10/2010 MN05010009Z-DE
ersetzt M000191-04, 09/2007

Netzwerk in Kürze

Powering Business Worldwide

Impressum

Hersteller
Eaton Automation AG
Spinnereistrasse 8-14
CH-9008 St. Gallen
Schweiz
www.eaton-automation.com
www.eaton.com

Support
Region North America
Eaton Corporation
Electrical Sector
1111 Superior Ave.
Cleveland, OH 44114
United States
877-ETN-CARE (877-386-2273)
www.eaton.com

Andere Regionen
Bitte kontaktieren Sie Ihren lokalen Lieferanten oder senden Sie eine E-Mail an:
automation@eaton.com

Originalsprache
Deutsch

Redaktion
Manfred Hüppi

Marken- und Produktnamen
Alle in diesem Dokument erwähnten Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Titelinhaber.

Inhaltsverzeichnis

Inhaltsverzeichnis

1 Zweck dieses Dokuments

Dieses Dokument soll Hilfestellung bieten bei der Integration von Computern und Panels in Netzwerken. Es enthält Informationen:

- zu Netzwerken im Allgemeinen und
- zur Integration von Computern und Panels in Netzwerken.

2 Netzwerktopologie

2.1 Hub

Ein Hub ist ein Gerät, das als Verbindung zwischen verschiedenen Netzwerkteilnehmern eingesetzt wird. Alle Daten werden an alle (per Patch-Kabel) angeschlossenen Geräte weiterverteilt.

2.2 Switch

Switches sind Weiterentwicklungen von Hubs. Sie unterscheiden sich besonders durch ihr "Mitdenken", indem sie die Datenpackete möglichst gut verteilen. Mehrere Datenpakete können den Switch gleichzeitig passieren. Die Gesamtbandbreite (der Datendurchsatz) ist wesentlich höher als bei einem Hub. Switches lernen nach und nach, welche Stationen mit welchen Ports verbunden sind, somit werden bei weiteren Datenübertragungen keine anderen Anschlüsse unnötig belastet, sondern nur der Anschluss, an dem die Zielstation angeschlossen ist. Switches haben ausser dem höheren Preis durchwegs nur Vorteile gegenüber Hubs.

2.3 Router

Dieses Gerät dient dazu, Aufrufe innerhalb eines Netzwerks ins Internet (oder ein anderes Netzwerk) weiterzuleiten bzw. zu routen. Dabei kann man außerhalb des Intranets nicht feststellen, von welchem Computer im Intranet Daten angefordert wurden. Alle Computer im Intranet erscheinen im Internet unter der gleichen IP-Adresse.

2.4 Firewall

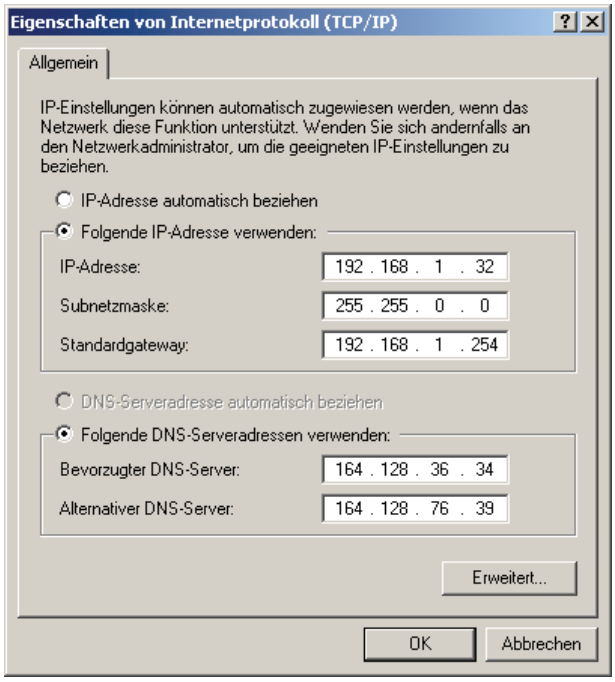
Eine Firewall dient dazu, Zugriffe auf IP-Adressen des Intranets von außen zu verhindern. Sie ist also ein Schutz der internen Daten. Bei entsprechender Konfiguration kann sie auch dazu genutzt werden, URLs durch Regeln oder Listen vom Aufruf auszuschließen, wenn sie z. B. nicht der Firmenethik entsprechen.

Hauptsächlich entscheidet eine Firewall an Hand der in einem Paket enthaltenen Informationen über Quell- und Ziel-IP-Adresse sowie Port, ob es passieren darf oder abgewiesen wird. Dadurch wird auch verhindert, dass Pakete, die gar nicht dafür bestimmt sind, das Netzwerk belasten und genauso wird verhindert, dass Pakete des Intranet in das Internet gelangen.

3 Einstellungen

3.1 Einführung

Folgendes Kapitel zeigt auf welche Netzwerkeinstellungen gemacht werden müssen, damit eine sinnvolle Kommunikation über Ethernet überhaupt möglich ist. Die Abbildung zeigt als Beispiel die Einstellungen unter Windows 2000. Unter anderen Betriebssystemen sehen die Eingabemasken ähnlich aus.



3.2 IP Adresse

Eine IP-Adresse ist 32 Bit (also 4 Byte) lang und dient zur eindeutigen Kennzeichnung von Netzen, Unternetzen und einzelnen Computern, die mit dem TCP/IP-Protokoll arbeiten.

Private Adressbereiche für lokale Netzwerke: (Intranet)
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Beispiele:
172.16.1.22
192.168.128.132

Öffentliche Adressen: (Internet)

Beispiele:
198.175.96.33 www.intel.com

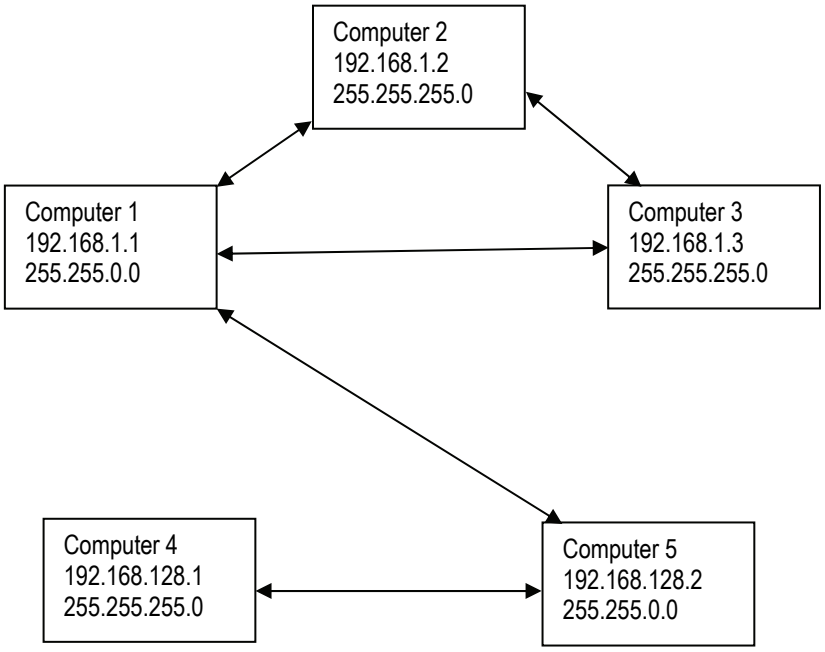
3.3 Subnetzmaske

Die Subnetzmaske ist ein IP-Address-"Filter". Sie ist aufgebaut wie eine IP-Adresse. Diese Maske definiert welche Computer miteinander innerhalb eines Netzes miteinander Daten austauschen können. Somit ist auch die maximale Grösse innerhalb eines Netzwerkes definiert.

Subnetzmaske	Anzahl Computer	Mögliche IP-Adressen
255.255.255.0	254	aaa.bbb.ccc.0 – aaa.bbb.ccc.255
255.255.0.0	65534	aaa.bbb.0.0 – aaa.bbb.255.255

Konfigurationsbeispiele:

Die Pfeile zeigen welche Computer miteinander kommunizieren können. Man beachte dass alle Computer physikalisch miteinander verbunden sind.



3.4 Gateway

Wenn zwei Computer, welche in verschiedenen Netzwerken liegen, miteinander kommunizieren wollen, müssen die Netzwerke durch einen Router verbunden werden. Zum Beispiel beim Surfen auf dem Internet muss das Datenpacket vom Internet zum Intranet und umgekehrt geroutet werden.

Anhand der Subnetzmaske weiss ein Computer, ob der Empfänger im gleichen Netzwerk zu suchen ist oder ob dieser ausserhalb liegt. Falls dieser ausserhalb liegt, sendet er das Datenpacket an den Router, der durch die IP-Adresse im Gateway- Eintrag spezifiziert wird.

3.5 DNS (Domain Name Server)

Wird in einem Browser oder FTP-Client eine Adresse wie www.intel.com eingegeben, kann der Computer gar nichts damit anfangen. Er muss zuerst jemanden fragen, welche IP-Adresse sich hinter diesem Namen verbirgt. Diese Information bekommt er von einem Domain Name Server. Jeder Internetprovider bietet diesen Dienst an.

Falls ein DNS ausfallen würde bieten die Provider meist einen zweiten DNS an.

Bei der DNS-Einträgen handelt es sich um die IP-Adressen dieser Server.

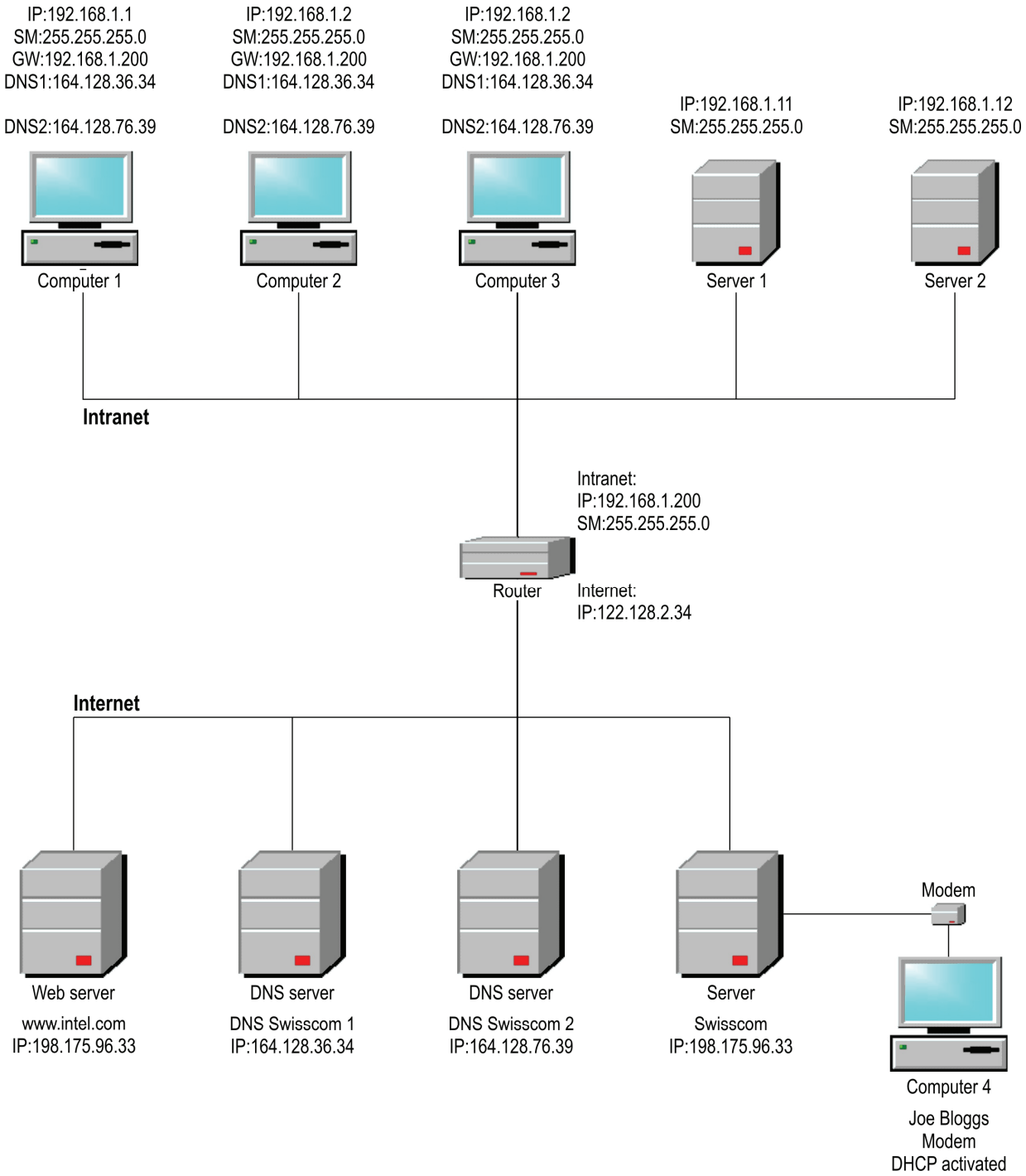
3.6 DHCP (IP-Adresse automatisch beziehen)

Falls man innerhalb eines Netzwerkes nicht jeden Computer konfigurieren möchte, und innerhalb des Netzwerkes ein DHCP-Server vorhanden ist, kann diese Einstellung aktiviert werden. Der Computer erhält dann die Informationen wie IP-Adresse, Subnetzmaske, Gateway und DNS vom DHCP-Server. Meist beherbergt der Router im Netzwerk auch noch einen DHCP-Server.

3.7 WINS

WINS ist die Abkürzung für Windows Internet Name Service. Dieser Dienst ist für die Namensauflösung im Intranet von Microsoft Netzwerken verantwortlich. Es muss jedoch ein WINS-Server existieren um diesen Dienst nutzen zu können. Ansonsten wird die Namensauflösung über Broadcasts und anderen Mechanismen ausgeführt.
Im WINS kann man die IP-Adresse einem festen Namen zuordnen lassen, so dass, wenn sich die IP ändert, der Computer trotzdem noch erkannt wird.

3.8 Beispiel eines Netzwerkes



4 Client Server Kommunikation

4.1 Port

Ein Port ist eine Art virtuelles Postfach für Datenpakete. Ein Computer kann auf 65536 verschiedenen Ports mit anderen Computern kommunizieren. Man kann sich das wie folgt vorstellen:

Wenn der Internet Explorer eine Webseite öffnen möchte, beantragt er vom Betriebsystem einen Port. Das Betriebsystem stellt ihm dann einen zur Verfügung z.B. Port 1000. Nun sendet der Internet Explorer ein Packet an den Webserver. Darin ist die Absender-IP-Adresse, der Absender-Port (Port 1000), die Empfänger-IP-Adress, der Empfängerport (für Webseiten standardmässig Port 80) sowie Nutzdaten (die Anfrage für eine bestimmte Webseite). Somit weiss, das Datenpacket wohin es gesendet werden muss. Der Webserver detektiert in seinem Port das Datenpacket, verarbeitet es und sendet eine Antwort an den Absender.

Jedes "wichtige" Protokoll hat einen allgemein bekannten Port. Die Portnummern von 1 bis 1024 sollten nur für bekannte Serverdienste verwendet werden.

Wichtige Portnummern:

Port-Nr.	Dienst	Beschreibung
20	FTP Data	Dateitransfer (Datentransfer vom Server zum Client)
21	FTP	Dateitransfer (Initiierung der Session und Senden der FTP-Steuerbefehle durch den Client)
23	Telnet	Terminalemulation
25	SMTP	E-Mail-Versand
80	HTTP	Webserver
110	POP3	Client-Zugriff für E-Mail-Server
143	IMAP	Zugriff und Verwaltung von Mailboxen
443	HTTPS	Verschlüsselte Webserver Übertragung, meist mit SSL- oder TLS-Verschlüsselung

4.2 Server

Als Server werden meistens Computer bezeichnet, welche in einem Netzwerk Dienste anbieten. Dies ist jedoch nicht ganz präzis. Server sind Applikationen in einem Computer, welche die Aufgabe haben Daten bereitzustellen oder Daten zu verarbeiten. Jeder Computer kann solche Dienste anbieten.

Ein Server ist von sich aus nicht aktiv. Er wartet, bis er von einem Client abgesprochen wird und verrichtet dann seine Aufgaben. Jede Serverapplikation bietet im Netzwerk seinen Dienst unter einem Port an.

Typische Server:

- Webserver Port 80
- FTP-Server Port 21
- Telnet-Server Port 23
- SMTP-Server Port 25
- POP-Server Port 110

4.3 Client

Als Client bezeichnet man eine Applikation, welche bestimmte Dienste von einem Server beansprucht.

Typische Clients:

- Internet Explorer
- WS-FTP
- Outlook

4.4 Peer to Peer (P2P)

Peer-to-Peer ist eine Bezeichnung für miteinander verbundene Computer mit der Voraussetzung, dass beide Computer die Rolle des Servers und des Clients übernehmen können. Berühmte P2P-Anwendungen sind Napster, Kazaa, eDonkey etc.

4.5 Client im Intranet – Server im Internet

Diese Zugriffsart ist für einen Internetuser der Normalfall.

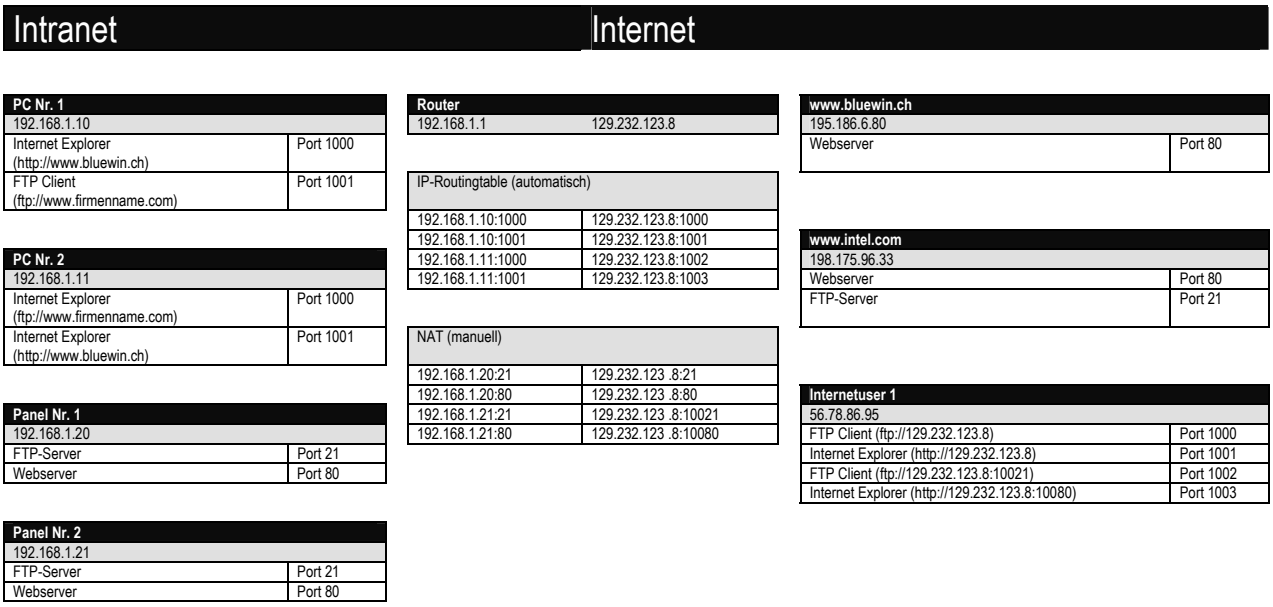
Beispiel: (siehe Kap. 4.7)
Der Benutzer Nr.2 mit der IP-Adresse 192.168.1.11 öffnet mit dem Internet Explorer eine Webseite. Das Betriebsystem teilt dem Internet Explorer den Port 1000 zu. Die Datenpackete werden danach zum Gateway beziehungsweise zum Router geschickt. Dieser macht automatisch in der Routing-Tabelle einen Eintrag wo er festhält, dass der User mit der IP-Adresse 192.168.1.11 und dem Port 1000 aufs Internet zugreifen möchte. Er erteilt diesem Eintrag eine neue Portnummer 1002. Der Router sendet das Datenpacket unter der neuen Absender IP-Adresse 129.232.123.8 Port 1002 weiter an den Webserver. Dieser verarbeitet die Anfrage und schickt dem Router eine Antwort zurück. Der Router sucht in der Routing-Tabelle die Portnummer 1002 und erhält die definitive IP-Adresse 192.168.1.11 Port 1000 des Benutzers Nr.2 zurück. Somit weiss der Router, wohin er das Datenpacket weiterleiten muss. Denn der Internet Explorer wartet schon sehnsüchtig in seinem Postfach Port 1000 auf eine Antwort.

4.6 Server im Intranet – Client im Internet

Beispiel: (siehe Kap. 4.7)
Der Internet Benutzer Nummer 1 möchte auf den FTP-Server eines Panel Nr. 1, welches im Intranet der Firma XYZ steht, zugreifen. Vom Internet aus ist die ganze Firma nur unter der IP-Adresse 129.232.123.8 sichtbar. Die IP-Adresse 192.168.1.20 des Panels würde für den Zugriff vom Internet aus keinen Sinn machen, weil es sich um eine private IP-Adresse handelt. Voller Zuversicht öffnet er mit einem FTP-Client die Verbindung 129.232.123.8 - leider ohne Erfolg. Der Router wusste nicht, was er mit dem Datenpacket überhaupt machen sollte. Der Netzwerkadministrator musste zuerst in der NAT des Routers manuell einen Eintrag machen, in dem dem Router mitgeteilt wird, dass wenn ein Datenpacket auf den Router Port 21 geschickt wird, dieses an die IP-Adresse 192.168.1.20 Port 21 weitergeleitet werden muss. Doch was ist, wenn ein zweites Panel im Intranet aufgestellt wird? Dieses kann ja nicht den selben Port auf dem Router belegen. Man ist dann gezwungen, einen neuen Port zu definieren, z.B. Port 10021. Beim Zugriff mit dem FTP-Client muss dann explizit die IP-Adresse 129.232.123.8 Port 10021 angegeben werden.

☞ **Nebst dem Router muss auch eine allfällige Firewall so konfiguriert werden, dass ein Zugriff von aussen überhaupt möglich ist. Fragen sie hierzu ihren Netzwerkadministrator.**

4.7 Beispiel



4.8 Statische oder dynamische IP-Adresse

Falls das Firmennetz eine Standleitung mit statischer IP-Adresse besitzt, ist der Zugriff von aussen auf das Intranet unproblematisch. Bei DSL Verbindungen wird teilweise dem Router mehrmals am Tag eine neue IP-Adresse zugewiesen. Ein Zugriff auf Server im Intranet ist nur möglich, wenn der Netzwerkadministrator dem Benutzer im Internet die aktuelle IP-Adresse mitteilt. Dies ist sehr umständlich. Es gibt jedoch die Möglichkeit, einen Dynamic Domain Name Server Dienst im Internet zu beanspruchen.

Wenn sie dazu mehr wissen möchten, besuchen sie die Webseite www.dyndns.org.

Es ist zu beachten, dass einige Provider bei Inaktivität der DSL-Verbindung diese trennen. Es ist dann unmöglich, das Firmennetz zu erreichen. Als Gegenmassnahme muss im Intranet eine Applikation die Internetverbindung aufrechterhalten, indem es dauernd Zugriffe auf das Internet macht. Teilweise können die Router so konfiguriert werden, dass diese die Verbindung aufrechterhalten.

Ist das Firmennetz über eine Einwählverbindung mit dem Internet verbunden, ist eine Verbindungsaufnahme fast unmöglich. Die Internetverbindung muss manuell aus dem Intranet aufgebaut werden.

5 Nützliche Befehle

Folgende Befehle können in der Eingabeaufforderung eines Windows-PC's oder teilweise auch unter Windows CE ausgeführt werden. Die Information, welche Befehle verfügbar sind, finden Sie in der Systembeschreibung des verwendeten Betriebsystems.

☞ **Es kann sein, dass folgende Befehle nur innerhalb des Intranets funktionieren, weil die Firewall in ihrem Firmennetzwerk solche Zugriffe aufs Internet nicht erlaubt. Fragen sie gegebenenfalls bei ihrem Netzwerkadministrator nach.**

5.1 PING

Durch den Befehl PING kann getestet werden, ob eine Netzwerkverbindung zu einem anderen Computer hergestellt werden kann.

Beispiele:
PING 192.168.1.1
PING www.intel.com

5.2 IPCONFIG

Mit den Befehl IPCONFIG erhält man die Netzwerkeinstellungen des eigenen Computers.

Beispiele:

IPCONFIG	Zeigt Informationen an.
IPCONFIG /all	Zeigt detaillierte Informationen an.

5.3 TRACERT

Mit dem Befehl TRACERT kann der Weg, der ein Datenpacket durchläuft angezeigt werden.

Beispiele:
TRACERT 192.168.1.1
TRACERT www.intel.com

5.4 NETSTAT

Zeigt Protokollstatistik und aktuelle TCP/IP-Netzwerkverbindungen an.

Beispiele:

`NETSTAT`	Zeigt den Status aller Client Verbindungen an.
`NETSTAT -a`	Zeigt den Status aller Verbindungen an.
`NETSTAT –n`	Zeigt Adressen und Portnummern numerisch an.