start-Adress-Pool bis End-Adress-Pool). Hier können beliebige im lokalen Netz gültige Adressen eingegeben werden.
- Wird stattdessen '0.0.0.0' eingegeben, so ermittelt der DHCP-Server selbstständig die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen für die DMZ-Adresse oder Intranet-Adresse im 'TCP/IP-Modul'. Dabei wird wie folgt vorgegangen:
  - Ist nur die Intranet-Adresse oder nur die DMZ-Adresse eingegeben, so wird über die zugehörige Netzmaske der Start bzw. das Ende des Pools bestimmt.
  - Sind beide angegeben, so hat die Intranet-Adresse den Vorrang bei der Bestimmung des Pools.

  Aus der verwendeten Adresse (Intranet- oder DMZ-Adresse) und der zugehörigen Netzmaske ermittelt der DHCP-Server die erste und die letzte mögliche IP-Adresse im lokalen Netz als Start- bzw. End-Adresse des Adress-Pools.
- Wenn der Router weder eine eigene Intranet- noch eine DMZ-Adresse hat, befindet sich das Gerät in einem besonderen Betriebszustand. Es verwendet dann selbst die IP-Adresse '172.23.56.254' und den Adress-Pool '172.23.56.x' für die Zuweisung der IP-Adressen im Netz.

Wenn nun ein Rechner im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Gerät mit aktiviertem DHCP-Modul die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine gültige Adresse aus dem Pool genommen.

DE

Wurde dem Rechner in der Vergangenheit schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die ausgesuchte Adresse im lokalen Netz noch frei ist. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

Zuweisung der Netzmaske

Die Zuweisung der Netzmaske erfolgt analog zur Adresszuweisung. Wenn im DHCP-Modul eine Netzmaske eingetragen ist, wird diese bei der Zuweisung verwendet. Ansonsten wird die Netzmaske aus dem TCP/IP-Modul verwendet. Die Reihenfolge ist dabei die gleiche wie bei der Adresszuweisung.

Zuweisung der Broadcast-Adresse

In der Regel wird im lokalen Netz für Broadcast-Pakete eine Adresse verwendet, die sich aus den gültigen IP-Adressen und der Netzmaske ergibt. Nur in Sonderfällen (z.B. bei Verwendung von Sub-Netzen für einen Teil der Arbeitsplatzrechner) kann es nötig sein, eine andere Broadcast-Adresse zu verwenden. In diesem Fall wird die zu verwendende Broadcast-Adresse im DHCP-Modul eingetragen.

Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen. Eine Fehlkonfiguration in diesem Bereich kann zu unerwünschten, kostenpflichtigen Verbindungsaufbauvorgängen führen!

Zuweisung des Standard-Gateways

Das Gerät weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse als Gateway-Adresse zu.

Falls erforderlich, kann diese Zuweisung durch die Einstellungen am Arbeitsplatzrechner überschrieben werden.

Zuweisung von DNS- und NBNS-Server

Hierzu werden die zugehörigen Einträge aus dem 'TCP/IP-Modul' herangezogen.

Ist bei den entsprechenden Feldern kein Server angegeben, so gibt der Router seine eigene IP-Adresse als DNS-Adresse weiter. Diese wird bestimmt, wie

unter 'Zuweisung einer IP-Adresse' beschrieben. Der Router verwendet dann DNS-Forwarding (siehe auch 'DNS-Forwarding'), um DNS- oder NBNS-Anfragen des Hosts aufzulösen.

Gültigkeitsdauer einer Zuweisung

Die dem Rechner einmal zugewiesenen Adressen haben nur eine begrenzte Gültigkeit. Nach Ablauf dieser Gültigkeitsdauer darf der Rechner sie nicht mehr verwenden. Damit der Rechner die Adressen (vor allem seine IP-Adresse) danach nicht immer wieder verliert, beantragt er rechtzeitig eine Verlängerung, die ihm in der Regel auch immer gewährt wird. Nur wenn die Gültigkeitsdauer abläuft, während der Rechner abgeschaltet ist, verliert er die Adresse.

Bei jeder Anfrage kann ein Host eine bestimmte Gültigkeitsdauer fordern. Ein DHCP-Server kann dem Host aber auch eine davon abweichende Gültigkeitsdauer zuweisen. Das DHCP-Modul bietet zwei Einstellungen, um die Gültigkeitsdauer zu beeinflussen:

- Maximale Gültigkeit in Minuten

  Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist.

  Fordert ein Host eine Gültigkeit an, die die maximale Dauer überschreitet, so wird ihm nur diese maximale Gültigkeit zugewiesen!

  Die Voreinstellung von 6000 Minuten entspricht ca. 4 Tagen.

- Default-Gültigkeit in Minuten

  Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert. Die Voreinstellung von 500 Minuten entspricht ca. 8 Stunden.

Vorfahrt für den DHCP-Server – Zuweisung anfordern

Standardmäßig sind fast alle Einstellungen in der Netzwerkumgebung von Windows so eingestellt, dass die benötigten Parameter über DHCP angefragt werden. Überprüfen Sie die Einstellungen mit einem Klick auf **Start** / **Einstellungen** / **Systemsteuerung** / **Netzwerk**. Wählen Sie den Eintrag für **TCP/IP** Ihres Netzwerkadapters, und öffnen Sie die **Eigenschaften**.

Auf den verschiedenen Registerkarten können Sie nun nachsehen, ob spezielle Einträge z.B. für die IP-Adresse oder das Standard-Gateway vorhanden sind. Wenn Sie alle Werte vom DHCP-Server zuweisen lassen wollen, löschen Sie nur die entsprechenden Einträge.

DE

Auf der Registerkarte 'WINS-Konfiguration' muss zusätzlich die Option 'DHCP für WINS-Auflösung verwenden' eingeschaltet werden, wenn man Windows-Netze über IP mit Namensauflösung über NBNS-Server verwenden will. Der DHCP-Server muss dann außerdem einen NBNS-Eintrag haben.

Vorfahrt für den Rechner – Zuweisung überschreiben

Sollte ein Rechner andere Parameter verwenden als die ihm zugewiesenen (z.B. ein anderes Standard-Gateway), so müssen diese Parameter direkt am Arbeitsplatzrechner eingestellt werden. Der Rechner ignoriert dann die entsprechenden Parameter in der Zuweisung durch den DHCP-Server.

Unter Windows 98 geschieht das z.B. über die Eigenschaften der Netzwerkumgebung.

Klicken Sie auf **Start** / **Einstellungen** / **Systemsteuerung** / **Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter und öffnen die **Eigenschaften**.

Auf den verschiedenen Registerkarten können Sie nun die gewünschten Werte eintragen.

IP-Adressen im LAN überprüfen

Konfigurationstool	Aufruf/Tabelle
WEBconfig	Experten-Konfiguration / Setup / DHCP-Modul / Tabelle-DHCP
Terminal/Telnet	`Setup/DHCP-Modul/Tabelle-DHCP`

Eine Übersicht über die IP-Adressen im LAN gibt die DHCP-Tabelle. Sie zeigt die zugewiesene bzw. verwendete IP-Adresse, die MAC-Adresse, die Gültigkeitsdauer, den Namen des Rechners (falls vorhanden) sowie den Typ der Adresszuweisung.

Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

- 'neu'
  Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
- 'unbek.'
  Bei der Überprüfung der Eindeutigkeit wurde festgestellt, dass die Adresse bereits an einen anderen Rechner vergeben wurde. Der

DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.

- 'stat.'
  Ein Rechner hat dem DHCP-Server mitgeteilt, dass er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr verwendet werden.
- 'dyn.'
  Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

4.2 DNS

Der Domain-Name-Service (DNS) stellt in TCP/IP-Netzen die Verknüpfung zwischen Rechnernamen bzw. Netzwerknamen (Domains) und IP-Adressen her. Dieser Service ist auf jeden Fall erforderlich für die Kommunikation im Internet, um z.B. einer Anfrage nach 'www.lancom.de' die entsprechende IP-Adresse zurückliefern zu können. Aber auch innerhalb eines lokalen Netzes oder bei der LAN-Kopplung ist es sinnvoll, die IP-Adressen im LAN den Namen der Rechner eindeutig zuordnen zu können.

4.2.1 Was macht ein DNS-Server?

Die bei einem DNS-Server nachgefragten Namen bestehen aus mehreren Teilen: Ein Teil besteht aus dem eigentlichen Namen des Hosts oder Dienstes, der angesprochen werden soll, ein anderer Teil kennzeichnet die Domain. Innerhalb eines lokalen Netzes ist die Angabe der Domain optional. Diese Namen können also z.B. 'www.domain.com' oder 'ftp.domain.com' heißen.

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannte Name über die Default-Route gesucht. Durch die Verwendung eines DNS-Servers können alle Namen, die mit ihrer IP-Adresse bekannt sind, direkt bei der richtigen Gegenstelle gesucht werden. Der DNS-Server kann dabei im Prinzip ein separater Rechner im Netz sein. Folgende Gründe sprechen jedoch dafür, den DNS-Server direkt im *LANCOM* anzusiedeln:

- Ein *LANCOM* kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbstständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der dynamischen Adressvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.

- Beim Routing von Windows-Netzen über NetBIOS kennt ein *LANCOM* außerdem die Rechnernamen und IP-Adressen in den anderen angeschlossenen NetBIOS-Netzen. Außerdem melden sich auch die Rechner mit fest eingestellter IP-Adresse ggf. in der NetBIOS-Tabelle an und sind damit mit Namen und Adressen bekannt.
- Der DNS-Server im *LANCOM* kann gleichzeitig als sehr komfortabler Filtermechnismus eingesetzt werden. Anfragen nach bestimmten Domains, die nicht besucht werden dürfen, können durch die einfache Angabe des Domain-Namens für das ganze LAN, nur für Teilnetze (Subnetze) oder sogar für einzelne Rechner gesperrt werden.

Wie reagiert der DNS-Server auf eine Anfrage?

Der DNS-Server bezieht bei Anfragen nach bestimmten Namen alle Informationen in die Suche mit ein, die ihm zur Verfügung stehen:

- Zuerst prüft der DNS-Server, ob der Zugriff auf diesen Namen nicht durch die Filterliste verboten ist. Wenn das der Fall ist, wird der anfragende Rechner mit einer Fehlermeldung darüber informiert, dass er auf diesen Namen nicht zugreifen darf.
- Dann sucht er in der eigenen statischen DNS-Tabelle nach Einträgen für den entsprechenden Namen.
- Steht in der DNS-Tabelle kein Eintrag für diesen Namen, wird die dynamische DHCP-Tabelle durchsucht. Die Verwendung der DHCP-Informationen kann bei Bedarf ausgeschaltet werden.
- Findet der DNS-Server in den vorausgegangenen Tabellen keine Informationen über den Namen, werden die Listen des NetBIOS-Moduls durchsucht. Auch die Verwendung der NetBIOS-Informationen kann bei Bedarf ausgeschaltet werden.
- Schließlich prüft der DNS-Server, ob die Anfrage über ein WAN-Interface an einen anderen DNS-Server weitergeleitet werden soll (Spezielles DNS-Forwarding über die DNS-Destinationstabelle).

Sollte der gesuchte Name in allen verfügbaren Informationen nicht gefunden werden, leitet der DNS-Server die Anfrage über den generellen DNS-Forwarding-Mechanismus an einen anderen DNS-Server (z. B. beim Internet-Provider) weiter oder schickt dem anfragenden Rechner eine Fehlermeldung.

DE

4.2.2 DNS-Forwarding

Wenn eine Anfrage nicht aus den eigenen DNS-Tabellen bedient werden kann, leitet der DNS-Server die Anfrage an andere DNS-Server weiter. Dieser Vorgang heißt DNS-Forwarding (DNS-Weiterleitung).

Dabei unterscheidet man zwischen

- speziellem DNS-Forwarding
  Anfragen nach bestimmten Namensbereichen werden an bestimmte DNS-Server weitergeleitet.
- generellem DNS-Forwarding
  Alle anderen nicht näher spezifizierten Namen werden an den „übergeordneten" DNS-Server weitergeleitet.

Spezielles DNS-Forwarding

Beim speziellen DNS-Forwarding können Namensbereiche definiert werden, für deren Auflösung festgelegte DNS-Server angesprochen werden.

Ein typischer Anwendungsfall für spezielles DNS-Forwarding ergibt sich beim Heimarbeitsplatz: Der Benutzer möchte gleichzeitig sowohl auf das firmeneigene Intranet als auch direkt auf das Internet zugreifen können. Die Anfragen ins Intranet müssen an den DNS-Server der Firma, alle anderen Anfragen an den DNS-Server des Providers geleitet werden.

Generelles DNS-Forwarding

Alle DNS-Anfragen, die nicht auf sonstige Weise aufgelöst werden können, werden an einen DNS-Server weitergeleitet. Dieser DNS-Server bestimmt sich nach folgenden Regeln:

- Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist. Wird er dort fündig, holt er die gewünschte Information von diesem Server. Bis zu zwei übergeordnete DNS-Server können angegeben werden.

LANconfig	TCP/IP / Adressen / Erster DNS-Server / Zweiter DNS-Server
WEBconfig	Experten-Konfiguration / Setup / TCP/IP-Modul / DNS-Default / DNS-Backup
Terminal/Telnet	`/Setup/TCP-IP-Modul/DNS-Default` `/Setup/TCP-IP-Modul/DNS-Backup`

DE

- Gibt es keinen eingetragenen DNS-Server im Router, versucht er auf einer evtl. bestehenden PPP-Verbindung (z.B. zum Internet-Provider) einen DNS-Server zu erreichen, und holt die Zuordnung der IP-Adresse zum Namen von dort. Das gelingt natürlich nur dann, wenn während der PPP-Verhandlung die Adresse eines DNS-Servers an den Router übermittelt worden ist.
- Besteht keine Verbindung, wird die Default-Route aufgebaut und dort nach dem DNS-Server gesucht.

Durch dieses Verfahren benötigen Sie keine Kenntnisse über die Adressen eines DNS-Servers. Der Eintrag der Intranet-Adresse Ihres Routers als DNS-Server bei den Arbeitsplatzrechnern reicht aus, um die Namenszuordnung zu ermöglichen. Außerdem wird damit die Adresse des DNS-Servers automatisch aktualisiert. Sollte z.B. der Provider, der diese Adresse mitteilt, seinen DNS-Server umbenennen, oder sollten Sie zu einem anderen Provider wechseln, erhält Ihr lokales Netz stets die aktuellen Informationen.

4.2.3 So stellen Sie den DNS-Server ein

Die Einstellungen für den DNS-Server finden Sie im folgenden Menü bzw. in folgender Liste:

Konfigurationstool	Aufruf/Tabelle
LANconfig	TCP/IP / DNS-Server
WEBconfig	Experten-Konfiguration / Setup / DNS-Modul
Terminal/Telnet	`cd /Setup/DNS-Modul`

Gehen Sie zur Einstellung des DNS-Servers wie folgt vor:

a Schalten Sie den DNS-Server ein.

WEBconfig	… / Zustand
Terminal/Telnet	`set Zustand ein`

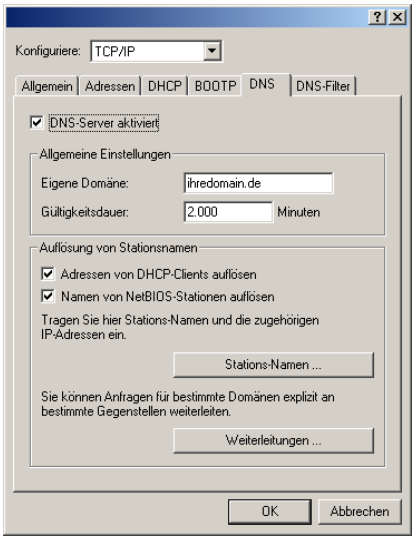
b Geben Sie die Domain ein, in der sich der DNS-Server befindet. Mit Hilfe dieser Domain erkennt der DNS-Server bei Anfrage, ob sich der gesuchte Name im eigenen LAN befindet oder nicht. Die Angabe der Domain ist optional.

DE

WEBconfig	… / Domain
Terminal/Telnet	`set Domain ihredomain.com`

c Geben Sie an, ob die Informationen aus dem DHCP-Server und dem NetBIOS-Modul verwendet werden sollen.

WEBconfig	… / DHCP-verwenden … / NetBIOS-verw.
Terminal/Telnet	`set DHCP-verwenden ja` `set NetBIOS-verw. ja`



Aktivierter DNS-Server in der TCP-IP-Konfiguration

d Der DNS-Server dient hauptsächlich dazu, Anfragen nach Namen im Internet von den Anfragen nach Namen bei anderen Gegenstellen zu trennen. Tragen Sie daher alle Rechner in die Stations-Namen-Tabelle ein,

- deren Name und IP-Adresse Sie kennen,
- die nicht im eigenen LAN liegen,
- die nicht im Internet liegen und
- die über den Router erreichbar sind.

DE

Mit folgenden Befehlen fügen Sie Stationen zur Stations-Namen-Tabelle hinzu:

LANconfig	TCP/IP / DNS / Stations-Namen / Hinzufügen
WEBconfig	… / DNS-Tabelle / Hinzufügen
Terminal/Telnet	`cd Setup/DNS-Modul/DNS-Tabelle` `set mail.ihredomain.de 10.0.0.99`

Wenn Sie z. B. in einem externen Büro arbeiten und über den Router den Mailserver in der Zentrale (Name: mail.ihredomain.de, IP: 10.0.0.99) erreichen wollen, tragen Sie ein:

Die Angabe der Domain ist dabei optional, aber zu empfehlen.

Wenn Sie nun das Mailprogramm starten, wird es vermutlich automatisch den Server 'mail.ihredomain.de' suchen. Der DNS-Server gibt daraufhin die IP-Adresse '10.0.0.99' zurück. Das Mailprogramm sucht dann nach dieser IP-Adresse. Mit entsprechenden Einträgen in IP-Routing-Tabelle und Namenliste etc. wird dann automatisch die Verbindung zum Netz in der Zentrale hergestellt, wo der Mailserver schließlich gefunden wird.

e Um ganze Namensbereiche von einem anderen DNS-Server auflösen zu lassen, fügen Sie einen Weiterleitungseintrag bestehend aus Namensbereich und Gegenstelle hinzu:

LANconfig	TCP/IP / DNS / Weiterleitungen / Hinzufügen
WEBconfig	… / DNS-Destinationstabelle / Hinzufügen
Terminal/Telnet	`cd Setup/DNS-Modul/Destinationstabelle` `set *.intern FIRMA`

Bei der Angabe der Namensbereiche dürfen die Wildcards '?' für einzelne Zeichen und '*' für mehrere Zeichen verwendet werden.

Um alle Domains mit der Endung '.intern' auf einen DNS-Server im LAN der Gegenstelle 'FIRMA' umzuleiten, erstellen Sie folgenden Eintrag:

Der DNS-Server kann entweder über den Name der Gegenstelle (für automatische Konfiguration über PPP) oder die explizite IP-Adresse des zuständigen Nameservers angegeben werden

4.2.4 URL-Blocking

f Mit der Filterliste können Sie schließlich den Zugriff auf bestimmte Namen oder Domains sperren.

Um die Domain (in diesem Fall den Web-Server) 'www.gesperrt.de' für alle Rechner im LAN zu sperren, sind die folgenden Befehle und Eingaben notwendig:

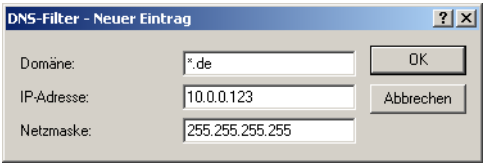
LANconfig	TCP/IP / DNS-Filter / DNS-Filter / Hinzufügen
WEBconfig	... / Filter-Liste / Hinzufügen
Terminal/Telnet	`cd Setup/DNS-Modul/Filter-Liste` `set 001 www.gesperrt.de 0.0.0.0 0.0.0.0`

Der Index '001' im Konsolenbefehl ist frei gewählt und dient lediglich der Übersichtlichkeit.

Bei der Eingabe der Domäne sind auch die Wildcards '?' (steht für genau ein Zeichen) und '' (für beliebig viele Zeichen) erlaubt.*

Um nur einem bestimmten Rechner (z. B. mit IP 10.0.0.123) den Zugriff auf DE-Domains zu sperren, tragen Sie folgende Werte ein:

DE



Im Konsolenmodus lautet der Befehl:

```
set 002 *.de 10.0.0.123 255.255.255.255
```

Die Hitliste in der DNS-Statistik zeigt Ihnen die 64 Namen, die am häufigsten nachgefragt werden, und bietet Ihnen damit eine gute Basis für die Einstellung der Filter-Liste.

Durch die geeignete Wahl von IP-Adressen und Netzmasken können bei der Verwendung von Subnetting in Ihrem LAN auch einzelne Abteilungen gefiltert werden. Dabei steht die IP-Adresse '0.0.0.0' jeweils für alle Rechner in einem Netz, die Netzmaske '0.0.0.0' für alle Netze.

4.2.5 Dynamic DNS

Damit auch Systeme mit dynamischen IP-Adressen über das WAN - also beispielsweise über das Internet - erreichbar sind, existieren eine Reihe von sog. Dynamic DNS-Server Anbietern (z.B. www.dynDNS.org).

Damit wird ein *LANCOM* immer unter einem bestimmten Namen (FQDN - 'fully qualified domain name') erreichbar (z.B. "http://MyLANCOM.dynDNS.org").

Der Vorteil liegt auf der Hand: Wenn Sie z.B. eine Fernwartung an einem Anschluss ohne ISDN durchführen wollen (z.B über WEBconfig / HTTPS), oder über den *LANCOM* VPN-Client auf eine Außenstelle mit dynamischer IP-Adresse zugreifen wollen, dann brauchen Sie lediglich den Dynamic DNS-Namen zu kennen.

Wie gelangt die aktuelle IP-Adresse zum Dynamic DNS Server?

Dynamic DNS Anbieter unterstützten eine Reihe von Clientprogrammen, die über verschiedene Methoden die aktuell zugewiesene IP-Adresse eines *LANCOM* ermitteln können, und im Falle einer Änderung an den jeweiligen Dynamic DNS Server übertragen.

Die aktuelle WAN-seitige IP-Adresse eines *LANCOM* kann unter folgender Adresse ausgelesen werden:

```
http://<Adresse des LANCOM>/config/1/6/8/3/
```

DE

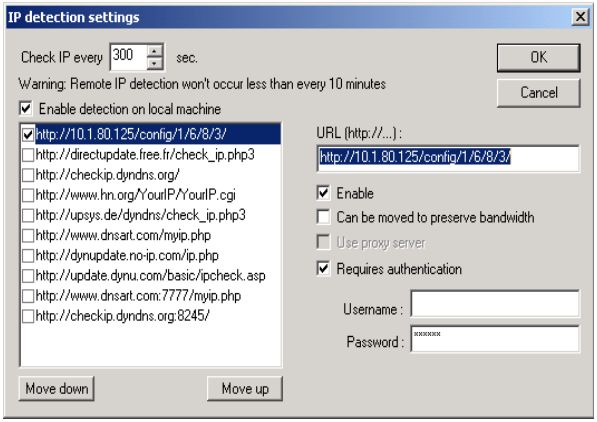


Abbildung: Auslesen der aktuellen IP-Adresse aus einem LANCOM

4.3 Gebührenmanagement

Die Eigenschaft des Routers, Verbindungen selbstständig zu allen gewünschten Gegenstellen aufzubauen und sie mit dem Ende der Übertragung automatisch wieder zu beenden, ermöglicht dem Benutzer sehr komfortablen Zugriff z.B. auf das Internet. Bei der Datenübertragung über kostenpflichtige Leitungen können jedoch durch Fehlkonfiguration des Routers (z.B. bei der Filterkonfiguration) oder durch übermäßigen Gebrauch des Angebots (z.B. andauerndes Surfen im Internet) recht hohe Kosten entstehen.

Um diese Kosten zu begrenzen, bietet die Software verschiedene Möglichkeiten:

- Die verfügbaren Online-Minuten können für eine bestimmte Periode eingeschränkt werden.
- Für ISDN-Verbindungen kann für eine bestimmte Periode ein Gebührenlimit oder ein Zeitlimit festgelegt werden.

4.3.1 Gebührenabhängige ISDN-Verbindungsbegrenzung

Werden an einem ISDN-Anschluss Gebühreninformationen übermittelt, können die anfallenden Verbindungsgebühren recht einfach eingeschränkt werden. Im Default-Zustand dürfen z.B. maximal 830 Gebühreneinheiten in

DE

sechs Tagen verbraucht werden. Ist diese Grenze erreicht, erlaubt der Router keinen weiteren aktiven Verbindungsaufbau.

*Die Gebührenüberwachung des Routers können Sie am besten bei freigeschalteter „Gebühreninformation **während** der Verbindung" im ISDN-Netz (nach AOCD) nutzen. Beantragen Sie ggf. die Freischaltung dieses Merkmals bei Ihrer Telefongesellschaft. Eine Gebührenüberwachung mit dem Merkmal „Gebühreninformation **nach** der Verbindung" ist im Prinzip auch möglich, jedoch werden dabei ggf. Dauerverbindungen nicht erkannt!*

Wenn Sie das Least-Cost-Routing für die Router-Module eingeschaltet haben, werden ggf. auch Verbindungen über Provider aufgebaut, die keine Gebühreninformationen übertragen!

4.3.2 Zeitabhängige ISDN-Verbindungsbegrenzung

Der Mechanismus der ISDN-Gebührenüberwachung greift nicht, wenn am ISDN-Anschluss keine Gebühreninformationen übertragen werden. Das ist z.B. dann der Fall, wenn die Übermittlung der Gebühreninformationen entweder nicht beantragt wurde oder die Telefongesellschaft diese Informationen grundsätzlich nicht übermittelt.

Um die Kosten für ISDN-Verbindungen auch ohne Gebühreninformationen begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeitbudget für eine Periode vereinbart. Im Default-Zustand dürfen z.B. für maximal 210 Minuten innerhalb von sechs Tagen Verbindungen aktiv aufgebaut werden.

Wird die Grenze eines Budgets erreicht, werden automatisch alle offenen Router-Verbindungen beendet, die der Router selbst aufgebaut hat. Erst nach dem Ablauf der aktuellen Periode werden die Budgets wieder freigegeben und aktive Verbindungen ermöglicht. Der Administrator kann die Budgets natürlich auch vorzeitig wieder freigeben!

Mit einem Budget von 0 Einheiten bzw. 0 Minuten kann die Gebühren- bzw. Zeitüberwachung der Routerfunktionen ausgeschaltet werden.

Nur die Router-Funktionen sind durch den Gebühren- oder Zeitschutz abgesichert! Verbindungen über LANCAPI werden davon nicht erfasst.

DE

4.3.3 Einstellungen im Gebührenmodul

Konfigurationstool	Aufruf/Tabelle
LANconfig	Management / Kosten
WEBconfig	Experten-Konfiguration / Setup / Gebuehren-Modul
Terminal/Telnet	`cd /Setup/Gebuehren-Modul`

Im Gebührenmodul können Sie die Onlinezeit überwachen und für den Aufbauschutz nutzen.

- Tage/Periode
  Dauer einer Überwachungsperiode in Tagen angegeben
- Budget-Einheiten, Online-Minuten-Budget
  Maximale ISDN-Einheiten bzw. Online-Minuten in einer Überwachungsperiode

Die Informationen über die Gebühren und Verbindungszeiten werden über einen Bootvorgang hinaus gesichert (z.B. beim Einspielen einer neuen Firmware) und gehen erst verloren, wenn das Gerät ausgeschaltet wird. Alle hier erwähnten Zeitangaben werden in Minuten gemacht.

4.4 Das SYSLOG-Modul

Mit dem SYSLOG-Modul besteht die Möglichkeit, Zugriffe auf den *LANCOM* protokollieren zu lassen. Diese Funktion ist insbesondere für Systemadministratoren interessant, da sie die Möglichkeit bietet, eine lückenlose Historie aller Aktivitäten aufzeichnen zu lassen.

Um die SYSLOG-Nachrichten empfangen zu können, benötigen Sie einen entsprechenden SYSLOG-Client bzw. -Dämon. Unter UNIX/Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Dämon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei.

Unter Linux wird in der Datei `/etc/syslog.conf` angegeben, welche Facilities (zu diesem Begriff später mehr) in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Dämons, ob auf Netzwerkverbindungen explizit gehört wird.

Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Dämons erfüllt.

DE

4.4.1 Einrichten des SYSLOG-Moduls

Konfigurationstool	Aufruf/Tabelle
LANconfig	Management / Meldungen
WEBconfig	Experten-Konfiguration / Setup / SYSLOG-Modul
Terminal/Telnet	`cd /Setup/SYSLOG-Modul`

4.4.2 Beispielkonfiguration mit *LANconfig*

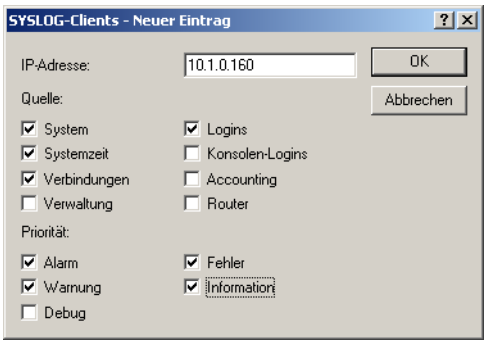
SYSLOG-Client anlegen

a Starten Sie *LANconfig*. Unter 'Management' wählen Sie die Karte 'Meldungen'.

b Schalten Sie das Modul ein, und klicken Sie auf **SYSLOG-Clients**.

c Im nächsten Fenster klicken Sie auf **Hinzufügen...**.

d Geben Sie zunächst die IP-Adresse des SYSLOG-Clients ein, und legen Sie im Weiteren die Quellen und Prioritäten fest.



SYSLOG kommt aus der UNIX-Welt, in der bestimmte Quellen vordefiniert sind. *LANCOM* ordnet seine eigenen internen Quellen diesen vordefinierten SYSLOG-Quellen, den sogenannten „Facilities“, zu.

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller Nachrichtenquellen, die Sie im *LANCOM* einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die Zuordnung zwischen den internen Quellen des *LANCOM* und den SYSLOG-Facilities an.

DE

Quelle	Bedeutung	Facility
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL
Logins	Meldungen über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über den Verbindungsauf- und -abbau sowie dabei auftretende Fehler (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

Die im SYSLOG ursprünglich definierten acht Prioritätsstufen sind im *LANCOM* auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen Alarmlevel, Bedeutung und SYSLOG-Prioritäten.

Priorität	Bedeutung	SYSLOG-Priorität
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z.B. Verbindungsfehler).	ERROR
Warning	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z.B. Accounting-Informationen).	NOTICE, INFORM

DE

Priorität	Bedeutung	SYSLOG-Priorität
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie sollten daher im Regelbetrieb ausgeschaltet sein und nur zur Fehlersuche verwendet werden.	DEBUG

e Wenn Sie alle Parameter definiert haben, bestätigen Sie die Eingaben mit **OK**. In der SYSLOG-Tabelle wird der SYSLOG-Client mit seinen Parametern eingetragen.

Facilities

Über die Schaltfläche **Facility-Zuordnung** können alle Meldungen vom *LANCOM* einer Facility zugeordnet und dadurch vom SYSLOG-Client ohne zusätzlichen Aufwand in eine spezielle Log-Datei geschrieben werden.

Beispiel

Alle Facilities werden auf 'local7' gesetzt. Unter Linux werden nun in der Datei `/etc/syslog.conf` durch den Eintrag

```
local7.* /var/log/lancom.log
```

alle Ausgaben des *LANCOM* in die Datei `/var/log/lancom.log` geschrieben.

4.5 Bürokommunikation mit *LANCAPI*

Die *LANCAPI* von LANCOM ist eine spezielle Form der weit verbreiteten CAPI-Schnittstelle. CAPI steht für Common ISDN Application Programming Interface und stellt die Verbindung von ISDN-Adaptern zu Kommunikationsprogrammen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation, wie z.B. ein Fax oder einen Anrufbeantworter, bereit.

Dieser Abschnitt stellt Ihnen die *LANCAPI* und ihre Anwendung für Aufgaben der Bürokommunikation kurz vor.

4.5.1 Welche Vorteile bietet die *LANCAPI*?

Der Einsatz der *LANCAPI* bringt vor allem wirtschaftliche Vorteile. Alle Windows-Arbeitsplätze, die im LAN integriert sind, erhalten über die *LANCAPI* uneingeschränkten Zugriff auf Bürokommunikations-Funktionen wie Fax, Anrufbeantworter, Onlinebanking und Eurofiletransfer. Ohne zusätzliche Hardware an jedem einzelnen Arbeitsplatz werden alle

Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsplätzen installiert.

Beim Versenden von Faxen wird z.B. am Arbeitsplatz ein Faxgerät simuliert. Mit der *LANCAPI* leitet der PC das Fax über das Netzwerk an einen Router weiter, welcher die Verbindung zum Empfänger herstellt.

Alle Anwendungen, die Sie über die LANCAPI betreiben, verwenden direkte ISDN-Verbindungen und laufen nicht über die Router-Funktion des Geräts. Daher funktionieren die Firewall- und Gebührenüberwachungsfunktionen nicht.

Das Client-Server-Prinzip

Die *LANCAPI* besteht aus zwei Komponenten, einem Server (im *LANCOM*) und einem Client (auf den PCs). Der *LANCAPI*-Client wird nur auf den Rechnern im lokalen Netz installiert, die die Funktionen der *LANCAPI* nutzen möchten.

4.5.2 Konfiguration des *LANCAPI*-Servers

Bei der Konfiguration des *LANCAPI*-Servers werden im Prinzip zwei Fragen behandelt:

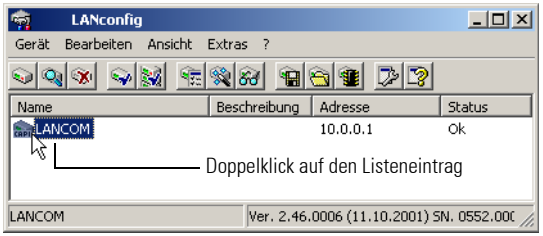
- Auf welche Rufnummer aus dem Telefonnetz soll die *LANCAPI* reagieren?
- Welche der Rechner im lokalen Netz sollen über die *LANCAPI* Zugang zum Telefonnetz erhalten?

Die Konfiguration am Router erfolgt über die Konfigurationstabellen von *LANconfig* oder *WEBconfig*. In den folgenden beiden Abschnitten finden Sie Schritt-für-Schritt-Anleitung für jedes dieser Konfigurationsprogramme.

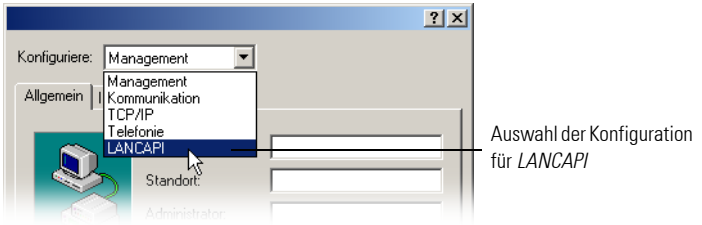
4.5.3 Anleitung für *LANconfig*

a Öffnen Sie die Konfiguration des Routers durch einen Doppelklick auf den Gerätenamen in der Liste und geben Sie auf Nachfrage Ihr Kennwort ein.

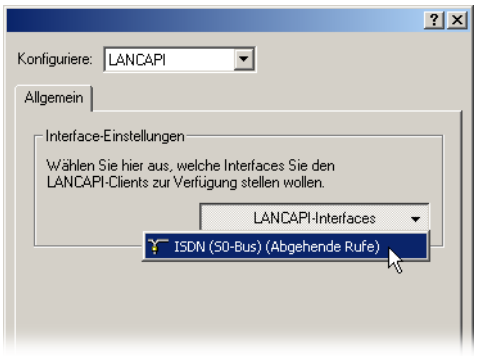
DE



b Wählen Sie den Konfigurationsbereich **LANCAPI**.

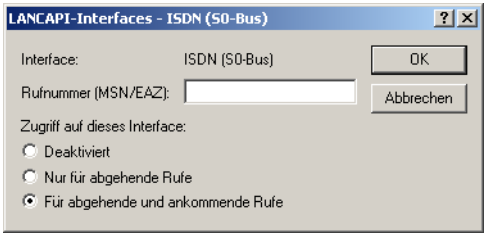


c Wählen Sie die ISDN-Schnittstelle aus.



d Aktivieren Sie den *LANCAPI*-Server für abgehende und ankommende Rufe, oder lassen Sie nur abgehende Anrufe zu.

DE



Wenn der *LANCAPI*-Server auch ankommende Rufe entgegen nehmen soll, so geben Sie im Feld 'Rufnummern (MSN/EAZ)' alle eigenen ISDN-Rufnummern an, auf denen die *LANCAPI* Anrufe entgegennehmen soll. Mehrere Rufnummern werden voneinander durch Semikola getrennt. Wenn Sie hier keine Rufnummer eingeben, nimmt die *LANCAPI* Anrufe an allen eigenen ISDN-Rufnummern entgegen.

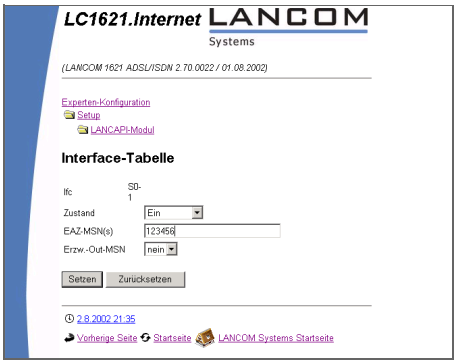
4.5.4 Anleitung für *WEBconfig*

a Wählen Sie im Hauptmenü die **Experten-Konfiguration**.

b Wählen Sie in den folgenden Menüs **Setup / LANCAPI-Modul** / **Interface-Tabelle**.

c Wählen Sie in der **Interface-Tabelle** den (einzigen) Eintrag **S0-1**.

d Aktivieren Sie den *LANCAPI*-Server für abgehende und ankommende Rufe ('Ein'), oder lassen Sie nur abgehende Anrufe zu ('Abgehend').



Wenn der *LANCAPI*-Server auch ankommende Rufe entgegen nehmen soll, so geben Sie im Feld 'EAZ/MSNs' alle eigenen ISDN-Rufnummern an, auf denen die *LANCAPI* Anrufe entgegennehmen soll. Mehrere

DE

Rufnummern werden voneinander durch Semikola getrennt. Wenn Sie hier keine Rufnummer eingeben, nimmt die *LANCAPI* Anrufe an allen eigenen ISDN-Rufnummern entgegen. Bestätigen Sie Ihre Angaben mit **Setzen**.

4.5.5 Installation des *LANCAPI*-Clients

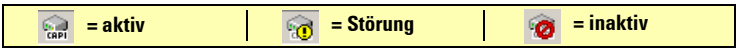
Für die Installation des LANCAPI-Clients auf einem System unter Windows XP oder Windows 2000 benötigen Sie Administrator-Rechte.

a Legen Sie an einem Client-PC die *LANCOM*-CD in Ihr CD-ROM-Laufwerk ein. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' im Hauptverzeichnis der *LANCOM*-CD.

b Wählen Sie den Eintrag **LANCOM Software installieren**.

c Markieren Sie die Option ***LANCAPI***. Klicken Sie auf **Weiter**, und folgen Sie den Hinweisen der Installationsroutine. Zum Abschluss wird (sofern erforderlich) ein Neustart des Rechners durchgeführt.

Der *LANCAPI*-Client startet von nun an automatisch. Seinen Status zeigt das zusätzliche Icon in der Windows-Taskleiste (neben der Uhr) an.



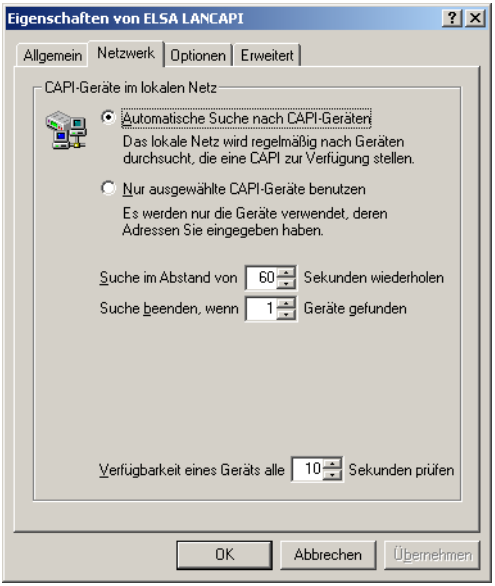
4.5.6 Konfiguration des *LANCAPI*-Clients

Bei der Einstellung der Clients für die *LANCAPI* legen Sie fest, welche *LANCAPI*-Server verwendet werden sollen und wie diese überprüft werden. Wenn Sie nur einen *LANCOM* in Ihrem LAN als *LANCAPI*-Server betreiben, können Sie im Prinzip alle Parameter in den Voreinstellungen belassen.

a Starten Sie den *LANCAPI*-Client aus der Programmgruppe 'LANCOM'. Auf der Registerkarte 'Allgemein' finden Sie Informationen zum Treiber zum bereitgestellten Dienst.

b Wechseln Sie im *LANCAPI*-Client auf das Register **Netzwerk**. Hier können Sie zunächst wählen, ob der PC seinen *LANCAPI*-Server selbst suchen soll oder ob ein bestimmter Server verwendet werden soll.

- Im ersten Fall legen Sie fest, in welchem zeitlichen Intervall der Client nach einem Server sucht. Dabei sucht er so lange, bis er die im nächsten Feld eingestellte Anzahl an Servern gefunden hat. Hat er die geforderte Zahl an Servern gefunden, hört er mit der Suche auf.
- Wenn der Client nicht automatisch nach Servern suchen soll, geben Sie in der Liste die IP-Adressen der Server an, die der Client verwenden soll. Diese Festlegung ist z.B. dann sinnvoll, wenn Sie mehrere *LANCOM* in Ihrem LAN als *LANCAPI*-Server betreiben und eine Gruppe von PCs einen bestimmten Server verwenden sollen.
- Für beide Optionen können Sie auch einstellen, in welchem Intervall der Client prüft, ob die gefundenen oder per Liste definierten Server noch aktiv sind.



4.5.7 So setzen Sie die *LANCAPI* ein

Zur Verwendung der *LANCAPI* gibt es zwei Möglichkeiten:

- Sie setzen eine Software ein, die direkt auf einer CAPI-Schnittstelle (in diesem Fall der *LANCAPI*) aufsetzt. Eine solche Software sucht bei der Installation nach der CAPI und verwendet diese anschließend automatisch.

DE

- Andere Programme, wie LapLink, können Verbindungen über verschiedene Wege aufbauen, z.B. über das DFÜ-Netzwerk von Windows. Beim Anlegen einer neuen DFÜ-Verbindung können Sie auswählen, welches der installierten Kommunikationsgeräte Sie verwenden möchten. Wählen Sie für die *LANCAPI* den Eintrag 'ISDN WAN Line 1'.

4.5.8 Das *LANCOM CAPI Faxmodem*

Mit dem *LANCOM CAPI Faxmodem* steht Ihnen unter Windows ein Faxtreiber (Fax Class 1) zur Verfügung, der als Schnittstelle zwischen *LANCAPI* und Anwendung den Betrieb von Standard-Faxprogrammen mit einem *LANCOM* ermöglicht.

Installation

Das *LANCOM CAPI Faxmodem* wird über das CD-Setup installiert. Installieren Sie das *LANCOM CAPI Faxmodem* immer zusammen mit der aktuellen *LANCAPI*. Nach dem Neustart steht Ihnen im System das *LANCOM CAPI Faxmodem* zur Verfügung, z.B. unter Windows 98 unter **Start** / **Einstellungen** / **Systemsteuerung** / **Modems**.

Faxen über *CAPI Faxmodem*

Das *CAPI Faxmodem* wird von den gängigen Faxprogrammen bei der Installation automatisch erkannt und als 'Class 1'-Faxmodem identifiziert. Damit sind Faxübertragungen mit bis zu 14.400 bit/s möglich. Falls Ihr Faxprogramm eine Unterscheidung erlaubt (z.B. WinFax bzw. Talkworks Pro), wählen Sie bei der Einrichtung des Modems die Option 'CLASS 1 (Software Flow Control)' aus

Faxen unter Windows 2000 und XP

Windows XP oder Windows 2000 bieten im Zusammenspiel mit dem *CAPI Faxmodem* volle Faxfunktionalität. Ein zusätzliches Faxprogramm ist nicht erforderlich.

Dazu starten Sie in der Systemsteuerung "Windows Komponenten hinzufügen / entfernen" und wählen die "Faxdienste" aus.

Nach der Installation befindet sich das Fax unter "Drucker und Faxgeräte", und kann von jedem Windows-Programm anstelle eines Drucker ausgwählt werden.

DE

Das CAPI Faxmodem ist nur dann für die Übertragung von Faxnachrichten bereit, wenn die LANCAPI aktiv ist.

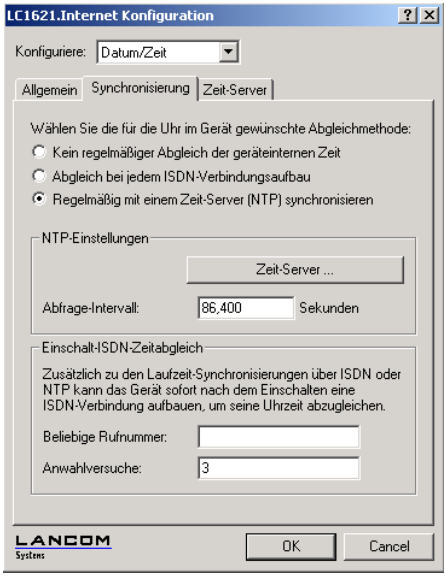
4.6 Zeit-Server für das lokale Netz

LANCOM Router können hochgenaue Zeitinformationen entweder über ISDN beziehen, oder aber über öffentlich zugängliche Zeit-Server im Internet (NTP-Server mit 'Open Acccess'-Policy, z.B. von der Physikalisch-Technischen Bundesanstalt).Die so ermittelte Zeit kann das *LANCOM* allen Stationen im lokalen Netz zur Verfügung stellen.

Nicht alle Betriebssysteme verfügen über einen integrierten NTP-Client: Windows XP verfügt über einen solchen, für andere Windows-Betriebssysteme ist ein separater NTP-Client notwendig, bei Linux-Distributionen muss NTP entsprechend mitinstalliert sein. Die NTP-Clients müssen so konfiguriert sein, dass sie die Zeitinformationen vom LANCOM verwenden..

Konfigurationstool	Aufruf/Tabelle
LANconfig	Management / Datum / Zeit
WEBconfig	Experten-Konfiguration / Setup / NTP-Modul
Terminal/Telnet	`cd /Setup/NTP-Modul`

DE


LC1621.Internet Konfiguration
Konfiguriere:
Datum/Zeit
Allgemein
Synchronisierung
Zeit-Server
Wählen Sie die für die Uhr im Gerät gewünschte Abgleichmethode:
Kein regelmäßiger Abgleich der geräteinternen Zeit
Abgleich bei jedem ISDN-Verbindungsaufbau
Regelmäßig mit einem Zeit-Server (NTP) synchronisieren
NTP-Einstellungen
Zeit-Server ...
Abfrage-Intervall:
86,400
Sekunden
Einschalt-ISDN-Zeitabgleich
Zusätzlich zu den Laufzeit-Synchronisierungen über ISDN oder NTP kann das Gerät sofort nach dem Einschalten eine ISDN-Verbindung aufbauen, um seine Uhrzeit abzugleichen.
Beliebige Rufnummer:
Anwahlversuche:
3
LANCOM Systems
OK
Cancel

DE

5 Routing und WAN-Verbindungen

Dieses Kapitel beschreibt die wichtigsten Protokolle und Konfigurationseinträge, die bei WAN-Verbindungen eine Rolle spielen. Es zeigt auch Wege auf, WAN-Verbindungen zu optimieren.

5.1 Allgemeines über WAN-Verbindungen

WAN-Verbindungen werden für folgende Anwendungen verwendet.

- Internet-Zugang
- LAN-LAN-Kopplung
- Remote Access

5.1.1 Brücken für Standard-Protokolle

WAN-Verbindungen unterscheiden sich von direkten Verbindungen (beispielsweise über die *LANCAPI*) dadurch, dass die Daten im WAN über standardisierte Netzwerk-Protokolle übertragen werden, die auch im LAN Anwendung finden. Direkte Verbindungen arbeiten hingegen mit proprietären Verfahren, die speziell für Punkt-zu-Punkt-Verbindungen entwickelt worden sind.

Über WAN-Verbindungen wird ein LAN erweitert, bei direkten Verbindungen erhält nur ein einzelner PC eine Verbindung zu einem anderen PC. WAN-Verbindungen bilden gewissermaßen Brücken für die Kommunikation zwischen Netzwerken (bzw. für die Anbindung einzelner Rechner an ein LAN).

Die enge Zusammenarbeit mit den Router-Modulen

Charakteristisch für WAN-Verbindungen ist die enge Zusammenarbeit mit den Router-Modulen im *LANCOM*. Die Router-Module (IP und IPX) sorgen für die Verbindung von LAN und WAN. Sie bedienen sich der WAN-Module, um Anfragen von PCs aus dem LAN nach externen Ressourcen zu erfüllen.

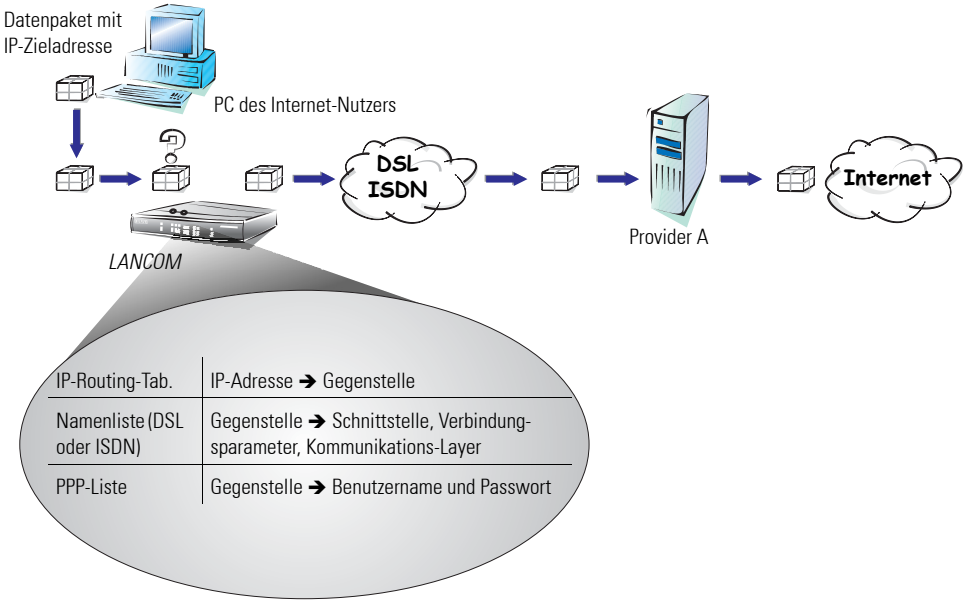
5.1.2 Was passiert bei einer Anfrage aus dem LAN?

Die Routermodule ermitteln zunächst nur, zu welcher Gegenstelle ein Datenpaket übertragen werden soll. Damit die entsprechende Verbindung ausgewählt und ggf. aufgebaut werden kann, müssen verschiedene Parameter für alle notwendingen Verbindungen vereinbart werden. Diese

DE

Parameter sind in unterschiedlichen Listen abgelegt, deren Zusammenspiel die richtigen Verbindungen erlaubt.

Wir wollen diesen Ablauf an einem vereinfachten Beispiel verdeutlichen. Dabei gehen wir davon aus, dass die IP-Adresse des gesuchten Rechners im Internet bekannt ist.



a **Auswahl der richtigen Route**
Ein Datenpaket aus einem Rechner findet den Weg ins Internet in erster Linie über die IP-Adresse des Empfängers. Mit dieser Adresse schickt der Rechner das Paket los über das LAN zum Router. Der Router ermittelt in seiner IP-Routing-Tabelle die Gegenstelle, über die die Ziel-IP-Adresse erreichbar ist, z.B. 'Provider_A'.

b **Verbindungsdaten für die Gegenstelle**
Mit diesem Namen prüft der Router dann die Namenliste und findet die notwendigen Verbindungsdaten für Provider A. Zu diesen Verbindungsdaten gehören z.B die WAN-Schnittstelle (DSL, ISDN) über die der Provider angewählt wird, Protokollinformationen oder die für eine

ISDN-Wählverbindung notwendige Rufnummer. Außerdem erhält der Router aus der PPP-Liste Benutzernamen und Passwort, die für die Anmeldung notwendig sind.

c **Aufbau der WAN-Verbindung**
Der Router kann dann eine Verbindung über eine WAN-Schnittstelle zum Providers A aufbauen. Er authentifiziert sich mit Benutzernamen und Passwort.

d **Weitergabe des Datenpaketes**
Sobald die Verbindung hergestellt ist, kann der Router das Datenpaket ins Internet weitergeben.

5.2 IP-Routing

Ein IP-Router arbeitet zwischen Netzen, die TCP/IP als Netzwerk-Protokoll verwenden. Dabei werden nur Daten übertragen, deren Zieladressen in der Routing-Tabelle eingetragen sind. In diesem Abschnitt erfahren Sie, wie die IP-Routing-Tabelle in einem Router von LANCOM Systems aufgebaut ist und mit welchen weiteren Funktionen das IP-Routing unterstützt wird.

5.2.1 Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welche Gegenstelle (also welchen anderen Router oder Rechner) er die Daten für bestimmte IP-Adressen oder IP-Adress-Bereiche schicken soll. So ein Eintrag heißt auch „Route", weil der Weg der Datenpakete damit beschrieben wird. Da Sie diese Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing". Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing". Dabei tauschen die Router selbstständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Die statische Routing-Tabelle kann bis zu 256 Einträge aufnehmen, die dynamische Tabelle 128. Bei aktiviertem IP-RIP beachtet der IP-Router beide Tabellen.

Außerdem sagen Sie dem Router in der IP-Routing-Tabelle, wie weit der Weg über diese Route ist, damit im Zusammenspiel mit IP-RIP bei mehreren Routen zum gleichen Ziel der günstigste ausgewählt werden kann. Die Grundeinstellung für die Distanz zu einem anderen Router ist 2, d.h., der Router ist direkt erreichbar. Alle lokal erreichbaren Geräte, also weitere Router im eigenen LAN oder Arbeitsplatzrechner, die über Proxy-ARP

DE

angeschlossen sind, werden mit der Distanz 0 eingetragen. Mit dem gezielten Eintrag einer höheren Distanz (bis 14) wird die „Qualität" dieser Route herabgesetzt. Solche „schlechteren" Routen sollen nur dann verwendet werden, wenn keine andere Route zu der entsprechenden Gegenstelle gefunden werden kann.

Konfiguration der Routing-Tabelle

Konfigurationstool	Aufruf
LANconfig	IP-Router / Routing / Routing-Tabelle
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / IP-Routing-Tab.
Terminal/Telnet	`cd /Setup/IP-Router/IP-Routing-Tab.`

Eine IP-Routing-Tabelle kann beispielsweise so aussehen:

IP-Adresse	IP-Netzmaske	Router-Name	Distanz	Maskierung
192.168.120.0	255.255.255.0	MAIN	2	Aus
192.168.125.0	255.255.255.0	NODE1	3	Aus
192.168.130.0	255.255.255.0	191.168.140.123	0	Aus

Was bedeuten die einzelnen Einträge in der Liste?

- IP-Adresse und IP-Netzmaske

  Das ist die Adresse des Zielnetzes, zu dem Datenpakete geschickt werden können, mit der zugehörigen Netzmaske. Mit der Netzmaske und der Ziel-IP-Adresse aus den ankommenden Datenpaketen prüft der Router, ob das Paket in das Zielnetz gehört.

  Die Route mit der IP-Adresse '255.255.255.255' und der Netzmaske '0.0.0.0' ist die Default-Route. Alle Datenpakete, die nicht durch andere Routing-Einträge geroutet werden können, werden über diese Route übertragen.

- Router-Name

  An diese Gegenstelle überträgt der Router die zur IP-Adresse und Netzmaske passenden Datenpakete. Ist die Gegenstelle ein Router in einem anderen Netz oder ein einzelner Arbeitsplatzrechner, dann steht hier ein Name. Kann der eigene Router die Gegenstelle nicht selbst

erreichen, steht hier die IP-Adresse eines anderen Routers, der den Weg ins Zielnetz kennt.

Der Router-Name gibt an, was mit den zur IP-Adresse und Netzmaske passenden Datenpaketen geschehen soll.

Routen mit dem Router-Namen '0.0.0.0' bezeichnen Ausschluss-Routen. Datenpakete für diese „Null-Routen" werden verworfen und nicht weitergeleitet. Damit werden z.B. die im Internet verbotenen Routen (private Adressräume, z.B. '10.0.0.0') von der Übertragung ausgeschlossen.

Wird als Router-Name eine IP-Adresse eingetragen, handelt es sich dabei um einen lokal erreichbaren Router, der für die Übertragung der entsprechenden Datenpakete zuständig ist.

- Distanz

  Anzahl der zwischen dem eigenen und dem Ziel liegenden Router. Dieser Wert wird bei Weitverkehrsverbindungen oft auch mit den Kosten der Übertragung gleichgesetzt und zur Unterscheidung zwischen preiswerten und teuren Übertragungswegen genutzt. Die eingetragenen Distanzwerte werden wie folgt propagiert:

  - Während eine Verbindung zu einem Zielnetz existiert, werden alle über diese Verbindung erreichbaren Netze mit einer Distanz von 1 propagiert.
  - Alle nicht verbundenen Netze werden mit der Distanz propagiert, die in der Routing-Tabelle eingetragen ist (mindestens jedoch mit einer Distanz von 2), solange noch ein freier Übertragungskanal verfügbar ist.
  - Ist kein Kanal mehr frei, so werden die verbleibenden Netze mit einer Distanz 16 (= unreachable) propagiert.
  - Eine Ausnahme bilden die Gegenstellen, die über Proxy-ARP angeschlossen sind. Diese „Proxy-Hosts" werden gar nicht propagiert.

- Maskierung

  Mit der Option 'Maskierung' in der Routing-Tabelle informieren Sie den Router darüber, welche IP-Adresse er bei der Weitergabe der Pakete verwenden soll.

  Weitere Informationen finden Sie im Abschnitt 'Das Versteck – IP-Masquerading (NAT, PAT)' auf Seite 80.

DE

5.2.2 Lokales Routing

Sie kennen das folgende Verhalten der Arbeitsplatzrechner in einem lokalen Netz: Möchte der Rechner ein Datenpaket an eine IP-Adresse senden, die nicht in seinem eigenen LAN liegt, sucht er nach einem Router, der ihm weiterhelfen kann. Dieser Router wird normalerweise dem Betriebssystem durch den Eintrag als Standard-Router oder Standard-Gateway bekanntgegeben. Gibt es in einem Netz mehrere Router, so kann oft nur ein Standard-Router eingetragen werden, der alle dem Arbeitsplatzrechner unbekannten IP-Adressen erreichen können soll. Manchmal kann dieser Standard-Router jedoch nicht selbst das Zielnetz erreichen, er kennt aber einen anderen Router, der zu diesem Ziel findet.

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

Standardmäßig schickt der Router dem Rechner eine Antwort mit der Adresse des Routers, der die Route ins Ziel-Netz kennt (diese Antwort nennt man ICMP-Redirect). Der Arbeitsplatzrechner übernimmt daraufhin diese Adresse und schickt das Datenpaket sofort an den anderen Router.

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing. Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem werden dann keine ICMP-Redirects mehr geschickt. Die Einstellung erfolgt unter:

Konfigurationstool	Aufruf
LANconfig	IP-Router / Allgemein / Pakete im lokalen Netz weiterleiten
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / Lok.-Routing
Terminal/Telnet	`set /Setup/IP-Router/Lok.-Routing Ein`

Lokales Routing kann im Einzelfall sehr hilfreich sein, sollte aber auch nur im Einzelfall verwendet werden. Denn lokales Routing führt zu einer Verdoppelung aller Datenpakete zum gewünschten Zielnetz. Die Daten werden erst zum Standard-Router und von diesem erneut zum eigentlich zuständigen Router im lokalen Netz geschickt.

DE

5.2.3 Dynamisches Routing mit IP-RIP

Neben der statischen Routing-Tabelle verfügen Router von LANCOM Systems auch über eine dynamische Routing-Tabelle mit bis zu 128 Einträgen. Diese Tabelle füllt der Anwender im Gegensatz zu der statischen nicht aus, das erledigt der Router selbst. Dazu nutzt er das Routing Information Protocol (RIP). Über dieses Protokoll tauschen alle Geräte, die RIP beherrschen, Informationen über die erreichbaren Routen aus.

Welche Informationen werden über IP-RIP propagiert?

Ein Router teilt in den IP-RIP-Informationen den anderen Routern im Netz die Routen mit, die er in seiner eigenen statischen Tabelle findet. Nicht berücksichtigt werden dabei die folgenden Einträge:

- Routen, die mit der Router-Einstellung '0.0.0.0' verworfen werden.
- Routen, die auf andere Router im lokalen Netz lauten.
- Routen, die einzelne Rechner über Proxy-ARP an das LAN anbinden.

Die Einträge in der statischen Routing-Tabelle werden zwar von Hand gesetzt, trotzdem ändern sich diese Informationen je nach Verbindungssituation der Router und damit auch die versendeten RIP-Pakete.

- Solange der Router eine Verbindung zu einer Gegenstelle aufgebaut hat, gibt er alle über diese Route erreichbaren Netze in den RIPs mit der Distanz '1' weiter. Damit werden andere Router im LAN darüber informiert, dass hier bei diesem Router eine bestehende Verbindung zu dieser Gegenstelle genutzt werden kann. So kann zusätzlicher Verbindungsaufbau von Routern mit Wählverbindungen verhindert und ggf. Verbindungskosten reduziert werden.
- Wenn darüber hinaus in diesem Router keine weitere Verbindung zu einer anderen Gegenstelle aufgebaut werden kann, werden alle anderen Routen mit der Distanz '16' im RIP weitergemeldet. Die '16' steht dabei für „Im Moment ist diese Route nicht erreichbar". Dass ein Router neben der bestehenden Verbindung keine weitere aufbauen kann, liegt an einer der folgenden Ursachen:
  - Auf allen anderen Kanälen ist schon eine andere Verbindung hergestellt (auch über *LANCAPI*).
  - Die Y-Verbindungen für den S_0-Anschluss sind in der Interface-Tabelle ausdrücklich ausgeschlossen.
  - Die bestehende Verbindung benutzt alle B-Kanäle (Kanalbündelung).

- Bei der bestehenden Verbindung handelt es sich um eine Festverbindung. Nur wenige ISDN-Anbieter ermöglichen es, neben einer Festverbindung auf dem ersten B-Kanal eine Wählverbindung auf dem zweiten B-Kanal aufzubauen.

Welche Informationen nimmt der Router aus empfangenen IP-RIP-Paketen?

Wenn der Router IP-RIP-Pakete empfängt, baut er sie in seine dynamische IP-Routing-Tabelle ein, und die sieht etwa so aus:

IP-Adresse	IP-Netzmaske	Zeit	Distanz	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

Was bedeuten die Einträge?

IP-Adresse und Netzmaske bezeichnen das Ziel-Netz, die Distanz gibt die Anzahl der zwischen Sender und Empfänger liegenden Router an, die letzte Spalte zeigt an, welcher Router diese Route bekannt gemacht hat. Bleibt die 'Zeit'. Damit zeigt die dynamische Tabelle an, wie alt die entsprechende Route ist. Der Wert in dieser Spalte gilt als Multiplikator für das Intervall, in dem die RIP-Pakete eintreffen, eine '1' steht also für etwa 30 Sekunden, eine '5' für etwa 2,5 Minuten usw. Wenn eine Information über eine Route neu eintrifft, gilt diese Route natürlich als direkt erreichbar und erhält die Zeit '1'. Nach Ablauf der entsprechenden Zeit wird der Wert in dieser Spalte automatisch erhöht. Nach 3,5 Minuten wird die Distanz auf '16' gesetzt (Route nicht erreichbar), nach 5,5 Minuten wird die Route gelöscht.

Wenn der Router nun ein IP-RIP-Paket empfängt, muss er entscheiden, ob er die darin enthaltenen Routen in seine dynamische Tabelle aufnehmen soll oder nicht. Dazu geht er wie folgt vor:

- Die Route ist in der Tabelle noch gar nicht vorhanden, dann wird sie aufgenommen (sofern Platz in der Tabelle ist).
- Die Route ist in der Tabelle vorhanden mit der Zeit von '5' oder '6'. Die neue Route wird dann verwendet, wenn sie die gleiche oder eine bessere Distanz aufweist.
- Die Route ist in der Tabelle vorhanden mit der Zeit von '7' bis '10', hat also die Distanz '16'. Die neue Route wird auf jeden Fall verwendet.

- Die Route ist in der Tabelle vorhanden. Die neue Route kommt von dem gleichen Router, der auch diese Route bekannt gegeben hat, hat aber eine schlechtere Distanz als der bisherige Eintrag. Wenn ein Gerät so die Verschlechterung seiner eigenen statischen Routing-Tabelle bekannt macht (z.B. durch den Abbau einer Verbindung steigt die Distanz von '1' auf '2', siehe unten), dann glaubt der Router ihm das und nimmt den schlechteren Eintrag in seine dynamische Tabelle auf.

RIP-Pakete aus dem WAN werden nicht beachtet und sofort verworfen! RIP-Pakete aus dem LAN werden ausgewertet und nicht im LAN weitergeleitet!

Zusammenspiel: statische und dynamische Tabelle

Aus der statischen und der dynamischen Tabelle stellt der Router die eigentliche IP-Routing-Tabelle zusammen, mit der er den Weg für die Datenpakete bestimmt. Dabei nimmt er zu den Routen aus der eigenen statischen Tabelle die Routen aus der dynamischen Tabelle auf, die er selber nicht kennt oder die eine kürzere Distanz aufweisen als die eigene (statische) Route.

Skalierung durch IP-RIP

Verwenden Sie mehrere Router in einem lokalen Netz mit IP-RIP, können Sie die Router im lokalen Netz nach außen hin als einen einzigen großen Router darstellen. Dieses Vorgehen nennt man auch „Skalierung". Durch den regen Informationsaustausch der Router untereinander steht so ein Router mit prinzipiell beliebig vielen Übertragungswegen zur Verfügung.

Konfiguration der IP-RIP-Funktion

Konfigurationstool	Menü/Tabelle
LANconfig	IP-Router / Allgemein / RIP-Optionen
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / RIP-Einstellung
Terminal/Telnet	`cd /Setup/IP-Router-Modul/RIP-Einstellung`

- Im Feld 'RIP-Unterstützung' (bzw. 'RIP-Typ') gibt es folgende Auswahl:
  - 'Aus': IP-RIP wird nicht verwendet (Standard).

- 'RIP-1': RIP-1- und RIP-2-Pakete werden empfangen, aber nur RIP-1-Pakete gesendet.
- 'RIP-1 kompatibel': es werden ebenfalls RIP-1- und RIP-2-Pakete empfangen. Gesendet werden RIP-2-Pakete als IP-Broadcast.
- 'RIP-2': Wie 'RIP-1 kompatibel', nur werden alle RIP-Pakete an die IP-Multicast-Adresse 224.0.0.9 gesendet.

- Der Eintrag unter 'RIP-1-Maske' (bzw. 'R1-Maske') kann auf folgende Werte gesetzt werden:
  - 'Klasse' (Standard): Die im RIP-Paket verwendete Netzwerkmaske ergibt sich direkt aus der IP-Adress-Klasse, d.h., für die Netzwerkklassen werden folgende Netzwerkmasken verwendet:

Klasse A	255.0.0.0
Klasse B	255.255.0.0
Klasse C	255.255.255.0

  - 'Adresse': Die Netzwerkmaske ergibt sich aus dem 1. gesetzten Bit der eingetragenen IP-Adresse. Dieses und alle höherwertigen Bits innerhalb der Netzwerkmaske werden gesetzt. Aus der IP-Adresse 127.128.128.64 ergibt sich so z.B. die IP-Netzmaske 255.255.255.192.
  - 'Klasse+Adresse': Die Netzwerkmaske wird aus der IP-Adressen-Klasse und einem angefügten Teil nach dem Adressverfahren gebildet. Aus obiger Adresse und der Netzmaske 255.255.0.0 ergibt sich somit die IP-Netzmaske 255.128.0.0.

RIP-fähige Router versenden die RIP-Pakete ungefähr alle 30 Sekunden. Der Router ist nur dann auf das Versenden und Empfangen von RIPs eingestellt, wenn er eine eindeutige IP-Adresse hat. In der Grundeinstellung mit der IP-Adresse xxx.xxx.xxx.254 ist das IP-RIP-Modul ausgeschaltet.

5.2.4 Policy Based Routing

Policy Based Routing bezeichnet ein Verfahren, bei dem bestimmte Datenpakete bevorzugt behandelt werden sollen. Dazu wird ein spezielles Feld innerhalb der IP-Datenpakete ausgewertet, das Type-of-Service(TOS)-Feld. Diese bevorzugte Behandlung einiger Datenpakete soll z.B. die Konfiguration der Router über das WAN erleichtern, wenn gleichzeitig viele Daten übertragen werden sollen.

Policy Based Routing kann wie folgt ein- und ausgeschaltet werden:

DE

Konfigurationstool	Menü/Tabelle
LANconfig	IP-Router / Allgemein / Type-Of-Service-Feld berücksichtigen
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / Routing-Methode / Routing-Methode

Terminal/Telnet	`cd /Setup/IP-Router-Modul/Routing-Methode`
	`set Routing-Methode TOS (ein)`
	`set Routing-Methode NORMAL (aus)`

5.2.5 SYN/ACK-Speedup

Das SYN/ACK-Speedup-Verfahren dient der Beschleunigung des IP-Datenverkehrs. Beim SYN/ACK-Speedup werden IP-Kontrollzeichen (SYN für Synchronisation und ACK für Acknowledge) innerhalb des Sendebuffers gegenüber einfachen Datenpaketen bevorzugt behandelt. Dadurch wird die Situation vermieden, dass Kontrollzeichen länger in der Sendeschlange hängen bleiben und die Gegenstelle deshalb aufhört, Daten zu senden.

Der größte Effekt tritt beim SYN/ACK-Speedup bei schnellen Verbindungen ein, wenn gleichzeitig in beiden Richtungen mit hoher Geschwindigkeit Datenmengen übertragen werden.

Werkseitig ist der SYN/ACK-Speedup eingeschaltet.

Ausschalten in Problemfällen

Durch die bevorzugte Behandlung einzelner Pakete wird die ursprüngliche Paketreihenfolge geändert. Obwohl TCP/IP keine bestimmte Paketreihenfolge gewährleistet, kann es in einzelnen Anwendungen zu Problemen kommen. Das betrifft nur Anwendungen, die abweichend vom Protokollstandard eine bestimmte Paketreihenfolge voraussetzen. Für diesen Fall kann der SYN/ACK-Speedup ausgeschaltet werden:

DE

Konfigurationstool	Menü/Tabelle
LANconfig	IP-Router / Allgemein / TCP SYN- und ACK-Pakete bevorzugt weiterleiten
WEBconfig	Experten-Konfiguration / Setup / IP-Router-Modul / Routing-Methode / SYN/ACK-Speedup
Terminal/Telnet	`cd /Setup/IP-Router-Modul/Routing-Methode` `set SYN/ACK-Speedup AUS`

5.3 Die Konfiguration von Gegenstellen

Gegenstellen werden in zwei Tabellen konfiguriert:

- In der Namenliste (bzw. den Namenlisten) werden alle Informationen eingestellt, die individuell für nur eine Gegenstelle gelten.
- Parameter für die unteren Protokollebenen (unterhalb von IP bzw. IPX) werden in der Kommunikations-Layer-Tabelle definiert.

In diesem Abschnitt wird die Konfiguration der Authentifizierung (Protokoll, Benutzername, Passwort) nicht behandelt. Informationen zur Authentifizierung finden Sie im Abschnitt 'Verbindungsaufbau mit PPP' auf Seite 139.

5.3.1 Namenliste

Die verfügbaren Gegenstellen werden in der Namenliste mit einem geeigneten Namen und zusätzlichen Parametern angelegt.

Konfigurationstool	Menü/Tabelle
LANconfig	Kommunikation / Gegenstellen / Namenliste
WEBconfig	Experten-Konfiguration / Setup / WAN-Modul / Namenliste
Terminal/Telnet	`cd /Setup/WAN-Modul` `set Namenliste [...]`

DE

5.3.2 Layer-Liste

Mit einem Layer definieren Sie eine Sammlung von Protokoll-Einstellungen, die für die Verbindung zu bestimmten Gegenstellen verwendet werden soll. Die Liste der Kommunikations-Layer finden Sie unter:

Konfigurationstool	Liste
LANconfig	Kommunikation / Allgemein / Kommunikations-Layer
WEBconfig	Experten-Konfiguration / Setup / WAN-Modul / Layer-Liste
Terminal/Telnet	`cd /Setup/WAN-Modul` `set Layer-Liste [...]`

In der Kommunikations-Layer-Liste sind die gängigen Protokollkombinationen bereits vordefiniert. Änderungen oder Ergänzungen sollten Sie nur vornehmen, wenn Gegenstellen inkompatibel zu den vorhandenen Layern sind. Die möglichen Optionen finden Sie in der folgenden Übersicht.

Beachten Sie, dass die im LANCOM vorhandenen Parameter vom Funktionsumfang des Gerätes abhängen. Es kann daher sein, dass Ihr Gerät nicht alle hier beschriebenen Optionen anbietet.

Parameter	Bedeutung	
Layername	Unter diesem Namen wird der Layer in den Namenlisten ausgewählt.	
Encapsulation	Für die Datenpakete können zusätzliche Kapselungen eingestellt werden.	
	'Transparent'	Keine zusätzliche Kapselung.
	'Ethernet'	Kapselung als Ethernet-Frames.
	'LLC-MUX'	Multiplexing über ATM mit LLC/SNAP-Kapselung nach RFC 2684. Mehrere Protokolle können im selben VC (Virtual Channel) übertragen werden.
	'VC-MUX'	Multiplexing über ATM durch Aufbau zusätzlicher VCs nach RFC 2684.

DE

Parameter	Bedeutung	
Layer-3	Folgende Optionen stehen für die Vermittlungsschicht (oder Netzwerkschicht) zur Verfügung:	
	'Transparent'	Es wird kein zusätzlicher Header eingefügt.
	'PPP'	Der Verbindungsaufbau erfolgt nach dem PPP-Protokoll (im synchronen Modus, d.h. bitorientiert). Die Konfigurationsdaten werden der PPP-Tabelle entnommen.
	'AsyncPPP'	Wie 'PPP', nur wird der asynchrone Modus verwendet. PPP arbeitet also zeichenorientiert.
	'... mit Script'	Alle Optionen können wahlweise mit eigenem Script ausgeführt werden. Das Script wird in der Script-Liste angegeben.
	'DHCP'	Zuordnung der Netzwerkparameter über DHCP.
Layer-2	In diesem Feld wird der obere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:	
	'Transparent'	Es wird kein zusätzlicher Header eingefügt.
	'X.75LAPB'	Verbindungsaufbau nach X.75 und LAPM (Link Access Procedure Balanced).
	'PPPoE'	Kapselung der PPP-Protokollinformationen in Ethernet-Frames.
Optionen	Hier können Sie die Kompression der übertragenen Daten und die Bündelung von Kanälen aktivieren. Die gewählte Option wird nur dann wirksam, wenn sie sowohl von den verwendeten Schnittstellen als auch von den gewählten Layer-2- und Layer-3-Protokollen unterstützt wird. Weitere Informationen finden Sie im Abschnitt 'Kanalbündelung mit MLPPP' auf Seite 149.	
Layer-1	In diesem Feld wird der untere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:	
	'AAL-5'	ATM-Anpassungsschicht
	'ETH-10'	Transparentes Ethernet nach IEEE 802.3.
	'HDLC'	Sicherung und Synchronisation der Datenübertragung nach HDLC (im 7- oder 8-bit-Modus).
	'V.110'	Übertragung nach V.110 mit maximal 38.400 bit/Sekunde, z.B. für Einwahl per HSCSD-Mobiltelefon
	Modem	Modem-Übertragung (benötigt Fax-Modem-Option)

DE

5.4 Verbindungsaufbau mit PPP

Router von LANCOM Systems unterstützen auch das Point-to-Point Protocol (PPP). PPP ist ein Sammelbegriff für eine ganze Reihe von WAN-Protokollen, die das Zusammenspiel von Routern verschiedener Hersteller erleichtern, denn dieses Protokoll wird von fast allen Herstellern unterstützt.

Und gerade weil das PPP nicht einer bestimmten Betriebsart der Router zugeordnet werden kann und natürlich auch wegen der großen und in Zukunft noch weiter steigenden Bedeutung dieser Protokoll-Familie, möchten wir Ihnen die Funktionen der Geräte im Zusammenhang mit dem PPP hier in einem eigenen Abschnitt vorstellen.

5.4.1 Das Protokoll

Was ist PPP?

Das Point-to-Point Protocol (PPP) wurde speziell für Netzwerkverbindungen über serielle Kanäle entwickelt und hat sich als Standard für Verbindungen zwischen Routern behauptet. Es realisiert folgende Funktionen:

- Passwortschutz nach PAP, CHAP oder MS-CHAP
- Rückruf-Funktionen
- Aushandlung der über die aufgebaute Verbindung zu benutzenden Netzwerkprotokolle (z.B. IP). Dazu gehören auch für diese Protokolle notwendige Parameter wie z.B. IP-Adressen. Diese Verhandlung läuft über das Protokoll IPCP (IP Control Protocol) ab.
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)
- Bündelung von mehreren ISDN-Kanälen (Multilink PPP

Für Router-Verbindungen ist PPP der Standard für die Kommunikation zwischen Geräten bzw. der WAN-Verbindungssoftware unterschiedlicher Hersteller. Um eine erfolgreiche Datenübertragung nach Möglichkeit sicherzu- stellen, erfolgt die Verhandlung der Verbindungsparameter und eine Einigung auf einen gemeinsamen Nenner über standardisierte Steuerungsprotokolle (z.B. LCP, IPCP, CCP), die im PPP enthalten sind.

Wozu wird PPP verwendet?

Das Point-to-Point Protocol wird bei folgenden Anwendungen sinnvoll eingesetzt:

- aus Kompatibilitätsgründen z.B. bei Kommunikation mit Fremdroutern

- Remote Access von entfernten Arbeitsplatzrechnern mit ISDN-Adaptern
- Internet-Access (mit der Übermittlung von Adressen)

Das im *LANCOM* implementierte PPP kann synchron oder asynchron sowohl über eine transparente HDLC-Verbindung als auch über eine X.75-Verbindung verwendet werden.

Die Phasen einer PPP-Verhandlung

Der Verbindungsaufbau über PPP startet immer mit einer Verhandlung der Parameter, die für die Verbindung verwendet werden sollen. Diese Verhandlung läuft in vier Phasen ab, deren Kenntnis für die Konfiguration und Fehlersuche wichtig sind.

- Establish-Phase

  Nach einem Verbindungsaufbau über den Datenkommunikationsteil startet die Aushandlung der Verbindungsparameter über das LCP.

  Es wird festgestellt, ob die Gegenstelle auch bereit ist, PPP zu benutzen, die Paketgrößen und das Authentifizierungsprotokoll (PAP, CHAP, MS-CHAP oder keines) werden festgelegt. Danach wechselt das LCP in den Opened-Zustand.

- Authenticate-Phase

  Falls notwendig, werden danach die Passworte ausgetauscht. Bei Authentifizierung nach PAP wird das Passwort nur einmalig übertragen. Bei Benutzung von CHAP oder MS-CHAP wird ein verschlüsseltes Passwort periodisch in einstellbaren Abständen gesendet.

  Evtl. wird in dieser Phase auch ein Rückruf über CBCP (Callback Control Protocol) ausgehandelt.

- Network-Phase

  Im *LANCOM* sind die Protokolle IPCP und IPXCP implementiert.

  Nach erfolgreicher Übertragung des Passwortes können die Netzwerk-Layer IPCP und/oder IPXCP aufgebaut werden.

  Ist die Verhandlung der Parameter für mindestens eines der Netzwerk-Layer erfolgreich verlaufen, können von den Router-Modulen IP- und/oder IPX-Pakete auf der geöffneten (logischen) Leitung übertragen werden.

- Terminate-Phase

  In der letzten Phase wird die Leitung geschlossen, wenn die logischen Verbindungen für alle Protokolle abgebaut sind.

Die PPP-Verhandlung im *LANCOM*

Der Verlauf einer PPP-Verhandlung wird in der PPP-Statistik der Geräte protokolliert und kann im Fehlerfall mit Hilfe der dort detailliert gezählten Protokoll-Pakete überprüft werden.

Eine weitere Analyse-Möglichkeit bieten die PPP-Trace-Ausgaben. Mit dem Befehl

```
trace + ppp
```

kann die Ausgabe der ausgetauschten PPP-Protokoll-Frames innerhalb einer Terminal-Sitzung gestartet werden. Wird diese Terminal-Sitzung in einem Log-File protokolliert, kann nach Abbruch der Verbindung eine detaillierte Analyse erfolgen.

5.4.2 Alles o.k.? Leitungsüberprüfung mit LCP

Beim Verbindungsaufbau über PPP handeln die beteiligten Geräte ein gemeinsames Verhalten während der Datenübertragung aus. Sie entscheiden z.B. zunächst, ob mit den Einstellungen der Sicherungsverfahren, Namen und Passwörter überhaupt eine Verbindung zustande kommen darf.

Wenn die Verbindung einmal steht, kann mit Hilfe des LCPs die Zuverlässigkeit der Leitung ständig überprüft werden. Innerhalb des Protokolls geschieht dies mit dem LCP-Echo-Request und dem zugehörigen LCP-Echo-Reply. Der LCP-Echo-Request ist eine Anfrage in Form eines Datenpakets, das neben den reinen Nutzdaten zur Gegenstelle übertragen wird. Wenn auf diese Anfrage eine gültige Antwort (LCP-Echo-Reply) zurückgeschickt wird, ist die Verbindung zuverlässig und stabil. Zur dauerhaften Überprüfung der Verbindung wird dieser Request in bestimmten Abständen wiederholt.

Was passiert nun, wenn der Reply ausbleibt? Zuerst werden einige Wiederholungen der Anfrage gestartet, um kurzfristige Störungen der Leitung auszuschließen. Wenn alle diese Wiederholungen unbeantwortet bleiben, wird die Leitung abgebaut und ein Ersatzweg gesucht. Streikt beispielsweise die Highspeed-Verbindung, kann als Backup eine vorhandene ISDN-Schnittstelle den Weg ins Internet bahnen.

Beim Remote Access von einzelnen Arbeitsplatzrechnern mit Windows-Betriebssystem empfehlen wir, die regelmäßigen LCP-Anfragen auszuschalten, weil diese Betriebssysteme die LCP-Echo-Requests nicht beantworten.

DE

Das Verhalten der LCP-Anfragen stellen Sie in der PPP-Liste für jede Verbindung einzeln ein. Mit dem Eintrag in die Felder 'Zeit' und 'Wdh.' legen Sie fest, in welchen Abständen die LCP-Anfrage gestellt werden soll und wie viele Wiederholungen beim Ausbleiben der Antwort gestartet werden, bis die Leitung als gestört bezeichnet werden darf. Mit einer Zeit von '0' und '0' Wiederholungen stellen Sie die LCP-Requests ganz ab.

5.4.3 Zuweisung von IP-Adressen über PPP

Zur Verbindung von Rechnern, die TCP/IP als Netzwerkprotokoll einsetzen, benötigen alle Beteiligten eine gültige und eindeutige IP-Adresse. Wenn nun eine Gegenstelle keine eigene IP-Adresse hat (z.B. der einzelne Arbeitsplatzrechner eines Teleworkers), dann kann der *LANCOM* ihm für die Dauer der Verbindung eine IP-Adresse zuweisen und so die Kommunikation ermöglichen.

Diese Art der Adresszuweisung wird während der PPP-Verhandlung durchgeführt und nur für Verbindungen über das WAN eingesetzt. Die Zuweisung von Adressen mittels DHCP wird dagegen (normalerweise) innerhalb eines lokalen Netzwerks verwendet.

Die Zuweisung einer IP-Adresse wird nur dann möglich, wenn der LANCOM die Gegenstelle beim Eintreffen des Anrufs über die Rufnummer oder den Namen identifizieren kann, d.h. die Authentifizierung erfolgreich war.

Beispiele

- Remote Access

  Die Zuweisung der Adresse wird durch einen speziellen Eintrag in der IP-Routing-Tabelle ermöglicht. Neben dem Eintrag der IP-Adresse, die der Gegenstelle aus dem Feld 'Router-Name' zugewiesen werden soll, wird als Netzmaske die 255.255.255.255 angegeben. Der Routername ist in diesem Fall der Name, mit dem sich die Gegenstelle beim *LANCOM* anmelden muss.

  Neben der IP-Adresse werden der Gegenstelle bei dieser Konfiguration auch die Adressen der DNS- und NBNS-Server (Domain Name Server und NetBIOS Name Server) inkl. des Backup-Servers aus den Einträgen im TCP/IP-Modul übermittelt.

  Damit das Ganze funktioniert, muss die Gegenstelle natürlich auch so eingestellt sein, dass sie die IP-Adresse und die Namensserver vom *LANCOM* bezieht. Das geschieht z.B. im DFÜ-Netzwerk von Windows

durch die Einträge in den 'TCP-Einstellungen' unter 'IP-Adresse' bzw. 'DNS-Konfiguration'. Hier werden die Optionen 'Vom Server zugewiesene IP-Adresse' und 'Vom Server zugewiesene Namensserveradressen' aktiviert.

- Internet-Zugang

  Wird über den *LANCOM* der Zugang zum Internet für ein lokales Netz realisiert, kann die Zuweisung von IP-Adressen den umgekehrten Weg nehmen. Hierbei sind Konfigurationen möglich, in denen der *LANCOM* selbst keine im Internet gültige IP-Adresse hat und sich für die Dauer der Verbindung eine vom Internet-Provider zuweisen lässt. Neben der IP-Adresse erhält der *LANCOM* während der PPP-Verhandlung auch Informationen über DNS-Server beim Provider.

  Im lokalen Netz ist der *LANCOM* nur mit seiner intern gültigen Intranet-Adresse bekannt. Alle Arbeitsplatzrechner im lokalen Netz können dann auf den gleichen Internet-Account zugreifen und auch z.B. den DNS-Server erreichen.

Die zugewiesenen Adressen schauen sich Windows-Anwender per *LANmonitor* an. Neben dem Namen der verbundenen Gegenstelle finden Sie hier die aktuelle IP-Adresse sowie die Adressen von DNS- und NBNS-Servern. Auch Optionen wie die Kanalbündelung oder die Dauer der Verbindung werden angezeigt.

5.4.4 Einstellungen in der PPP-Liste

In der PPP-Liste können Sie für jede Gegenstelle, die mit Ihrem Netz Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen.

Konfigurationstool	Liste
LANconfig	Kommunikation / Protokolle / PPP-Liste
WEBconfig	Experten-Konfiguration / Setup / WAN-Modul / PPP-Liste
Terminal/Telnet	`cd /Setup/WAN-Modul` `set PPP-Liste [...]`

Die PPP-Liste kann bis zu 64 Einträge aufnehmen und die folgende Werte enthalten:

DE

In dieser Spalte der PPP-Liste ...	... tragen Sie folgende Werte ein:
Gegenstelle (Gerätename)	Name der Gegenstelle, mit dem sich diese bei Ihrem Router anmeldet
Benutzername (Username)	Name, mit dem sich Ihr Router bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Gerätename Ihres Routers verwendet.
Passwort	Passwort, das von Ihrem Router an die Gegenstelle übertragen wird (falls gefordert). * in der Liste zeigt an, dass ein Eintrag vorhanden ist.
Überprüfung der Gegenstelle (Authentifizierung)	Verfahren zur Sicherung der PPP-Verbindung ('PAP', 'CHAP' oder 'keine'). Ihr eigener Router verlangt von der Gegenstelle die Einhaltung dieses Verfahrens! Nicht etwa umgekehrt. Daher bietet sich die Sicherung nach 'PAP', 'CHAP' nicht an bei Verbindungen zu Internet Service Providern, die uns vielleicht kein Passwort übermitteln wollen. Für solche Verbindungen wählen Sie 'keine' Sicherung.
Zeit	Zeit zwischen zwei Überprüfungen der Verbindung mit LCP (siehe folgender Abschnitt). Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z.B. 2 für 20 Sek.). Der Wert ist gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein. Für Gegenstellen mit Windows-Betriebssystem muss die Zeit auf '0' gesetzt werden!
Wiederholungen (Wdh)	Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluss kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen. Gleichzeitig die Anzahl der „Configure Requests", die der Router maximal aussendet, bevor es von einer Leitungsstörung ausgeht und selber die Verbindung abbaut.
Conf, Fail, Term	Mit diesen Parametern wird die Arbeitsweise des PPPs beeinflusst. Die Parameter sind in der RFC 1661 definiert und werden hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im allgemeinen sind die Default-Einstellungen ausreichend. Diese Parameter können nur über *LANconfig*, SNMP oder TFTP verändert werden!

DE

5.5 Dauerverbindung für Flatrates – Keep-alive

Als Flatrates bezeichnet man pauschale Verbindungstarife, die nicht nach Verbindungszeiten, sondern pauschal für feste Perioden abgerechnet werden. Bei Flatrates lohnt sich der Verbindungsabbau nicht mehr. Im Gegenteil: Neue Mails sollen direkt am PC gemeldet werden, der Heimarbeitsplatz soll kontinuierlich mit dem Firmennetzwerk verbunden sein und man möchte für Freunde und Kollegen über Internet Messenger Dienste (ICQ und ähnliche) pausenlos erreichbar sein. Es ist also wünschenswert, dass Verbindungen ununterbrochen aufrechterhalten werden.

Beim *LANCOM* sorgt das Keep-alive-Verfahren dafür, dass Verbindungen immer dann aufgebaut werden, wenn die Gegenstelle sie gekappt hat.

Konfiguration des Keep-alive-Verfahrens

Das Keep-alive-Verfahren wird in der Namensliste konfiguriert.

Wird die Haltezeit auf 0 Sekunden gesetzt, so wird die Verbindung nicht aktiv vom *LANCOM* beendet. Der automatische Abbau von Verbindungen, über die längere Zeit keine Daten mehr übertragen wurden, wird mit einer Haltezeit von 0 Sekunden also deaktiviert. Durch die Gegenseite unterbrochene Verbindungen werden in dieser Einstellung allerdings nicht automatisch wiederhergestellt.

Bei einer Haltezeit von 9999 Sekunden wird die Verbindung nach jeder Trennung immer automatisch wieder neu aufgebaut. Ebenso wird die Verbindung nach dem Booten des Gerätes automatisch wieder aufgebaut ('auto reconnect').

5.6 Rückruf-Funktionen

LANCOM mit ISDN-Schnittstelle unterstützen einen automatischen Rückruf.

Neben dem Rückruf über den D-Kanal wird auch das von Microsoft spezifizierte CBCP (**C**allback **C**ontrol **P**rotocol) sowie der Rückruf über PPP nach RFC 1570 (PPP LCP Extensions) angeboten. Zusätzlich besteht die Möglichkeit eines besonders schnellen Rückrufs über ein von LANCOM entwickeltes Verfahren. PCs mit Windows-Betriebssystem können nur über das CBCP zurückgerufen werden.

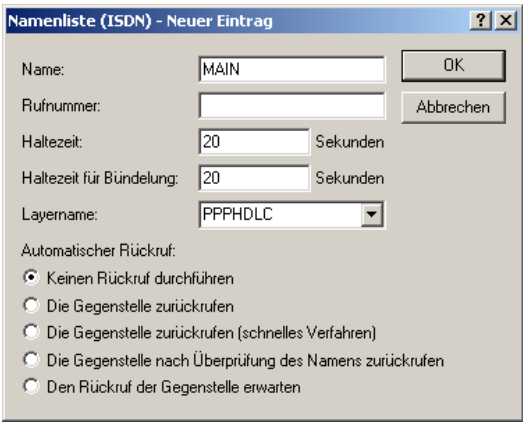
DE

5.6.1 Rückruf nach Microsoft CBCP

Das Microsoft CBCP erlaubt verschiedene Arten, die Rückrufnummer zu bestimmen:

- Der Angerufene ruft nicht zurück.
- Der Angerufene erlaubt es dem Anrufer, die Rückrufnummer selbst anzugeben.
- Der Angerufene kennt die Rückrufnummer und ruft auch **nur** diese zurück.

Über das CBCP ist es möglich, von einem Rechner mit einem Windows-Betriebssystem eine Verbindung zum *LANCOM* aufzunehmen und sich von diesem zurückrufen zu lassen. Die drei möglichen Einstellungen werden über den Rückruf-Eintrag sowie den Rufnummern-Eintrag in der Namenliste ausgewählt.



Keinen Rückruf durchführen

Für diese Einstellung muss der Rückruf-Eintrag bei der Konfiguration über *WEBconfig* oder in der Konsole den Wert 'Aus' haben.

Rückrufnummer vom Anrufer bestimmt

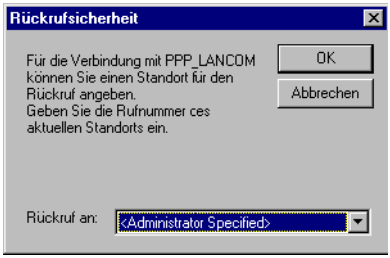
Für diese Einstellung muss der Rückruf-Eintrag auf 'Die Gegenstelle nach Überprüfung des Namens zurückrufen' stehen (bzw. in *WEBconfig* oder in der Konsole den Wert 'Name' haben). In der Namenliste darf **keine** Rufnummer angegeben sein.

Nach der Authentifizierung erscheint beim Anrufer in Windows ein Eingabefenster, das ihn nach der ISDN-Rufnummer des PC fragt.

Rückrufnummer im *LANCOM* bestimmt

Für diese Einstellung muss der Rückruf-Eintrag auf 'Die Gegenstelle nach Überprüfung des Namens zurückrufen' stehen (bzw. in *WEBconfig* oder in der Konsole auf den Wert 'Name' gesetzt sein). In der Namenliste muss **eine** Rufnummer angegeben sein.

Einige Windows-Versionen (insbesondere Windows 98) fordern den Benutzer mit einem Eingabefenster auf, den Rückruf an die im *LANCOM* hinterlegte Rufnummer ('Administrator Specified') zu bestätigen. Andere Windows-Version informieren den Benutzer nur darüber, dass der PC auf den Rückruf vom *LANCOM* wartet.



Der Rückruf an einen Windows-Rechner erfolgt ca. 15 Sekunden, nachdem die erste Verbindung abgebaut wurde. Diese Zeit kann nicht verkürzt werden, da sie von Windows vorgegeben wird.

5.6.2 Schneller Rückruf mit dem LANCOM-Verfahren

Sollen zwei *LANCOM* miteinander kommunizieren, wobei der eine zurückgerufen wird, bietet sich der schnelle Rückruf über das LANCOM-spezifische Verfahren an.

- Der Anrufer, der gerne zurückgerufen werden möchte, stellt in der Namenliste 'Den Rückruf der Gegenstelle erwarten' ein ('Looser' bei Konfiguration über *WEBconfig*, Terminalprogramm oder Telnet).
- Der Rückrufer wählt 'Die Gegenstelle zurückrufen (schnelles Verfahren)' in der Namenliste und stellt die Rufnummer ein ('fast' bei Konfiguration über *WEBconfig*, Terminalprogramm oder Telnet).

Für den schnellen Rückruf nach LANCOM-Verfahren muss die Nummernliste für die Rufannahme auf beiden Seiten gepflegt sein.

DE

5.6.3 Rückruf nach RFC 1570 (PPP LCP Extensions)

Der Rückruf nach 1570 ist das Standardverfahren für den Rückruf von Routern anderer Hersteller. Diese Protokollerweiterung beschreibt fünf Möglichkeiten, einen Rückruf anzufordern. Alle Versionen werden vom *LANCOM* akzeptiert. Es wird jedoch bei allen Varianten gleich verfahren:

Der *LANCOM* baut nach der Authentifizierung der Gegenstelle die Verbindung ab und ruft diese dann einige Sekunden später zurück.

Konfiguration

Für den Rückruf nach PPP wählen Sie in *LANconfig* die Option 'Die Gegenstelle zurückrufen' bzw. 'Auto' bei Konfiguration über *WEBconfig*, Terminalprogramm oder Telnet.

Für den Rückruf nach PPP muss die Nummernliste für die Rufannahme im LANCOM gepflegt sein.

5.6.4 Konfiguration der Rückruf-Funktion im Überblick

In der Namenliste stehen unter *WEBconfig* und Terminalprogramm/Telnet für den Rückruf-Eintrag folgende Optionen zur Verfügung:

Mit diesem Eintrag ...	... stellen Sie den Rückruf so ein:
'Aus'	Es wird nicht zurückgerufen.
'Auto' (nicht bei Windows-Betriebs-systemen, s.u.)	Wenn die Gegenstelle in der Nummernliste gefunden wird, so wird diese zurückgerufen. Hierzu wird der Ruf zunächst abgelehnt und, sobald der Kanal wieder frei ist, zurückgerufen (Dauer ca. 8 Sekunden). Wird die Gegenstelle nicht in der Nummernliste gefunden, so wird sie zunächst als DEFAULT-Gegenstelle angenom-men, und der Rückruf wird während der Protokollverhandlung ausge-handelt. Dabei fällt eine Gebühr von einer Einheit an.
'Name'	Bevor ein Rückruf erfolgt, wird immer eine Protokollverhandlung durchgeführt, auch wenn die Gegenstelle in der Nummernliste gefunden wurde (z.B. für Rechner mit Windows, die sich auf dem Gerät einwählen). Dabei fallen geringe Gebühren an.

Mit diesem Eintrag ...	... stellen Sie den Rückruf so ein:
'fast'	Wenn die Gegenstelle in der Nummernliste gefunden wird, wird der schnelle Rückruf durchgeführt, d.h., der *LANCOM* sendet ein spezielles Signal zur Gegenstelle und ruft sofort zurück, wenn der Kanal wieder frei ist. Nach ca. 2 Sekunden steht die Verbindung. Nimmt die Gegenstelle den Ruf nicht unmittelbar nach dem Signal zurück, so erfolgt zwei Sekunden später ein Rückfall auf das normale Rückrufverfahren (Dauer wieder ca. 8 Sekunden). Dieses Verfahren steht nur an DSS1-Anschlüssen zur Verfügung.
'Looser'	Benutzen Sie die Option 'Looser', wenn von der Gegenstelle ein Rückruf erwartet wird. Diese Einstellung erfüllt zwei Aufgaben gleichzeitig. Zum einen sorgt sie dafür, dass ein eigener Verbindungsaufbau zurückgenommen wird, wenn ein Ruf von der gerade angerufenen Gegenstelle hereinkommt, zum anderen wird mit dieser Einstellung die Funktion aktiviert, auf das schnelle Rückruf-Verfahren reagieren zu können. D.h., um den schnellen Rückruf nutzen zu können, muss sich der Anrufer im 'Looser'-Modus befinden, während beim Angerufenen der Rückruf auf 'LANCOM' eingestellt sein muss.

Die Einstellung 'Name' bietet die höchste Sicherheit, wenn sowohl ein Eintrag in der Nummernliste als auch in der PPP-Liste konfiguriert ist. Die Einstellung 'LANCOM' ermöglicht die schnellste Rückrufmethode zwischen zwei LANCOM Systems-Routern.

*Bei Windows-Gegenstellen **muss** die Einstellung 'Name' gewählt werden.*

5.7 Kanalbündelung mit MLPPP

Wenn Sie eine ISDN-Verbindung zu einer PPP-fähigen Gegenstelle aufbauen, können Sie Ihren Daten Beine machen: Sie können die Daten komprimieren und/oder mehrere B-Kanäle zur Übertragung verwenden (Kanalbündelung).

Die Verbindung mit Kanalbündelung unterscheidet sich von „normalen" Verbindungen dadurch, dass nicht nur ein, sondern mehrere B-Kanäle parallel für die Übertragung der Daten verwendet werden.

Für die Kanalbündelung wird dabei MLPPP (**M**ultilink **PPP**) verwendet. Dieses Verfahren steht natürlich nur zur Verfügung, wenn PPP als B-Kanal-Protokoll verwendet wird. MLPPP bietet sich z.B. an für den Internet-Zugang über Provider, die bei Ihren Einwahlknoten ebenfalls MLPPP-fähige Gegenstellen betreiben.

Zwei Methoden der Kanalbündelung

- Statische Kanalbündelung

  Wenn eine Verbindung mit statischer Kanalbündelung aufgebaut wird, versucht der *LANCOM* nach dem ersten B-Kanal sofort, auch den zweiten B-Kanal aufzubauen. Gelingt dies nicht, weil z.B. dieser Kanal schon durch ein anderes Gerät oder durch eine andere Verbindung im *LANCOM* besetzt ist, wird dieser Aufbauversuch automatisch und regelmäßig solange wiederholt, bis auch der zweite Kanal für diese Verbindung zur Verfügung steht.

- Dynamische Kanalbündelung

  Bei einer Verbindung mit dynamischer Kanalbündelung baut der *LANCOM* zunächst nur einen B-Kanal auf und beginnt mit der Datenübertragung. Wenn er dann während der Verbindung feststellt, dass der Durchsatz eine Weile über einem bestimmten Schwellwert liegt, versucht er den zweiten Kanal dazuzunehmen.

  Wenn der zweite Kanal aufgebaut ist und der Datendurchsatz wieder unter den Grenzwert zurückgeht, wartet der *LANCOM* noch die eingestellte B2-Haltezeit ab und schließt den Kanal dann automatisch wieder. Dabei werden die begonnenen Gebühreneinheiten ausgenutzt, sofern die Gebühreninformationen während der Verbindung übermittelt werden. Der *LANCOM* benutzt den zweiten B-Kanal also nur, wenn und solange er ihn auch wirklich braucht!

So stellen Sie die Kanalbündelung ein

Die Konfiguration der Kanalbündelung für eine Verbindung setzt sich aus drei Einstellungen zusammen:

a Wählen für die Gegenstelle einen Kommunikations-Layer aus der Layer-Liste aus, der in den Layer-2-Optionen die Bündelung aktiviert hat. Wählen Sie unter folgenden Layer-2-Optionen:

  - **compr.** nach dem LZS-Datenkompressionsverfahren (Stac) reduziert das Datenvolumen, wenn die Daten nicht schon vorher komprimiert waren. Dieses Verfahren wird auch von Routern anderer Hersteller und von ISDN-Adaptern unter Windows-Betriebssystemen unterstützt.
  - **buendeln** verwendet zwei B-Kanäle für eine Verbindung.

- **bnd+cmpr** nutzt beides (Komprimierung und Kanalbündelung) und stellt damit die maximal mögliche Übertragungsleistung zur Verfügung.

b Erstellen Sie nun einen neuen Eintrag in der Namenliste. Achten Sie dabei auf die Haltezeiten für die Verbindung. Beachten Sie folgende Regeln:

- Die B1-Haltezeit sollte je nach Anwendungsfall so groß gewählt werden, dass die Verbindung nicht durch das kurzzeitige Ausbleiben von Paketen zu früh abgebaut wird. Erfahrungsgemäß sind Werte zwischen 60 und 180 Sekunden für den Beginn eine gute Basis, die man im Betrieb dann weiter anpassen kann.
- Die B2-Haltezeit entscheidet darüber, ob es sich um eine statische oder dynamische Kanalbündelung handelt (siehe oben). Mit einer B2-Haltezeit von '0' oder '9999' wird die Bündelung statisch, mit Werten dazwischen schaffen Sie die Möglichkeit der dynamischen Kanalbündelung. Die B2-Haltezeit definiert, wie lange der Datendurchsatz unter der Schwelle für die dynamische Kanalbündelung liegen darf, ohne dass der zweite B-Kanal automatisch abgebaut wird.

c Legen Sie in der Router-Interface-Liste mit dem Eintrag für die Y-Verbindung fest, was geschehen soll, wenn während einer laufenden Verbindung mit Kanalbündelung der Wunsch nach einer zweiten Verbindung zu einer anderen Gegenstelle angemeldet wird.

WEBconfig	Experten-Konfiguration / Setup / WAN-Modul / Router-Interface-Liste
Terminal/Telnet	`cd /Setup/WAN-Modul` `set Router-Interface-Liste [...]`

- Y-Verbindung **Ein**: Der Router unterbricht die Bündelverbindung, um die zweite Verbindung zur anderen Gegenstelle aufzubauen. Wenn der zweite Kanal wieder frei wird, holt sich die Bündelverbindung diesen Kanal automatisch wieder zurück (bei statischer Bündelung immer, bei dynamischer nur bei Bedarf).
- Y-Verbindung **Aus**: Der Router hält die bestehende Bündelverbindung, die zweite Verbindung muss warten.

Bitte beachten Sie, dass bei Verwendung der Kanalbündelung die Kosten für zwei Verbindungen anfallen. Dabei sind keine weiteren Verbindungen über die LANCAPI möglich! Setzen Sie die Kanalbündelung also nur dann ein, wenn die doppelte Übertragungsleistung auch tatsächlich ausgenutzt werden kann.

DE

6 Index

DE

DE

DE

DE