AUSGABE 1/06

SWITCHED

T.D.T.®
Transfer Data Test GmbH

CALLING ALEC
Security-Netze mit ALEC GmbH und T.D.T.-Routern

T.D.T.-Neuentwicklungen

Routerfamilie R52
fuer UMTS/EDGE/GPRS

Routerfamilie R450
fuer DSL/ISDN/PSTN

OEM WiFi
fuer serielle Daten

Multiservice Router M3000
die Routerplattform fuer Multiprotokolle

Standleitungsrouter R64SX
ersetzt teure Standleitungen

Editorial
Die Karawane zieht weiter

Hochverfuegbarkeits-netze
Die Seite 3

T.D.T.-Produkte
Alle Geraete - alle Features

T.D.T.-Online-Shop
fuer Produktzubehoer und Pocket Guides

Andreas Pahne, Geschaeftsfuehrer der ALEC GmbH

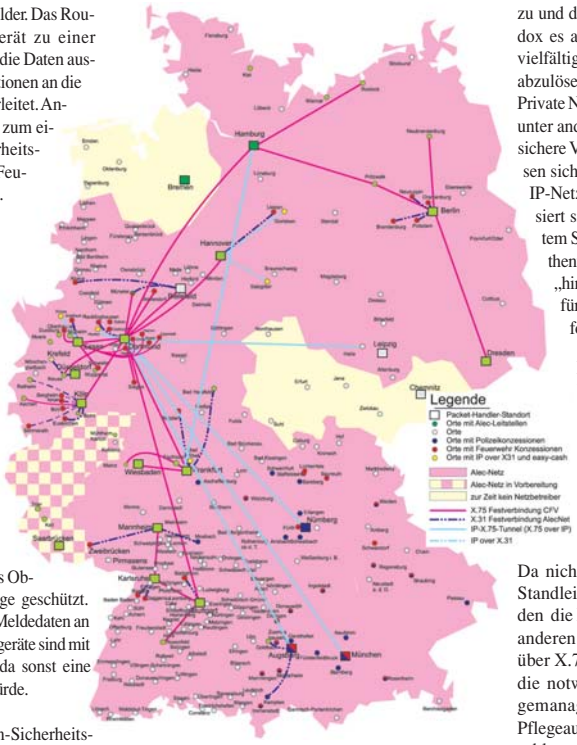
CALLING ALEC

Wenn Sicherheitsunternehmen nach einem schlüssigen Konzept zur Datenübermittlung suchen, ist die ALEC Sicherheitssysteme GmbH aus Dortmund erster Ansprechpartner. Denn erst die optimale Nutzung der einzelnen Komponenten gewährt ein sicheres und effektives Alarmmanagement. Ein besonderes Augenmerk legt das Dortmunder Unternehmen dabei auf die Migration neuer Übertragungsmöglichkeiten von der Gefahrenmeldestelle zu den Leitstellenzentralen und setzt dabei künftig auch auf IPSec. Wie nicht anders zu erwarten, holte Geschäftsführer Andreas Pahne mit T.D.T. einen bewährten Partner ins Boot, um den neuen Sicherheits-Standard für seine Netze nutzen zu können.

Sicherheitsunternehmen haben einen aufreibenden Job. Sie müssen für ihre Kunden Sicherheit rund um die Uhr und auf allen Ebenen gewährleisten. Das Spektrum der zu überwachenden Objekte erweitert sich ständig und die Anforderungen werden immer anspruchsvoller. Die ursprünglichen Alarmanlagen gegen Einbruch, Diebstahl, Überfall, Brände, Wasser usw. haben sich zu komplexen Meldeüberwachungsanlagen entwickelt. Dabei lassen sich die Aufgaben wie folgt definieren: Das Einrichten der Gefahrenmeldeanlage, zum Beispiel einer Brandmeldeanlage mit Rauch- oder Feuermelder. Das Routen der Meldedaten vom Meldegerät zu einer Empfangseinrichtung, die wiederum die Daten auswertet und alle notwendigen Informationen an die betreffende Leitstellenzentrale weiterleitet. Angebundene Leitstellenzentralen sind zum einen die Privaten Wach- und Sicherheitsunternehmen, aber auch Polizei und Feuerwehr-Leitstellen sind eingebunden.
Die Einstufung von Gefahrengruppen nimmt der Verband der Schadensversicherer (VdS) in die Stufen A, B und C vor. Die Kategorie C steht für die höchste Sicherheitsstufe und fordert zwingend die permanente Aufschaltung zu einer ständig besetzten Leitstelle. Hierbei muss für jeden Teilnehmer die Verfügbarkeit des Netzes mindestens alle 20 Sekunden geprüft werden. Unternehmen mit hohem Diebstahlrisiko, wie Banken oder Lebensmitteleinzelhandel, greifen auf die Möglichkeit, Gebäude und Waren über den stillen Alarm wirkungsvoll zu sichern, zurück. Jedes zu überwachendes Objekt ist mit einer Gefahrenmeldeanlage geschützt. Sensoren übermitteln dabei definierte Meldedaten an Übertragungsgeräte. Die Übertragungsgeräte sind mit einer Festverbindung aufgeschaltet, da sonst eine Sabotage nicht rechtzeitig bemerkt würde.

Die ALEC GmbH bietet das Rundum-Sicherheitspaket, das sich vom Übertragungsgerät über den Übertragungsweg und die Empfangseinrichtung erstreckt. Als Gesamtlöser und Carrier mit einem Festverbindungsnetz ist das Überwachen und die Fehlersuche ohne großen Aufwand durchzuführen. Die Leitungen sind überwiegend von der Telekom gemietet, auf deren Dienste man in absehbarer Zeit auch weiterhin setzen wird. Kann sie doch an allen Orten, an denen die Übertragungsgeräte und Empfangseinrichtungen stehen müssen oder werden, einen digitalen Telefonanschluss zur Verfügung stellen.

Im Zuge ganzheitlicher Lösungen von komplexen Aufgaben ist oft eine Kooperation zwischen mehreren Sicherheitsunternehmen, respektive Wach- und



Schließgesellschaften, erforderlich. Die ALEC GmbH koordiniert und legt großen Wert auf die Beratung aller beteiligter Unternehmen und unterstützt sie mit Schulungen und Hotlines. Dies gilt sowohl für die Errichter von Gefahrenmeldeanlagen als auch für die Installation von Leitsystemen.

Der ALEC-Datenhighway

Vom verwebten Datennetz zum Sternnetz durch IPSec. Seit mehr als 15 Jahren stützt sich ALEC GmbH auf das historisch gewachsene X.25-Netz. Es war lange Zeit das Nonplusultra bei der Übertragung hochsensibler Daten. Das Protokoll ist genormt, lässt eine Mehrfachnutzung der Anschlussleitungen zu und die Datenübertragung ist fehlerfrei. So paradox es auch klingt, gerade das Internet mit seinen vielfältigen Diensten schickt sich an, das X.25-Netz abzulösen. So setzt die Alec GmbH auf Virtuelle Private Netzwerke (VPN), um mit geringem Aufwand unter anderem teure Standleitungen durch zukunftssichere VPNs zu ersetzen. IPSec-gestützte VPNs lassen sich kostengünstig betreiben, da sie öffentliche IP-Netze als Verkehrsweg nutzen. IPSec kristallisiert sich als neuer De-facto-Standard mit höchstem Sicherheitsstandard für VPNs heraus. Die Authentifizierung erfolgt über Pre Shared Keys oder „hinterlegten" Zertifikaten, wie vom Bundesamt für Sicherheit in der Informationstechnik empfohlen (www.bsi.de).

Die bisherige Netzstruktur

Um eine „stehende Verbindung" von der zu überwachenden Außenstelle zu einem der 21 Packet-Handler in Deutschland gewährleisten zu können, ist jedes Übertragungsgerät mit einer ISDN-Leitung verbunden. Die geforderten Signaldaten werden über den D-Kanal der ISDN-Leitung (X.31) zu einem Packet-Handler übertragen.
Da nicht jeder Packet-Handler mit einer teuren Standleitung an Dortmund angebunden ist, werden die Daten oft von einem Packet-Handler zum anderen gereicht. Diese Kommunikation findet über X.75 statt. Das bedeutet auch, dass bei allen die notwendige Technik vor Ort installiert und gemanagt werden muss. Der Investitions- und Pflegeaufwand für Hardware, Service und Routing schlugen enorm zu Buche. Ebenso kostenintensiv ist die Anbindung einzelner Stützpunkte mittels teurer Standleitungen, zu denen es erst seit kurzem mit IPSec eine echte Alternative gibt.

Die neue Netzstruktur
Durch IPSec und den T.D.T.-Routern, die dieses Verfahren unterstützen, lassen sich sowohl Administration und Aufwand für die Hardware bei den Packet-Handlern und bei der Datenübertragung nach Dortmund erheblich reduzieren.
An den Standorten setzt ALEC künftig die T.D.T.-Router R525 mit der X.75-Schnittstelle ein. Das günstige Einstiegsgerät tunnelt die X.75-Daten des Packet Handlers transparent mit IPSec. Durch diese „Verlängerung der Leitung" kommen die Daten von den Paket Handlern über IPSec in Dortmund an. In der Zentrale übernehmen die Vermittlungsrechner, zur Zeit die bewährten DCC System3, die Daten. Durch diese smarte Lösung wird der Nachteil von XoT gekonnt umgangen. Im Gegensatz zu XoT, wo nur die oberen Schichten übertragen werden, reicht X.75 auch die Layer 2-Daten durch, die für die Leitungsüberwachung zwingend notwendig sind. Denn nur dann kann die Zentrale einen Leitungsausfall diagnostizieren.
Als Backup wird ISDN in derselben Form verwendet: X.75 over ISDN, also die transparente Datenübertragung mit Übertragung ab Schicht 2. Kommt es zu einem Ausfall der Internetschiene, nutzen die Router die vorhandene ISDN-Leitung. Nach einem Aufbau der Verbindung bleibt das Gerät solange in Betrieb, bis das Internet wieder funktioniert. Parallel zur ISDN-Übertragung wird dazu ständig am Aufbau des IPSec-Tunnels gearbeitet und die Leitung getestet. Sobald der Router eine sichere Verbindung erkennt, schaltet er zur IPSec-Variante zurück.

Die Dortmunder Zentrale
Die ALEC GmbH wäre nicht so erfolgreich, wenn das Unternehmen nicht schon immer Sonderlösungen konzipiert und gefordert hätte. Mit T.D.T. steht seit Beginn ein Partner zur Seite, der die Konzepte mit der technischen Umsetzung in den T.D.T.-Geräten ermöglichte. So entwickelte die niederbayerische EDV-Schmiede die Transparentkarte für den DCC System3. In Verbindung mit einem IP-Gateway kann der DCC3 die transparenten Daten in X.75 auflösen und bedienen. Entscheidender Vorteil der Transparentkarten: Sie ermöglichen die gleichzeitige Nutzung von über 1.000 logischen Kanälen. Diese Zahl ist unbedingt erforderlich, da zwar das Datenaufkommen gering ist, die Daten jedoch parallel verarbeitet werden müssen, da auf einer IPSec-Verbindung mehrere tausend Verbindungen bestehen können. Für die zeitnahe Verarbeitung der Alarme setzt ALEC GmbH auf ein spezifisches Betriebssystem.
Zum Sicherheitskonzept gehört es, dass jedes Gerät eine logische Verbindung zu seinem Hilfeleister aufbaut. Um Datennetze zu überwachen, bedarf es eines ausgeklügelten Netzwerkmanagement-Systems. Hier stand der T.D.T.-NetMacs Pate. Ein eigenes Programm wurde dazu geschrieben, das auf die speziellen Sicherheitsbedürfnisse abgestimmt ist. So interessiert zum Beispiel die Statistik nicht, während es unabdingbar ist, Linkdown und Linkup der Leitungen zu überwachen und zeitnah zu bearbeiten.

Der T.D.T-Router G5000
Durch die Umstellung auf IPSec werden sukzessive die DCC System3-Geräte in den Außenstellen und in der Zentrale durch Router ersetzt. Das neue T.D.T.-Paradepferd, der G5000, übernimmt die Auflösung der IPSec-Verbindungen , die über IP bzw. ISDN eintreffen. Im Falle eines Backups löst er die ISDN-Daten in IP-Daten auf und reicht sie zu den angeschlossenen Rechnern durch. Somit stehen die Daten der Packet Handler immer auf Ethernet zur Verfügung.
Zusätzliche unabhängige Verwaltungsfunktionen stehen im G5000 über eine sichere, webbasierte Schnittstelle (SSL) bereit. Darüber hinaus sind eine Vielzahl von erweiterten Verwaltungs- und Berichtsfunktionen integriert. Das System arbeitet auf Basis einer T.D.T.-eigenen Linux-Distribution und bietet alle damit gebundenen Features, einschließlich eines leistungsfähigen Firewallings mit Net-Filter. Die Sicherheit der Daten geht ebenso einher mit der Architektur des Backup-Standortes. Durch die neue Struktur ist der Backup-Standort identisch mit der Dortmunder Zentrale. So macht es keinen Unterschied, über welchen Übertragungsweg die Daten in der Zentrale oder im Backup-Standort ankommen, da die Daten die gleiche Struktur aufweisen. Ein geschickter Schachzug, zumal damit auch ein effektiver Beitrag zur Minimierung der Administrationsaufgaben gelingt.

„Wir designen unsere Übertragungsgeräte - und nach Fertigstellung durch einen Partner wird die Software dazu geschrieben. Denn nur Software, die man selbst schreibt, hat man unter Kontrolle." (A. Pahne)

Höhere Unternehmens-Flexibilität durch IPSec
Musste bisher bei jeder Neuinstallation bzw. Erweiterung des Netzes entschieden werden, in welche Konten sinnvoll geroutet wird, damit die Daten dann über eine Standleitung die Zentrale erreichen - ist dies durch die IPSec-Stern-Übertragung nicht mehr relevant. Durch IP wird es für die ALEC GmbH wesentlich einfacher, neue Standorte zu erschließen und blitzschnell zu reagieren. Zwar hat sich die Telekom immer bemüht, Leitungen schnellstmöglich zur Verfügung zu stellen, doch vom Antrag bis zur Freischaltung sind einige Tage einzurechnen. Ein Nachteil, den es durch die künftige IP-Übertragung nicht mehr geben wird. Sobald die Geräte installiert sind, ist auch die Datenübertragung gewährleistet.

Kostenreduzierung
Die Einsparmöglichkeiten sind enorm, da der DSL-Anschluss, und damit die monatlichen Gebühren für den Anschluss künftig wesentlich geringer sind, als dies bei einer Festverbindung der Fall ist. In der Zentrale reicht ein symmetrischer Interconnect-Anschluss der Telekom. Die für die Aufgabe zugeschnittenen R525 Router in den „Außenstellen" sind eine äußerst kostengünstige Lösung gegenüber der bisherigen Ausstattung.

Ausblick
Bisher ließen sich bei der Ausweitung der Dienste Insellösungen und ein vermehrter Routing-Aufwand nicht vermeiden. Durch die neue Strategie kann die ALEC GmbH die lange gewünschte Sterntopologie in Anspruch nehmen. Denn die Aufrüstung von einundzwanzig R525 Routern ist als Investitionssumme immer noch erheblich günstiger als die Erweiterung der Standleitungen. Der Großteil der Einsparung wird jedoch in der günstigen Datenübertragung liegen. „Der Wegfall der Kosten für die Standleitung ermöglicht uns, Kapital für neue Entwicklung freizusetzen", so A. Pahne. „T.D.T. zeichnet es aus, dass sie genau die Geräte anbieten, bzw. so konfigurieren, dass sie für die beschriebene Lösungen exakt abgestimmt sind. Keine überdimensionierte Geräte, sondern auf das Bit programmierte Features."

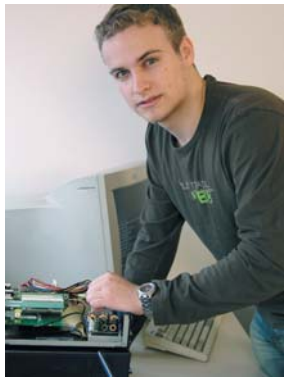
Die sukzessive Umstellung auf IPSec wird mit einer großen Gelassenheit in Angriff genommen, zumal mit T.D.T. ein Partner zur Verfügung steht, der die Migration von X.75 in IP perfekt beherrscht.

Ansprechpartner: Andreas Pahne
ALEC Sicherheitssysteme GmbH
Friedrich-Hölscher-Straße 367, 44328 Dortmund
Tel. 0231 92370-0, Fax 92370-10
eMail: alec.gmbh@t-online.de

EDITORIAL

T.D.T.-Linux-Distribution ist das Ergebnis eines konsequenten Weges!

Und die Karawane zieht weiter! Diese noch im Ohr klingende politische Aussage trifft auch auf die veränderte Situation in der Datenkommunikation zu. Mit IPSec hat das Internet endgültig Einzug in Bereiche erhalten, die lange Zeit eine Bastion der hinlänglich bekannten konventionellen Netze war. T.D.T. ist nun an der Spitze der Karawane und migriert alle bekannten Protokolle mit den Internetdiensten.



Wie stark dieses Investment forciert wird, lesen Sie auf Seite vier.
Um möglichst unabhängig von Herstellern bzw. von Betriebssystemen zu sein, setzen wir bei der Softwareentwicklung auf Linux. Dabei greifen wir zum Teil auf erprobte Linux-Pakete zurück und entwickeln spezielle Features für die T.D.T.-Geräte.
Mit dieser Schlüsseltechnologie sind wir in der Lage, spezielle Anforderungen für Sie zu schreiben. Dabei sind Sie und wir unabhängig von der Vertriebspolitik der großen Softwareunternehmen. Sicherlich ein zusätzlicher Grund, warum Sie sich für T.D.T.-Leistungen entscheiden sollten.

Ihr Martin Schiller, Dipl.-Inf. (FH)
Entwicklung und Progammierung

Aktuelle T.D.T.-Produktpalette

Mit den aktuellen T.D.T-.Geräten und Dienstleistungen stehen unseren Geschäftspartnern alle Optionen offen: Ob Datenübermittlung über private oder öffentliche Netze, ob LAN- und WAN-Verbindungen, ob Datentransfer via Internet durch VPN/IPSec-Router oder ob Speziallösungen zur Migration (z.B. X.25) der bisherigen Lösungen mit neuen Komponenten. Wir haben für jede Anforderung die richtige Lösung und erstellen auf Wunsch das effiziente Gesamtkonzept, einschließlich der Betreuung Ihres Netzes.

Transfer Data Test GmbH

	10/100BaseT	1000BaseT	ISDN BRI	ISDN PRI	GSM	GPRS	EDGE	UMTS	Analog Modem (PSTN)	UR2 (DSL-Modem)	X.21	X.21bis (V.24)	V.35	V.36	G.703	RS485	USB 2.0 Port	TCP/IP	Frame Relay	PPP	PPPoE	X.25	X.31	V.110/X.75	Asynchron	AMP	V.120	1Wire Bus (MicroLAN)	TCP/IP over X.25 (ToX)	X.25 over TCP/IP (XoT)	X.25PAD (X.3/X.28/X.29)	IP-X.25 Gateway	VPN	Pre Shared Keys	Zertifikate	DES/3DES/AES	SSL/SSH	SNMP	RIP V1, V2c	VRRP	Statefull Inspection FW	DHCP	NAT	PAP/CHAP	DDNS Client	Quality of Service	Web-Interface	Command Line Interface
G5000	●	●	●	●	-	-	-	-	●	●	●	●	●	●	●	-	4		●	●	●	●	●	●	●	-	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
M3000	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	4		●	●	●	●	●	●	●	-	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R421	1	-	1	-	-	-	-	-	-	-	⊙	●	-	-	-	-	-		●	-	●	●	●	●	●	-	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R450	4	-	-	-	-	-	-	-	●	●	⊙	●	-	-	-	-	-		●	-	●	●	●	●	●	-	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R450p	4	-	-	-	-	-	-	-	●	●	⊙	●	-	-	-	-	-		●	-	●	●	●	●	●	-	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R450i	4	-	1	-	-	-	-	-	●	●	⊙	●	-	-	-	-	-		●	-	●	●	●	●	●	-	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R526i	4	-	1	-	-	-	-	-	-	-	⊙	●	-	-	-	-	2		●	-	●	●	●	●	●	-	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R526ie	4	-	1	-	●	●	●	-	-	-	⊙	●	-	-	-	-	2		●	-	●	●	●	●	●	-	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R526pe	4	-	-	-	●	●	●	-	●	-	⊙	●	-	-	-	-	2		●	-	●	●	●	●	●	-	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R52	1	-	-	-	●	●	-	-	-	-	⊙	●	-	-	-	-	2		●	-	●	●	●	-	-	●	-	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R52e	1	-	-	-	●	●	●	-	-	-	⊙	●	-	-	-	-	2		●	-	●	●	●	-	-	●	-	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R52u	1	-	-	-	●	●	●	●	-	-	⊙	●	-	-	-	-	2		●	-	●	●	●	-	-	●	-	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
R626	5	-	1	-	⊙	⊙	⊙	-	⊙	●	-	●	-	-	-	-	-		●	-	●	●	●	●	●	●	●	-		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
TA ALPHA	-	-	1	-	-	-	-	-	-	-	-	1	-	-	-	1	-		●	-	●	-	●	●	-	●	●	-	-	●	●	●	●	●	-	-	-	-	-	❶	-	-	-	-	●	●	-	-	-	●
TA DELTA	-	-	1	-	-	-	-	-	-	-	-	2	-	-	-	1	-		●	-	●	-	●	●	-	●	●	-	-	●	●	●	●	●	-	-	-	-	-	❶	-	-	-	-	●	●	-	-	-	●
TA SIGMA	-	-	1	-	-	-	-	-	-	-	1	1	-	1	-	-	-		●	-	●	-	●	●	-	●	●	-	-	●	●	●	●	●	-	-	-	-	-	❶	-	-	-	-	●	●	-	-	-	●
TA OMEGA	-	-	2	-	●	-	-	-	-	-	4	4	-	4	-	-	-		●	-	●	-	●	●	-	●	●	-	-	●	●	●	●	●	-	-	-	-	-	❶	-	-	-	-	●	●	-	-	-	●
TA MICRO	-	-	1	-	-	-	-	-	-	-	-	1	-	-	-	-	-		●	-	●	-	●	●	-	●	●	-	-	●	●	●	●	●	-	-	-	-	-	❶	-	-	-	-	●	●	-	-	-	●
ALPHA Com$_{sync}$	1	-	-	-	-	-	-	-	-	-	1	1	-	1	-	-	-		●	-	●	●	●	-	-	-	-	-	-	●	●	-	●	●	-	-	-	-	-	❶	-	-	-	●	●	●	-	-	-	●
ALPHA Com$_{async}$	1	-	-	-	-	-	-	-	-	-	1	1	-	1	-	1	-		●	-	●	●	●	-	-	●	●	-	-	-	-	●	-	-	-	-	-	-	-	❶	-	-	-	●	●	●	-	-	-	●

⊙ Optional ❶ In Verbindung mit NetMACS und SPA

Hochverfügbarkeits-Netze

Redundanz mittels VRRP

Ausfallsicheres Netzdesign

Modernisierungen von vorhandenen IT-Infrastrukturen erfordern meist die redundante Auslegung kritischer Komponenten, um einen störungsfreien Betrieb zu garantieren.
Das dynamische Routing von Datenpaketen in Netzwerken wirkt in der Regel dem Ausfall von Teilstrecken durch Nutzung von alternativen Routen entgegen. Fällt jedoch der erste Router einer Strecke aus, so ist dieser Fehler nicht durch dynamisches Routing zu beheben, da ein Host im Normalfall nur ein statisches Standardgateway nutzt.

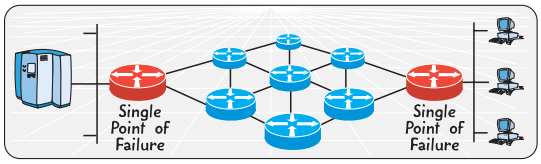


Abb. 1: Dynamisches Routing und Single Point of Failure.

Sogenannte „Single Points of Failure", wie in Abb. 1 ein Gateway, können bei einem Ausfall einer einzigen Hardwarekomponente komplette Netzwerke zum Erliegen bringen und diese unbrauchbar machen. Der finanzielle Schaden eines Ausfalles liegt meist in keinerlei Relation zu den Anschaffungskosten einer zweiten Hardware, die im Fehlerfall die Aufgaben der fehlerhaften Komponente übernimmt. Das Umschalten auf das Reserve-System macht jedoch nur Sinn, wenn dies zeitnah und völlig automatisch, das heißt ohne Eingriff von außen - und für das Netzwerk unbemerkt - vollzogen wird.

Eine Möglichkeit zum Aufbau eines solchen Hochverfügbarkeits-Netzwerks bietet das Virtual Router Redundancy Protocol (RFC 3768), kurz VRRP. Mittels VRRP wird der „Single Point of Failure" im Fehlerfall völlig automatisch auf die gespiegelte Hardware umgeschaltet.

Aufbau einer VRRP-Gruppe

Eine logische VRRP-Gruppe besteht immer aus einem VRRP-Master und einem oder mehreren VRRP-Slaves, die sich im gleichen Subnet befinden. Diese VRRP-Gruppe stellt sich für die Hosts als ein virtueller Router mit einer oder mehreren virtuellen IP-Adressen dar. Im Störungsfall bemerkt der Host den Ausfall des VRRP-Masters nicht, da zwar alle Funktionen vom VRRP-Slave übernommen werden, sich dieser jedoch im Netzwerk als der virtuelle Router darstellt. Für die Hosts ist es somit völlig untransparent, über welche Hardware sie kommunizieren, da immer nur der virtuelle Router angesprochen wird.

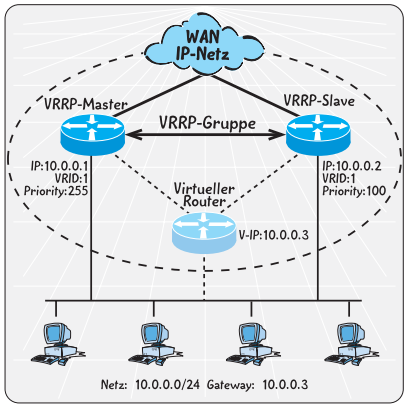


Abb. 2: Einfacher Aufbau einer VRRP-Gruppe.

Im praktischen Betrieb kommt dieser Aufbau jedoch selten vor, da der VRRP Slave im störungsfreien Betrieb keinerlei Funktion übernimmt und somit auch eine Fehlfunktion des Slaves eventuell nicht bemerkt werden würde. Eine einfache VRRP-Gruppe wird meist so aufgebaut, dass der VRRP-Master der Gruppe 1 gleichzeitig der Slave der Gruppe 2 ist und umgekehrt.
Daraus ergibt sich der Vorteil, dass die angeschlossenen Clients so konfiguriert werden können, dass der erste Teil der Clients als Standard-Gateway den Master der Gruppe 1 benutzt und der zweite Teil der Clients den Master der Gruppe 2. Somit ist es möglich, eine statische Lastverteilung (Load Balancing) über zwei VRRP-Router zu realisieren.

VRRP-Ablauf des Masters

Im störungsfreien Betrieb übernimmt der VRRP-Master die virtuellen IP-Adressen der Gruppe und weist diesen eine virtuelle Ethernet-Adresse zu, die sich wie folgt zusammensetzt: Die ersten 3 Oktetts (00-00-5E) stehen für die IANA OUI (Internet Assigned Numbers Authority, Organisation Unique Identifier). Die nächsten zwei Oktetts (00–01) kennzeichnen das VRRP-Protokoll. Das letzte Oktett wird mit der VRID (Virtual Router Identifier) dargestellt.

Der VRRP-Master sendet nach jedem Ablauf des Advertisement-Intervalles ein VRRP-Advertisement an die Multicast-Adresse 224.0.0.18, um der Gruppe seine ordnungsgemäße Funktion zu bestätigen.

VRRP-Ablauf des Slaves

Da das VRRP-Protokoll nicht vorsieht, dass ein Slave aktiv an der Kommunikation der Gruppe teilnimmt, weiß der Slave nach seiner Initialisierung weder ob der Master der Gruppe aktiv ist, noch seine Stellung innerhalb der Prioritätenliste.
Der Slave wartet aus diesen Gründen nach seiner Initialisierung ab, bis sein „Master Down Timer" abläuft. Dieser berechnet sich wie folgt:

*Master Down Timer = (3*Advertisement Interval) + Skew Time*
Skew Time = (256-Priority)/256

Empfängt nun der Slave innerhalb des Master Down Timers ein gültiges Advertisement, weiß er, dass der Master aktiv ist und wartet auf das nächste Advertisement innerhalb des neu gestarteten Master Down Timers .

Läuft der Master Down Timer aus, ohne dass der Slave ein gültiges Advertisement erhält, muss der Slave den Ausfall des Masters annehmen. Da der Slave mit der höchsten Priorität den Master Down-Zustand als erster erkennt, geht er in den Master-Zustand über und sendet die VRRP-Advertisements. Damit teilt er den anderen Routern mit, dass er jetzt die Funktion des Master-Routers übernommen hat.

Sollte das neue VRRP-Advertisement nicht rechtzeitig, d.h. vor dem Ablauf des Master Down Timers, bei eventuell anderen vorhandenen Slaves eintreffen, würden diese ebenfalls ein VRRP-Advertisement senden. Falls zwei oder mehr Backup-Router gleichzeitig ein VRRP-Advertisement senden, in dem sie sich als neuer Master-Router melden, wird der Slave mit der höchsten Priorität zum Master.
Der neue VRRP-Master übernimmt nun die Funktionalität, indem er die virtuellen IP-Adressen im Netzwerk bereitstellt. Nimmt der VRRP-Master mit der Priorität 255 (Adress Owner) seinen Betrieb wieder auf, sendet er automatisch ein Advertisement, in dem er sich wieder als der Master bekannt macht. Hat der ausgefallene Master eine Priorität kleiner 255, geht er in den Slave Modus bis er ein Advertisment erhält, das eine geringere Priorität hat als seine eigene. In diesem Fall gibt er sich als Master zu erkennen, indem er ein Advertisement an die VRRP-Gruppe sendet.

Das Layer 3-Protokoll: VRRP (RFC 3768)

In der für VRRP vorgesehenen RFC wird festgelegt, dass im regulären Betrieb nur der VRRP-Master VRRP-Pakete versendet. Dazu sendet der VRRP-Master in bestimmten Intervallen, den Advertisement Intervallen, VRRP-Advertisements an die für VRRP reservierte Multicast-Adresse 224.0.0.18.

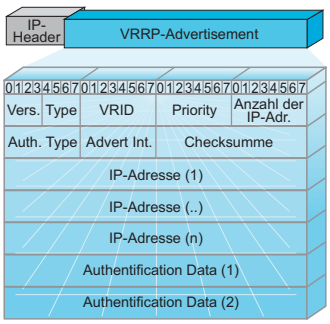


Abb. 3: Aufbau eines VRRP-Advertisements.

Die Verwendung der Multicast-Adresse bewirkt, dass alle Geräte, die physikalisch mit der Ethernet-Schnittstelle (Layer1) des VRRP-Masters verbunden sind, das Advertisement erhalten, egal in welchem Subnet sie sich befinden.

IP-Header

- **Quelladresse:** Die physikalische IP-Adresse des VRRP-Routers, der das Advertisement versendet.
- **Zieladresse**: Ein VRRP-Advertisement wird immer an die Multicast-Adresse 224.0.0.18 gesendet.
- **Time to Live:** Bei einem VRRP-Advertisement muss die TTL immer auf 255 gesetzt werden. Erhält ein VRRP-Router ein TTL kleiner 255 wird davon ausgegangen, dass das Paket bereits über einen anderen Router geroutet wurde, der den TTL um 1 verringert hat, und wird deshalb verworfen.
- **Protokoll-Nummer:** Die IP-Protokoll-Nummer für VRRP ist von der IANA (Internet Assigned Numbers Authority) auf 112 festgesetzt worden.

VRRP-Advertisement

- **Version:** Dieser Wert ist für die Versionsangabe reserviert. Derzeit ist nur die Version zwei gültig.
- **Type:** Dieser Wert ist für den Type reserviert. Derzeit ist nur der Type eins (Advertisement-Paket) erlaubt. Pakete mit einem anderen Type als eins werden verworfen.
- **VRID:** Der Virtual Router Identifier-Wert weist den Router der entsprechenden Gruppe zu. Alle Router einer Gruppe müssen den gleichen Wert zugewiesen haben, da ansonsten das Advertisement-Paket verworfen wird. Der mögliche Wertebereich beträgt 0 bis 255.
- **Priority:** Der Wert legt die Priorität eines VRRP-Routers innerhalb seiner Gruppe fest. Der Wert für die VRRP-Slaves ist standardmäßig auf 100 festgelegt, kann aber im Wertebereich von 1-254 an das vorhandene Netzwerk angepasst werden. Ein VRRP-Master mit der Priority 255 ist der Adress Owner der virtuellen IP-Adresse und versendet, anders als ein Master mit einer Priorität kleiner 255, direkt nach der Initialisierung VRRP-Advertisements. Wenn eine Priority gleichzeitig an mehrere Slaves vergeben ist, wird die Priorität anhand der IP-Adresse der betroffenen Slaves festgelegt. In diesem Falle gilt: je höher die IP-Adresse, desto höher die Gewichtung.
  Der Priority-Wert wird in die Berechnung des „Master Down Timer" miteinbezogen, um zu ermöglichen, dass der VRRP-Router mit der höchsten Priorität den Ausfall des VRRP-Masters am schnellsten bemerkt und darauf reagieren kann.
- **Anzahl der IP-Adresse(n):** Dieser Wert gibt die Anzahl der verwalteten virtuellen IP-Adressen der VRRP-Gruppe an.
- **Authentification Type:** Dieser Wert bestimmt die Authentifizierungsmethode für das gesendete Advertisement-Paket. Folgende Werte sind möglich:
  0 = Keine Authentifizierung
  1 = Einfaches Text-Passwort mit max. 8 Stellen
  2 = IP Authentification Header (HMAC-MD5)
- **Advertisement Intervall:** Dieser Wert legt die Zeitabstände fest, in welchen VRRP Advertisements verschickt werden. Standardmäßig beträgt der Wert 1 Sekunde. Das Advertisement Intervall muss für alle Router in der VRRP-Gruppe den gleichen Wert haben, da es sonst unterschiedliche Empfangs- bzw. Sendezeiten erwarten würde, was zu einem instabilen Verhalten der VRRP-Gruppe führen würde.
- **Checksumme:** Prüfsumme zur Sicherstellung der korrekten Übertragung des Advertisements.
- **IP-Adresse(n):** Virtuelle IP-Adresse(n), die der VRRP-Gruppe zugeordnet sind. Die Anzahl der Adressen wird im Feld „Anzahl der IP-Adressen" festgelegt.
- **Authentification Data:** Das Authentification Data-Feld wird derzeit lediglich für die Übertragung eines Passwortes im Klartext verwendet (Auth. Type 1). Das Feld darf maximal 8 Zeichen enthalten. Ist der konfigurierte Authentifizierungsstring dabei kürzer als 8 Zeichen, wird der verbleibende Platz mit Nullen aufgefüllt. Jedes ankommende VRRP-Paket, bei dem der Authentifizierungsstring nicht mit dem lokal konfigurierten übereinstimmt, wird verworfen.

Quellen:

Ayikudy Srikanth, Adnan Adam Onart „VRRP: Increasing Reliability and Failover with the Virtual Router Redundancy Protocol", Okt. 2002, ISBN 0-2017-1500-7

Carsten Harnisch, „Routing&Switching", Jul.2005, ISBN 3-8266-9370-1

http://www.ietf.org/rfc/rfc3768.txt

T.D.T.-Neuentwicklungen

UMTS/EDGE/GPRS/ Routerfamilie R52

Mit der **R52** Mobile Router- Familie reagiert T.D.T. auf die Forderung nach flexibler Standortwahl für die Anbindung verschiedenster Datenendgeräte.
Mit dem Übertragungsstandard UMTS und dem **R52u** lassen sich Datenverbindungen mit bis zu 384 KBit/s erreichen. Mit dem neuen Übertragungsstandard HSDPA werden sogar Datenraten von bis zu 1,8 MBit/s erreicht. Außerhalb des UMTS- Versorgungsbereichs schaltet der **R52u** automatisch auf EDGE bzw. GPRS um.
Das Multislot Class 6 EDGE Modem im **R52e** ermöglicht eine ca. dreimal höhere Übertragungsrate als das GPRS Class 10 Modem. So steigt die Geschwindigkeit, im Vergleich zu GPRS, von 42,8 kbps im Upstream auf 118,4 kbps und von 85,6 kbps im Downstream auf 177,6 kbps.
Der R52 GPRS Router erlaubt mobile Datenübertragungsraten von 85,6 kbps im Downstream und 42,8 kbps im Upstream.
Der **R52** bietet mehr CPU-Leistung, mehr Speicher und erreicht schnellere Verbindungsraten als sein Vorgänger. Zudem wurden die User Ports um zwei USB 2.0 Ports erweitert, die z.B für Backup, Authentifizierung oder Anschluss eines ADSL-Modems genutzt werden können.
Datenübertragung via UMTS/EDGE/GPRS ermöglicht mehr Flexibilität bei der Standortwahl und senkt die Kosten beim Betrieb an Drittplatzstandorten oder bei mobilen Anwendungen.

Verfügbare Hardware:

- 1 x **UMTS / EDGE / GPRS Modem** (je nach Typ) 2 SIM Slots für Provider Backup
- 1 x **10/100BaseT Ethernet** Autosense
- 1 x **synchroner/asynchroner Port** X.21bis (V.24) oder X.21
- 1 x **asynchroner Expansions Port** Dallas 1-Wire, GPS Empfänger
- 2 x **USB 2.0 Ports** z. B. für Authentifizierung, Backup oder serielle Ports
- 1 x **GPS Receiver** (optional) z. B. für Flottenmanagement

Die Leistungsbandbreite und das robuste Gehäuse des **R52** erleichtern den Anwendern die zügige Realisierung neuer Applikationen in Bereichen wie Telemetrie und Telematik.
Mit dem integrierten BASIC-Interpreter erstellen Sie in kürzester Zeit und in einer komfortablen Entwicklungsumgebung eigene Anwendungen (Messwerterfassung, Schwellwert-Abfragen, Ein-/Ausschalten, komplexe Monitoring-Applikationen etc.). Der BASIC-Interpreter und Pre-Compiler stellen einen weiten Bereich an String, Numeric und IP-Handling Features zur Verfügung. Hohe Benutzerfreundlichkeit und Zuverlässigkeit sind weitere Ausstattungsmerkmale des **R52**. Für eine schnelle und einfache betriebssystemunabhängige Inbetriebnahme sorgt die Konfiguration via integriertem Web-Browser oder Telnet.

OEM WiFi seriell Modul

Mit dem WiFi to seriell Modul werden serielle Daten wie RS232 oder RS485 über ein IEE 802.g Wireless-Netzwerk transparent getunnelt. Der Anwender spricht die serielle Schnittstelle über einen virtuellen COM-Port, über das TCP/IP-Protokoll, wie bei einer Kabelverbindung an. Das WiFi to seriell Modul ermöglicht eine drahtlose Kommunikation mit bis zu 300 m Reichweite und einer Übertragungsrate von bis zu 460.8 Kbps.

Durch die geringe Abmessung von 70 mm x 35 mm x 8 mm und dem weiten Spannungsbereich von 2,4–15 Volt ist das OEM-Modul leicht in bestehende Layouts einzudesignen.

Das Modul ist für verschiedenste Geräte, wie Barcode Scanner, POS-Systeme, TK-Anlagen und in anderen seriellen Geräten verwendbar.
Technische Daten:
RS-432, Tx, Rx, RTS, CTS
RS-485: Data in, Data out
RS-422: Data in+, Data in-, Data out+, Data out-

DSL/ISDN/PSTN/ Routerfamilie R450

T.D.T. offeriert mit der neuen R450-Familie eine DSL/ISDN/Analog Router-Serie mit voll implementierter VPN IPSec Suite. Zudem erlaubt der Router die Anbindung von X.25-Endgeräten.
Konzipiert wurde der Router speziell für den Einsatz in kleinen und mittleren Unternehmen sowie für die Anbindung von Kassensystemen und Geldausgabeautomaten. Alle Features, die heute eine moderne Datenkommunikation fordert, sind im R450 implementiert. Neben der Funktion als VPN Access Router bietet der R450 die Verwendung als VPN Gateway. Umfangreiche und komplexe Adressumsetzungs- und Routingfunktionen erlauben die Anbindung unterschiedlichster Netze. Bestehende und künftige Netzwerke von Partnerunternehmen, Home Offices oder Filialen werden so problemlos in ein VPN integriert.

- **(A)DSL UR2 Modem**
- 1 x **ISDN BRI (R450i)**
- 1 x **Analog Modem (R450p)**
- 1 x **synchroner/asynchroner Port** X.21bis(V.24)
- 4 x **10/100BaseT Ethernet** (Autosense)

Volle Unterstützung der IPSec Suite (max. 50 Tunnels) mit Verschlüsselungsverfahren wie z.B. AES, DES oder 3DES, garantieren systemübergreifende Kompatibilität und schützen sensible Daten vor Zugriff unbefugter Dritter. Eine leistungsfähige Firewall, detaillierte Monitoring-, Accounting-und Content-Filter-Funktionen kennzeichnen die sicherheitsorientierte Ausrichtung des Routers.

Multiservice Router M3000

Der M3000 ist eine modular aufgebaute und deshalb flexibel einsetzbare Multiprotokoll Router-Plattform. Sie wurde speziell für das Umfeld in kleineren und mittleren Unternehmen optimiert. So z.B. als High-Speed VPN Access-Router oder aber als VPN-Gateway.
Durch den modularen Aufbau der M3000 Architektur ist sie die ideale Plattform für alle Arten von Anschlüssen, wie:

- **(A)DSL UR2 Modem**
- **UMTS / EDGE / GPRS Modem**
- **ISDN BRI / PRI**
- **Analog Modem**
- **synchrone/asynchrone Ports**
- **10/100/1000BaseT Ethernets, usw.**

Die Implementierung von individuellen Software-Modulen kann unter Verwendung der T.D.T.-eigenen Linux Distribution einfach und schnell realisiert werden.

- **bis zu 1000 VPN Tunnel**
- **Verschlüsselung durch IPSec Standards**
- **Authentifizierung durch IPSec Standards**
- **Unterstützung von Zertifikaten und PreShared Keys**
- **High Security Firewall mit Intrusion Detection**
- **High Accessibility mittels VRRP, usw.**

Netz. Sicherheit und Zuverlässigkeit finden dabei ganz besondere Beachtung.

Das intelligente Backup-Management im M3000 steuert im Bedarfsfall vollautomatisch die einzelnen Backupwege. Die Umschaltung und Rückschaltung nach ISDN, UMTS/GPRS oder einem beliebigen anderen Ersatzweg erfolgt vollautomatisch. Die Anwendung bleibt davon unberührt.

Die Nutzung mit Secure DynDNS eröffnet weitere Möglichkeiten. So ist der M3000 trotz dynamischer IP-Adresse stets von außen zu erreichen und stellt damit eine Vielzahl von zusätzlichen Diensten, wie FTP-Server, bereit.
Das integrierte Remote Management erlaubt die Administration des M3000 Systems von einem beliebigen Standort im

Ersetzt Standleitungen: R64SX

Auf Grund mangelnder Information oder Bedenken bezüglich Sicherheit nutzen noch zahlreiche Unternehmen teure D64S/S2- oder DDV-Standleitungen, um ihre Firmenstandorte zu verbinden.
Modernste und geprüfte Verschlüsselungs- und Authentifizierungs-Verfahren erlauben es, günstige öffentliche IP-Netze für die Übertragung von hoch sensitiven Daten zu nutzen.
Der Router R64SX wurde speziell für diesen Einsatz entwickelt. Bestehende Endgeräte können damit ohne Änderung der Betriebsparameter und ohne Änderung der Schnittstellen an ein kostengünstiges IP-Netz angebunden werden. Die ursprünglichen Kosten werden dann oft um ein Vielfaches unterboten.

Neben dem speziellen Feature der transparenten Datenübertragung und der Anpassung an die verschiedensten Schnittstellen (ISDN, X.21bis, X.21 und Ethernet) verfügt der R64SX über alle Standard-Features der Router-Serie. Die hohe Verfügbarkeit der Standleitung wird durch ein intelligentes Backup- und Fallback-Konzept im R64SX noch übertroffen (Backup z. B. über ISDN-Wählleitung).

Beispiel: Eine D64S2-Leitung von Essenbach (ca. 70 km NÖ von München) nach Reinheim (Nähe Frankfurt) kostet 530,- Euro pro Monat. Die Lösung mit dem R64SX kommt monatlich auf nur 55,- Euro (Stand 01/06).

IMPRESSUM

Herausgeber: T.D.T. Transfer Data Test GmbH, Siemensstraße 18, 84051 Essenbach, Tel. 08703 929-00, Fax 08703 929-201, E-Mail: info@tdt.de, http://www.tdt.de

Verantwortlich für den Inhalt: Michael Pickhardt, Geschäftsführer; H. J. Büttner, Vertriebsleiter

Gesamtproduktion: MCW, Marketing-Consulting GbR, Ulmenstraße 21, 84051 Essenbach, Telefon 08703 91360, eMail: jwimmer@rze.de

Auflage: 9.000 Exemplare

Ausgabe 1/2006 Auf Umweltpapier gedruckt

Sie können die SWITCHED kostenlos auf unserer Homepage abonnieren und alle Infos über die neuen TDT-Produkte anfordern!

T.D.T.-Online-Shop

Im Zuge der Leistungsfähigkeit und Kundennähe stellt T.D.T. ausgewähltes Produktzubehör für T.D.T.-Geräte und die beliebte Pocket Guide-Reihe online. Damit können Sie per Mausklick direkt bestellen.

Den Online Shop finden Sie unter **http://shop.tdt.de** oder über die T.D.T.-Homepage (www.tdt.de)