Dr. Suppan International Institute

Der Netzwerk Insider

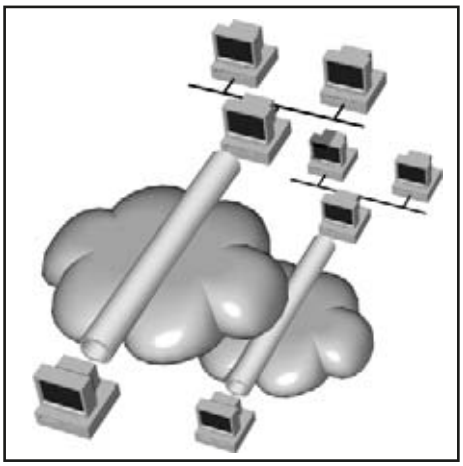
November 2003

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktartikel

Problematische VPN-Aspekte – Redundanz und NAT

von Dipl.-Inform. Andreas Meder



Thema 1: Redundanz

VPNs werden – mit Blick auf Kosten und Sicherheit der Datenübertragung zu recht – immer beliebter. Gleichzeitig wird ihr Einsatz immer unkomplizierter, da immer mehr Hersteller entsprechende Funktionen in ihre Produkte integrieren und über Zusatzmechanismen auch für ein vereinfachteres Handling sorgen. Dennoch tauchen häufig Fragestellungen auf, die auf Basis von Out-of-The-Box-Lösungen nicht oder nur unzureichend geklärt werden können.

Zwei dieser Themen sollen in diesem Artikel etwas näher beleuchtet und Anregungen zur Klärung gegeben werden.

weiter Seite 20

Thema 2: NAT

Drittthema

Anwenderbericht: IP-Telefonie

von Karl-Heinz Hommen-Menz

Im September 2002 wurde an dieser Stelle erstmals über die Erfahrungen mit dem Cisco Call Manager berichtet und einige fehlende, aber zur vollständigen Ablösung einer TK-Anlage erforderlichen Leistungen erwähnt. Nachdem mit der Version 3.2.2 des Call Managers, Grundlage des damaligen Berichts, die für einen Produktionsbetrieb geforderte Zuverlässigkeit erreicht war, kann die aktuelle Software mit dem Versionsstand 3.3(2) eine Reihe neuer Leistungsmerkmale vorweisen, auf die der deutsche Markt schon seit geraumer Zeit gewartet hat.

Neben der Möglichkeit verschiedene Klingeltöne für unterschiedliche Leitungen am Telefon zu definiert, wurden nun auch Funktionen wie „Rückruf bei besetzt“, „Rückruf bei frei bzw. nicht angenommen“, die fallweise Rufnummernunterdrückung und eine Chef-Sekretärin Funktion implementiert.

Das Cisco-XML unterstützt inzwischen die Push-Technologie. Mit dieser Technik ist es möglich, auf dem Telefondisplay eigenständige Informationen ein- und wieder auszublenden.

Der Administrator kann die Menütastenbelegung der IP-Telefone unterschiedlich gestalten und mehrere Ebenen für die Zugriffsrechte auf die Call Manager Administrationsoberfläche einrichten, die unterschiedlichen Personen mit abgestuften Rechten zugewiesen werden können.

Neben dem Call Manager bietet auch die Version 4 des Produktes Unity, das Unified Messaging System der Firma Cisco, einige Mehrwerte in der Telefonie. Dies wird in diesem Artikel am Beispiel eines Call Handling verdeutlicht.

weiter Seite 4

Top-Event

Das Wireless LAN Forum 2003

auf Seite 14

Zum Geleit

IP-Telefonie: das Ende der Nachrichten-technik(er)?

auf Seite 2

Studie des Monats

Voice over IP Report: Zeitverzug (Delay)

auf Seite 16

Zum Geleit

IP-Telefonie: das Ende der Nachrichtentechnik(er)?

IP-Telefonie breitet sich immer weiter aus. Betrachtet man die inzwischen realisierten Projekte, dann decken diese eine erhebliche Bandbreite von kleinen Testinstallationen bis hin zu Installationen von mehreren Tausend Telefonen ab. Auf den ersten Blick liegen die Hauptursachen für die zunehmende Verbreitung sowohl im inzwischen konkurrenzfähigen Preis als auch in der erreichten Produktqualität mit der Abdeckung der meisten geforderten Leistungsmerkmale.

Auf den zweiten Blick liegt ein wesentliches Merkmal dieser Entwicklung in einem ganz anderen Bereich. Die Konfiguration einer IP-Telefonie-Lösung erfordert ein anderes Wissen als die Konfiguration einer klassischen TK-Anlage. Letztere ist dem gut ausgebildeten Nachrichtentechniker vorbehalten, der in der Lage ist, zwischen Linienschaltungen, der Konfiguration von Einbaugruppen, der Gestaltung umfangreicher Rufnummernpläne einen Weg zu einer funktionsfähigen Anlage zu finden. Stellt man dem eine Lösung wie den CISCO Call Manager gegenüber, so verschieben sich die Themenschwerpunkte. Da werden kleine fehlende Lösungen mal eben in XML programmiert, ein kleines Skript hier, ein größeres da und schon ist das Leistungsspektrum der Anlage verändert. Fehlt dann noch etwas, so kann eine geschickte Kombination mit einer CTI-Lösung erstaunliches vollbringen, vom hoch funktionalen Vermittlungsarbeitsplatz bis zur Chef-Sekretärinnen-Schaltung. Nicht immer ist dabei nachvollziehbar, was da eigentlich geschehen ist. Es verwundert angesichts dieser Situation nicht, dass der typische Betreiber einer IP-Telefonie-Lösung mehr aus dem Bereich der Informatik kommt und eine Vorliebe für das tägliche Schreiben neuer Skripte hat (als besonders gefährlich gelten Linux-infizierte Systemverbieger ohne jeden Respekt vor traditioneller Technik).

Naturgemäß wird die Bewertung dieser Situation davon abhängen, welche Ausbildung die bewertende Person hat. Für die Nachrichtentechniker ist die neue Welt der IP-Telefonie, solange sie so aussieht wie beschrieben, eine Spielwiese für Sandalen-tragende Turnschuh-Fanatiker. Auf keinen Fall darf man diesen Leuten eine derartig wichtige zentrale Infrastruktur überlassen. Aus der Sicht der Informatik wurde es Zeit, dieses kryptische Gehampel um Linien und Baugruppen zu beenden.

Wer hat nun Recht? Nun erst einmal ist festzustellen, dass beide Ansätze zur Problemlösung tragfähig und akzeptabel sind. In der IP-Telefonie zeigt allerdings der überdurchschnittlich hohe Customizing-Aufwand, dass die Produkte noch nicht am Ende ihrer Entwicklung angekommen sind. Trotzdem weisen die vielen erfolgreichen Projekte der letzten Monate eine Nutzbarkeit der IP-Telefonie nach. Tatsächlich liegt der Hauptnachteil der IP-Telefonie in dem Umfang und den Kosten des notwendigen Customizings. Dies muss für einen Kostenvergleich mit einer traditionellen TK-Lösung beachtet werden, bereitet aber in der Kalkulation häufig das Problem, dass der Kostenaufwand zu Projektbeginn nur schwer quantifizierbar ist.

Der Gewinner kann auf Dauer nur die IP-Telefonie sein. Die hier eingesetzte Technik ist Teil der sich immer weiter entwickelnden Standard-Kommunikationstechnik unserer gesamten Unternehmens-IT. Man betrachte nur Microsoft Office 11 oder die Entwicklung um J2EE (IBM Webshere, BEA, …) und deren immer größere Rolle für die strategischen Applikationen der Unternehmen. Wir sind erst am Anfang der Entwicklung. Diese Art von Technik wird die gesamte IT in allen Bereichen in den nächsten Jahren prägen. Und IP-Telefonie liegt voll auf dieser Welle, ihre Technologie ist integraler Bestandteil unserer zukünftigen IT-Landschaft.

Und damit nicht genug. Bisher war Telefonie eine isolierte Technologie. Der aktuelle Trend geht hin zu integrierten Kommunikationslösungen (siehe den aktuellen Microsoft Messenger). Auch der neue Ansatz der Teamkommunikation mit Präsenz-Anzeige wie sie als Basis durch den Realtime Communication Server von Mircosoft zusammen mit der Open Scape Applikation von Siemens gezeigt wird, zeigt in diese Richtung. Die Vereinigung von e-Mail, Telefonie und Video in Richtung eines frei wählbaren Kommunikations-Mix ist voll im Gange. Die harmonische Integration dieser standortübergreifenden Team-Funktionalität in unsere Arbeitsplatz-Systeme und Applikationen, sei es auf einem PC, einem PDA oder in einer Terminal-Anwendung, das ist der augenblickliche Trend. In diesem Trend hat die traditionelle TK-Anlage keinen Platz mehr.

Trotzdem bleibt zu kritisieren, dass viele der angebotenen IP-Telefonie-Produkte in ihrem Aufbau zu komplex sind. Hier wurde eine große Chance vertan, Kommunikation wesentlich transparenter in der Konfiguration zu machen. Aber die Entwicklung ist ja noch nicht am Ende und man soll die Hoffnung ja nie aufgeben.

Die Entwicklung in Deutschland wird zudem noch geprägt durch die Produkte und zukünftigen Technologien des Marktführers Siemens. Viele der auf dem Weltmarkt angebotenen und funktional durchaus interessanten Produkte werden in Deutschland zerrieben in der Konkurrenz zwischen CISCO und Siemens um den künftigen TK-Markt. Aber auch im Hause Siemens hat der Wandel angefangen. OpenScape mag als Produkt eine noch unklare Zukunft haben (es müsste ja erst einmal vorzeigbar existieren), es ist aber ein Indikator für eine veränderte Grundhaltung von Siemens zu diesen Technologien. Zudem muss Siemens im Gegensatz zu CISCO den Spagat zwischen den vielen bestehenden Nutzern traditioneller TK und dem zunehmenden Druck in Richtung IP-Telefonie in neuen Projekten machen. Eine sicher nicht leichte Aufgabe.

IP-Telefonie: das Ende der Nachrichtentechnik(er)? In einem gewissen Sinne ja. Aber auf der einen Seite ist Nachrichtentechnik nicht auf Telefonie reduziert und auf der anderen Seite haben Nachrichtentechniker eine der besten Ausbildungen, die es in Deutschland neben dem Maschinenbau gibt. Natürlich sollten sie mit dieser Ausbildung in der Lage sein, sich die neuen Kommunikations-Technologien zu erschließen. Das ist sicher nicht leicht, viele müssen dafür wieder bei Null anfangen. Nur wer diesen Weg nicht geht, der könnte in Zukunft schlechte Karten haben.

IP-Telefonie: das Ende der Nachrichtentechnik(er)?

Wie können wir Ihnen auf dem Weg in die IP-Telefonie helfen? Brandaktuell ist die Winterschule 2003, die sich an 5 Tagen intensiv dem Thema IP-Telefonie-Evaluierung stellt. Eine einmalige Chance, den aktuellen Stand der Technik und die wichtigsten Entwicklungen kompakt präsentiert zu bekommen.

Die Winterschule wird begleitet durch die Vorstellung der neuesten Studie von ComConsult-Research: „CISCO kontra Siemens, wer hat die bessere TK-Lösung?“. Schon der Titel gibt die gesamte Brisanz dieser Studie wieder, die ein Muss für jeden Entscheider in diesem Bereich ist.

Ihr Dr. Jürgen Suppan

Aktuelles Seminar

Winterschule 2003: IP-Telefonie-Intensiv-Evaluierung und IP Betriebsgrundlagen

Vom 1. bis 5. Dezember veranstaltet die ComConsult Akademie im Technologiezentrum der AGIT Aachen ihre diesjährige Winterschule mit dem Schwerpunkt "IP-Telefonie".

Die Intensiv-Evaluierung von IP-Telefonie ist der Inhalt dieser Winterschule. Wir halten das Thema für so wichtig, dass wir ihm alle 5 Tage der Winterschule widmen. Wir möchten alle Aspekte einer VoIP-Entscheidung beleuchten und Ihnen auf diese Weise wesentlich langwierigere Projektarbeiten ersparen.

Die Vorträge im Einzelnen:

- Aktuelle Marktsituation und Trends für Voice over IP
- Einführung in IP Telefonie
- Einsatz von Hardphones und das Problem "Power über LAN"
- Die verfügbaren Standards – ITU vs. IETF
- Monitoring und Troubleshooting in Voice Netzwerken
- Voice over Wireless

- DNS und Voice Endgeräte
- DHCP und Voice Endgeräte
- Network Adress Translation (NAT)
- Security-Maßnahmen und Lösungen für Voice over IP
- Architektur und Lösungsmöglichkeiten für VoIP mit Alcatel
- Architektur und Lösungsmöglichkeiten für VoIP mit Avaya
- Architektur und Lösungsmöglichkeiten für VoIP mit Nortel
- Architektur und Lösungsmöglichkeiten für VoIP mit Tenovis
- Realisierung einer IP Telefonie-Lösung mit Mitel
- Realisierung einer IP Telefonie-Lösung mit Swyx
- VoIP-Projekterfahrungen
- Kriterien für Evaluierung und Produktauswahl
- Cisco: Aktuelle Neuankündigungen und Roadmap
- Siemens: Aktuelle Neuankündigungen und Roadmap
- Cisco versus Siemens: Technische Bewertung
- Cisco versus Siemens: Sicherheitsbewertung
- Cisco versus Siemens: Strategische Bewertung
- ROI Überlegungen
- Design und Betrieb von Voice-Lösungen
- Anforderungen an die Netzwerk-Architektur

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Winterschule

☐ Ich melde mich an zum
Winterschule der ComConsult Akademie 2003: IP-Telefonie-Intensiv-Evaluierung
vom 01.12. - 05.12.03 in Aachen
(Preis: € 2.290,-- zzgl. MwSt.)

☐ Buchen Sie für mich ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Zweitartikel November 2003

Anwender-bericht: IP-Telefonie

Fortsetzung von Seite 1

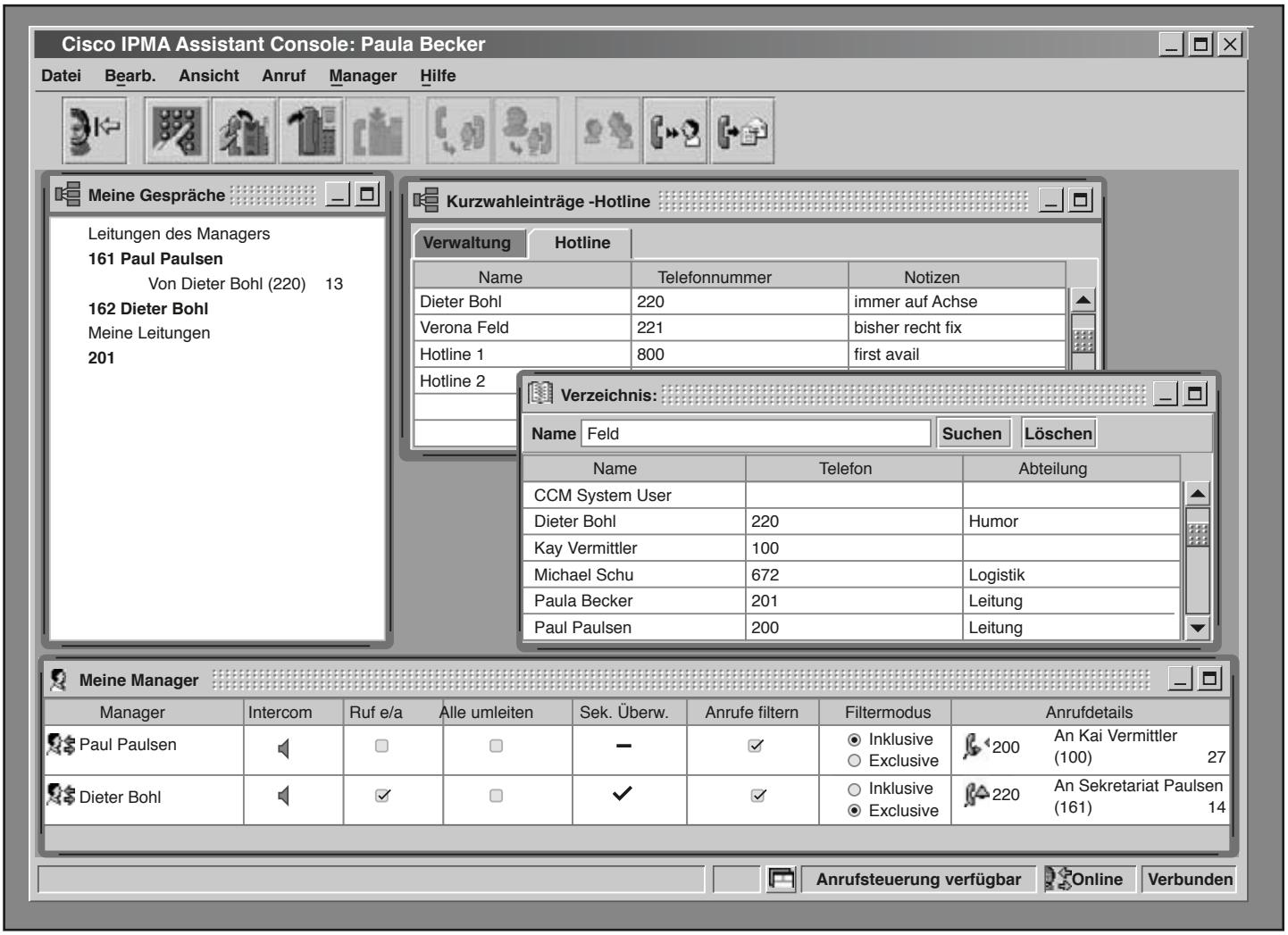
Karl-Heinz Hommen-Menz
ist seit 1979 im Rechenzentrum der Finanzverwaltung NRW tätig. Heute ist er als Dezernent für den Bereich "Systemtechnik Netze" verantwortlich und beschäftigt sich seit 1991 mit Planung, Realisierung, Tuning, Dokumentation und Betrieb von Netzen.

Neue Funktionen des Call Managers

Die Chef-Sekretärin Funktion wurde von Cisco auf eine Windows Anwendung abgebildet. Die IPMA Assistant Console ermöglicht es, am PC-Arbeitsplatz einer Sekretärin mehrere Cheftelefone zu verwalten. Die Anwendung wurde so konzipiert, dass die Chefs als „mobile Manager“ die Funktion Extension Mobility nutzen können und sich so mobil an unterschiedlichen IP-Telefonen anmelden können.

In der Anwendung werden eingehendeGespräche dem jeweiligen Telefon zugeordnet angezeigt, sie bietet ein eigenes Telefonbuch mit Kurzwahlzielen, eine Suchfunktion im Unternehmensverzeichnis und eine Reihe von Vermittlungsfunktionen über Schaltflächen oder per „drag and drop“.

Bild 1



Anwenderbericht: IP-Telefonie

Bild 2

Sehr schön gelöst ist die Möglichkeit Rufnummernfilter zu definieren. Durch setzen von Ex- oder Inklusivfilter, über die Anwendung oder den Internet-Explorer, können bestimmte Teilnehmer direkt mit einem Chef sprechen, während alle anderen Anrufe zur Sekretärin geleitet werden.

An den Cheftelefonen wird im Display ein zusätzliches Fenster dargestellt. Die Symbole (Bild 2) zeigen, ob die Sekretärin anwesend ist, Filter aktiviert oder deaktiviert sind, der Klingelton des Cheftelefons an- oder abgeschaltet ist und ob die Anrufe zur Sekretärin umgeleitet werden oder nicht.

Diese Funktionen können von der Sekretärin über die IPMA Assisant Console und vom Chef über ein entsprechendes Menü am Telefon ein- oder ausgeschaltet werden.

Mit der aktuellen Software wurde auch die Call Distribution (Anrufverteilung), wie sie für Hotlines benötigt wird, verbessert und weist nun ein zuverlässiges Laufzeitverhalten auf. Der Administrator kann zwischen zwei unterschiedlichen Verfahren wählen und in Kombination mit Unity ergeben sich gewinnbringende Lösungen.

Bei der Variante „Longest idle first“, werden die Gespräche zu dem Teilnehmer geleitet, der am längsten nicht telefoniert hat. Sollen die Gespräche immer zum ersten freien Platz einer vorgegebenen Reihenfolge gelangen, so richtet der Administrator die Eigenschaft "First Available" ein.

Auch das An- und Abmelden von Bearbeitern an einer oder mehreren Hotline-Schaltungen kann über „Extension Mobility“ konfiguriert werden. Sind alle Telefone besetzt oder keiner der Bearbeiter angemeldet, so können die Gespräche automatisch zur Unity Voice-Mail geleitet werden.

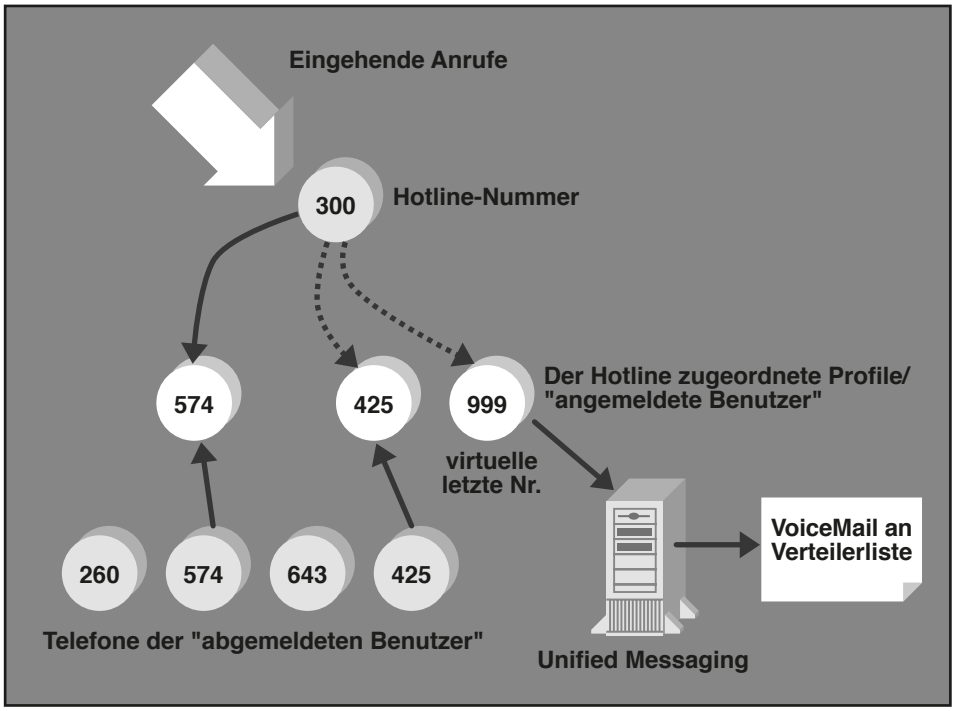


Bild 3

Im Bild 3 sind nur die Mitarbeiter mit den Telefonnummern 574 und 425 an der Hotline mit der Rufnummer 300 angemeldet. Alle eingehenden Gespräche werden auf diese beiden Teilnehmer verteilt oder, falls diese nicht erreichbar sind oder gerade ein Gespräch führen, auf die Voice-Mail geleitet.

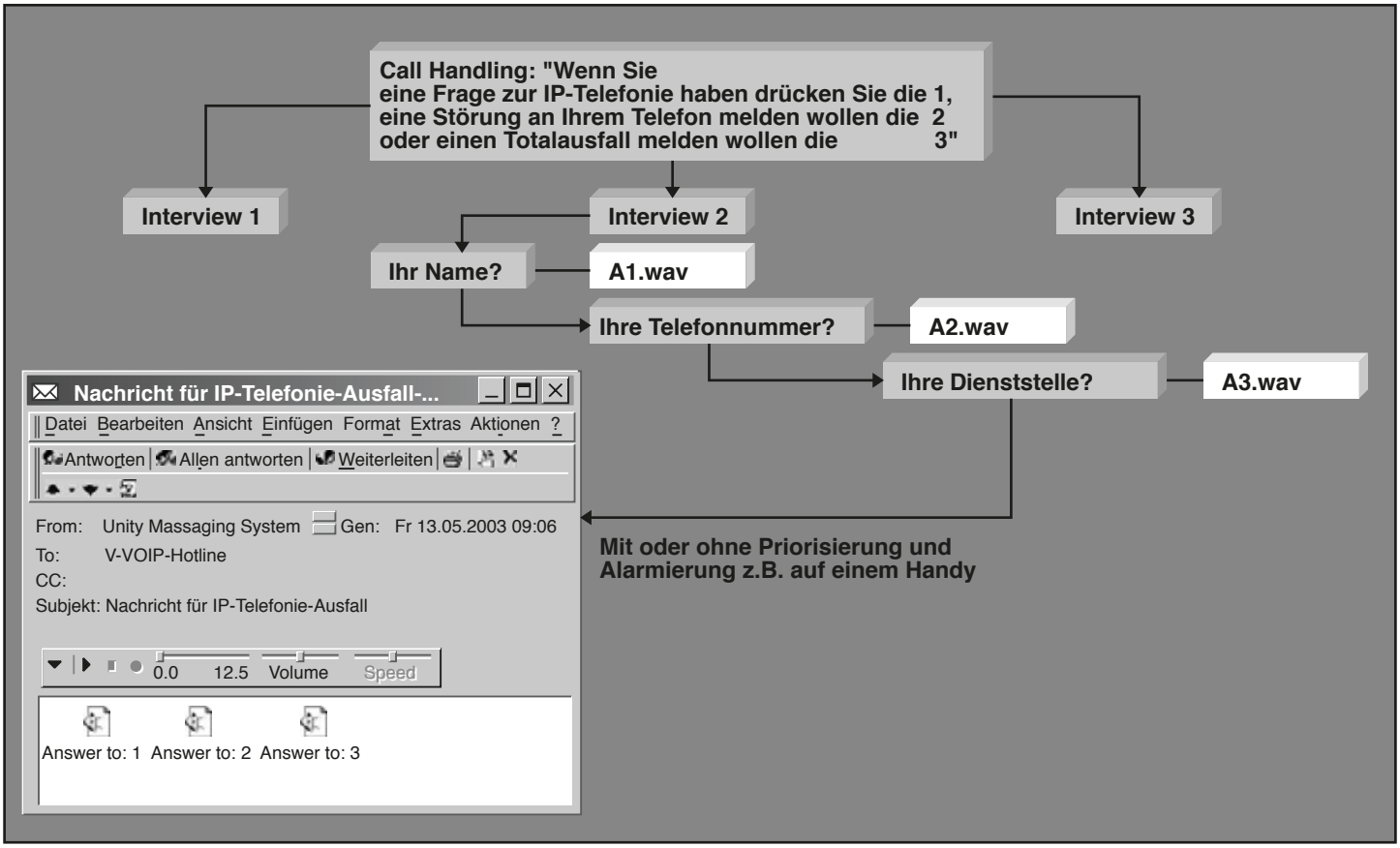


Bild 4

Das Call Handling von Unity

Das Unity-System erlaubt es, an dieser Stelle ein automatisches Callhandling einzubauen.

Zu Beginn kann der Anrufer über eine akustische Ansage aufgefordert werden, sein Anliegen genauer zu spezifizieren.

Über die entsprechende Zifferneingabe an seinem Telefon gelangt der Anrufer danach zu einem Interviewhandler.

Dieser Interviewhandler führt mit dem Anrufer einen zuvor definierten Dialog auf der Basis aufgezeichneter Fragen.

Die Antworten werden in Wave-Dateien gespeichert und als Anhänge der letztlich erzeugten Voice-Mail beigestellt.

Entsprechend der Wichtigkeit können für die unterschiedlichen Zweige dieser interaktiven, automatischen Gesprächsabwicklung weitere Aktionen definiert werden.

So kann eine Voice-Mail über ein gemeinsames Postfach aller Hotline-Bearbeiter abgearbeitet oder einem Bearbeiter gezielt zugeleitet werden. Eine Mail kann als „Wichtig“ markiert werden und für die besonders dringenden Fälle wird als Aktion ein Anruf zu einer definierten Rufnummer konfiguriert. Die dargestellten Möglichkeiten verbessern sowohl die Erreichbarkeit der Mitarbeiter als auch die Effizienz bei der Bearbeitung.

Ab der Version 3.3(2) ist der Call Manager also ein ganzes Stück erwachsener und sehr zuverlässig geworden. Um jedoch den funktionalen Anforderungen eines großen Unternehmens oder einer großen Behörde gewachsen zu sein, benötigt er einen leistungsstarken Partner. Diesen Partner hat die Firma Cisco in der Telesnap AG aus Stuttgart, einem Unternehmen mit langjähriger Erfahrung im Telefonmarkt, gefunden.

Die Cisco zertifizierten Produkte der Telesnap AG, wie der PM Operator und die XML-Clients, wurden speziell für den Call Manager entwickelt. Zusammen mit der Snapware, die auch diverse TK-Anlagen unterstützt, veredeln diese Anwendungen den Call Manager zu einer gelungenen Gesamtlösung für die Telefonie und das mit einem einzigen zusätzlichen Server, der in das lokale Netz integriert wird.

Die Produkte der Firma Telesnap

Die Telesnap-Produkte bereichern den Call Manager um einem leistungsstarken Vermittlungsarbeitsplatz, bringen zusätzliche Leistungsmerkmale für IP-Telefone und elegante CTI-Funktionen, die eine effiziente Arbeitsweise ermöglichen sowie zusätzlichen Komfort schaffen.

Der XML-Client der Telsnap AG erweitert den Funktionsumfang der Cisco IP-Telefone um Leistungsmerkmale wie Ablehnen eines Anrufs, Anruferkennung, Rufumleitungsprofile, Telefonjournale, Anzeige der häufigsten Verbindungen etc. und um die Möglichkeit, Privatgespräche zu kennzeichnen oder Gespräche einer besonderen Kostenstelle zuordnen zu können.

Die Kennzeichnung von Privatgesprächen ist insbesondere beim Einsatz im Behördenumfeld erforderlich, da diese grundsätzlich privat abzurechnen sind.

Über die Taste Services bekommt der Benutzer Zugang zu den XML-Services. Im Menü wählt er die Snapware-XML-Services und danach ist eine der vier kontextsensitiven Funktionstasten des Telefons mit der PIN-Funktion belegt. Drückt der Benutzer diese Taste, so wird er über das Display am Telefon aufgefordert seine PIN einzugeben.

Die verdeckt eingegebene PIN wird vom System mit der vom Administrator, für den jeweiligen Benutzer, gesetzten PIN verglichen. Ist die PIN identisch, drei Eingabeversuche sind zulässig, so wird nach verlassen der Services ein Push-Fenster auf dem Display angezeigt. Das nächste Gespräch ist dann automatisch als Privatgespräch gekennzeichnet. (Bild 5-8)

Entschließt sich ein Benutzer nach dem setzen der Privatgesprächskennung doch kein privates Telefonat zu führen, so kann die PIN über den XML-Service wieder verworfen werden oder er wartet einen vom Administrator einstellbaren Zeitraum ab. Durch Führen eines Gesprächs oder durch Zeitablauf verschwindet das Push-Fenster aus dem Display und damit auch die Kennung.

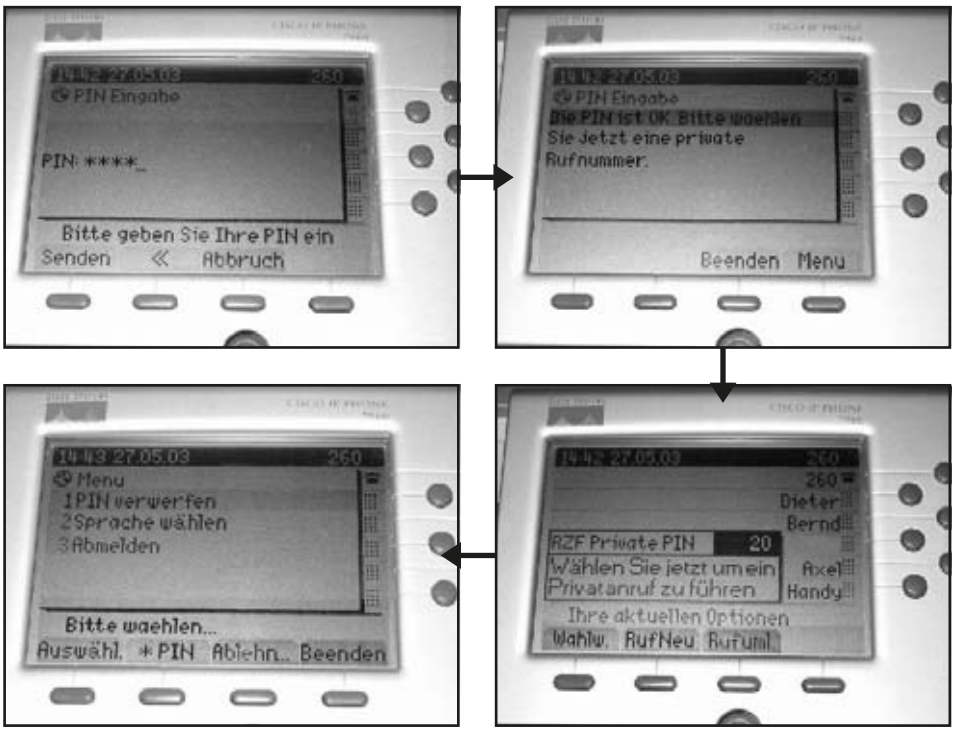
Nach einem Privatgespräch trägt die Anwendung in der CDR-Datenbank (Call Detail Records) des Call Managers die PIN nebst einer Kennung ein. Die Datensätze der gesondert abzurechnenden Gespräche können so von einer Gebührendatenverarbeitung erkannt und ausgewertet werden.

Dieses Verfahren hat den Vorteil, dass jede Rufnummer, die zum Beispiel direkt aus den Outlook-Kontakten, aus einer WEB-Seite oder aus einer beliebigen CTI-Anwednung am PC angewählt wird, als dienstlich oder privat gekennzeichnet werden kann. Entscheidend ist lediglich, ob vor dem Gespräch die PIN gesetzt wurde oder nicht. Da das Verfahren mit Extension Mobility kombiniert werden kann, kann ein Benutzer von jedem IP-Telefon ein Privatgespräch führen.

Der PM-Operator von Telesnap, ein speziell für den Cisco Call Manager entwickelter Vermittlungsarbeitsplatz, wartet neben den reinen Vermittlungsfunktionen, den üblichen Warteschlangen, automatischen Ansagen und Wartemusik mit einer Reihe komfortabler Merkmale auf. Die Anwendung ist als Client-Server Applikation entwickelt und unterstützt mit einem Server mehrere Clients, also Vermittlungsarbeitsplätze.

Ein Pluspunkt bezüglich der Wirtschaftlichkeit der Lösung ist, dass für alle Telesnap-Produkte, also für die XML Clients, die PM-Operator Clients und die Snapware Clients, nur ein Server zu betreiben ist, der alle Arten von Klienten unterstützt.

Bilder 5 - 8



Anwenderbericht: IP-Telefonie

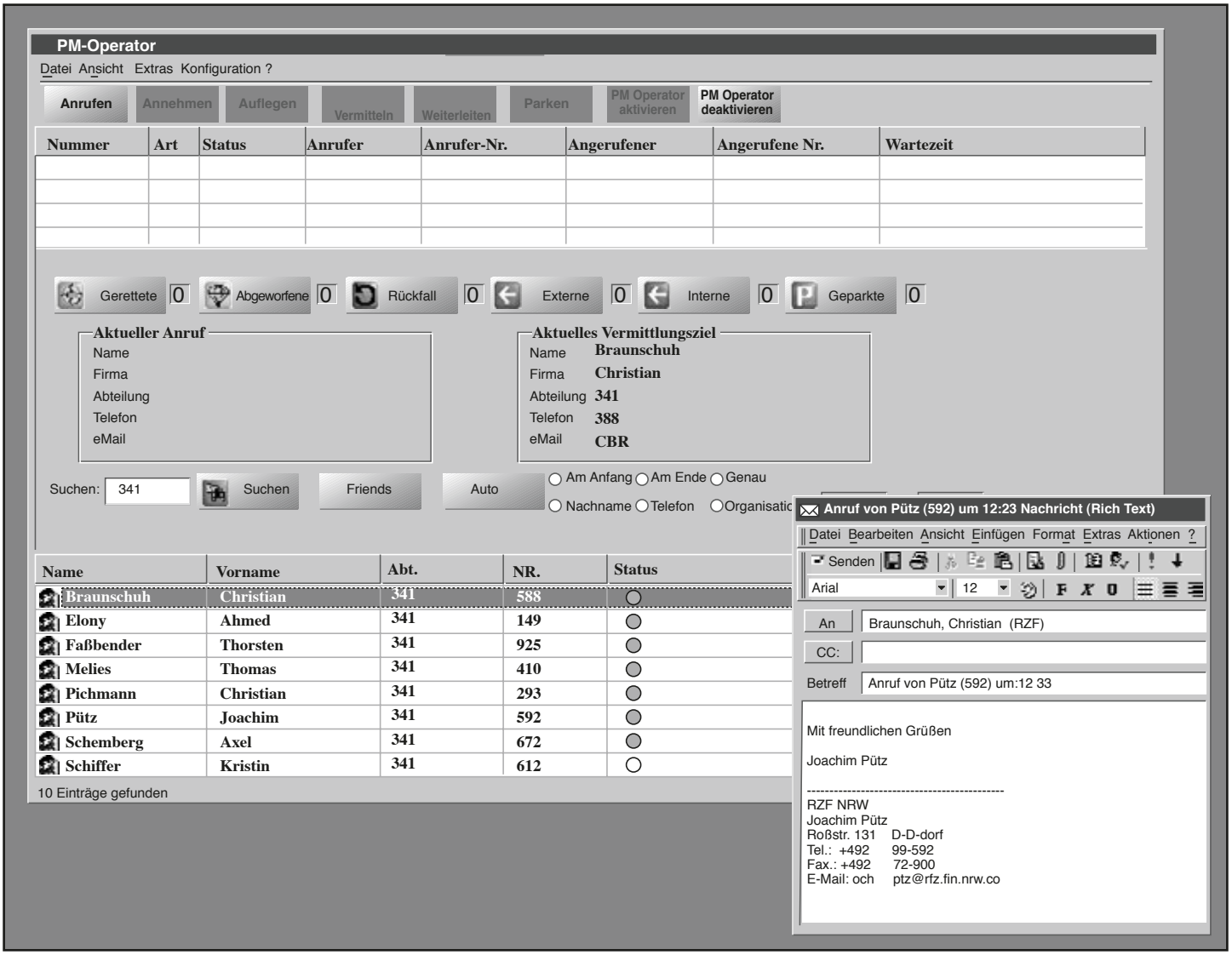


Bild 9

Der in folgende grobe Bereiche unterteile Desktop ist sehr übersichtlich gestaltet. Im oberen Menü befinden sich die Bedienungselemente für die Gesprächsannahme und Weitergabe, darunter werden die eingehenden Anrufe dargestellt. Im mittleren Bereich befinden sich die Gesprächswarteschlangen, die Suchoptionen sowie das Eingabefeld für die Suche, deren Ergebnis im unteren Bereich dargestellt wird. An der rechten Seite des Desktops werden die gespeicherten Kurzwahlziele angezeigt. (Bild 9)

Die Suche läuft direkt per LDAP über definierbare Attribute eines Unternehmensverzeichnisses. Falls ein globales Unternehmensverzeichnis nicht existiert, kann auch über die konfigurierten Teilnehmer im Call Manager gesucht werden, da dieser selbst als LDAP-Server fungieren kann.

Alle Funktionen des Vermittlungsplatzes können von der Vermittlungskraft selbst auf individuelle Softkeys gelegt, die Suchoptionen können eingestellt und Kurzwahlziele definiert werden.

Falls ein Teilnehmer nicht erreichbar ist, so kann die Vermittlungskraft direkt aus dem PM-Operator eine e-Mail versenden. Dieser Nachricht wird automatisch die Telefonnummer bzw. der Name des Anrufers sowie die Uhrzeit beigestellt und kann vor dem Absenden durch einen Freitext im Rumpf ergänzt werden. So geht keine Information mehr verloren.

Fast selbstverständlich versteht sich, dass in der Anwendung der Status von Vermittlungszielen, also IP-Telefonen angezeigt wird. Sucht die Vermittlungskraft beispielsweise über die Organisation, so werden als Vermittlungsziele neben den Namen, Vornamen, Rufnummern, Oranisationsbezeichnung etc. der entsprechenden Teilnehmer, die Stati in Form von farbigen Symbolen angezeigt. Grün heißt, der Apparat ist frei, grau bedeutet, dass der Teilnehmer nicht am Telefon angemeldet ist also vermutlich nicht am Arbeitsplatz ist. Ist das Symbol rot, so telefoniert der Teilnehmer gerade. Alternativ können die Stati auch durch einen Text angezeigt werden.

Selbst die Eigenschaften des entsprechenden Eingabefeldes für die Suche können administriert werden. Hier kann eingestellt werden nach wieviel eingegebenen Zeichen und welcher Mindestzeitspanne in Millisekunden die Suche automatisch beginnt.

Besonderheiten für sehbehinderte Menschen

Die Eigenschaften einer Vermittlungsanwendung sind besonders für die Adaption von Hilfsmitteln für blinde oder stark sehbehinderte Personen, die häufig in Behörden an Vermittlungsplätzen eingesetzt sind, von großer Wichtigkeit.

Bei der gesamten Benutzerführung und dem Layout des PM-Operator wurde Wert auf eine möglichst einfache Anpassung für blinde und sehbehinderte Personen gelegt. Neben der alternativen Darstellung von Symbolen als Text ist die automatische Cursor-Fokussierung ein für die Handhabbarkeit durch blinde Menschen erforderliches Merkmal.

Bei einem eingehenden Anruf steht der Fokus automatisch in der Zeile, in welcher der Ruf angezeigt wird, nach Eingabe eines Softkeys im Suchfeld und nach der Suche automatisch auf dem ersten Vermittlungsziel.

Die Anpassung des PM-Operator an eine Braillezeile ist unter diesen Voraussetzungen mit der Software Jaws, die als Brückensoftware zwischen einer Microsoft-Anwendung und verschiedener Braillezeilen eingesetzt werden kann, innerhalb weniger Stunden machbar.

Die Vermittlungskraft ist danach in der Lage, alle Informationen in Blindenschrift (Braille) auf der Braillezeile zu lesen und über deren Tastatur und Funktionstasten die Anwendung und das IP-Telefon zu bedienen.

Durch die Einhaltung bestimmter Richtlinien bei der Programmierung der Oberfläche, kann die Oberfläche ohne Verluste von grafischen Informationen vollständig auf eine kontrastreiche schwarz/weiß Darstellung umgestellt werden und ist so optimal, über eine Vergrößerungssoftware wie Zoomtext, von Menschen mit geringem Restsehvermögen zu bedienen.

Mit dem Einsatz der genannten Zusatzsoftware wird auch die Sprachausgabe der im PM-Operator angezeigten Informationen unterstützt.

Wie sieht aber eine Lösung für blinde oder sehbehinderte Sachbearbeiter aus, die nicht über eine Vermittlungsanwendung auf ihren PC verfügen?

Der Mitarbeiter nutzt zur Bedienung seines Cisco IP-Telefons ein Cisco Softphone auf seinem PC, er wählt aus den Outlook-Kontakten oder aus einer WEB-Seite heraus und verwaltet die Konfiguration seiner Kurzwahltasten und seines persönliches Adressbuchs über die Weboberfläche des Call Managers.

Der Vorteil gegenüber herkömmlichen TK-Anlagen liegt darin, dass zusätzlich zu den bereits über eine Braillezeile bedienbaren Office-Anwendungen lediglich das Softphone über Jaws anzupassen ist.

Die in der Konzeption des Call Managers vorgesehene Bedienung der IP-Telefone über PC-Anwendungen schafft hier erhebliche Vorteile.

Durchdachte Funktionalität, individuelle Einstellungsmöglichkeiten und die gelungene Benutzerführung machen den PM-Operator zu einem effizienten, leistungsfähigen Vermittlungsplatz für den Call Manager. Seine grundlegende Bedienung ist innerhalb weniger Stunden gleichermaßen von sehenden als auch sehbehinderten Personen zu erlernen.

Anwenderbericht: IP-Telefonie

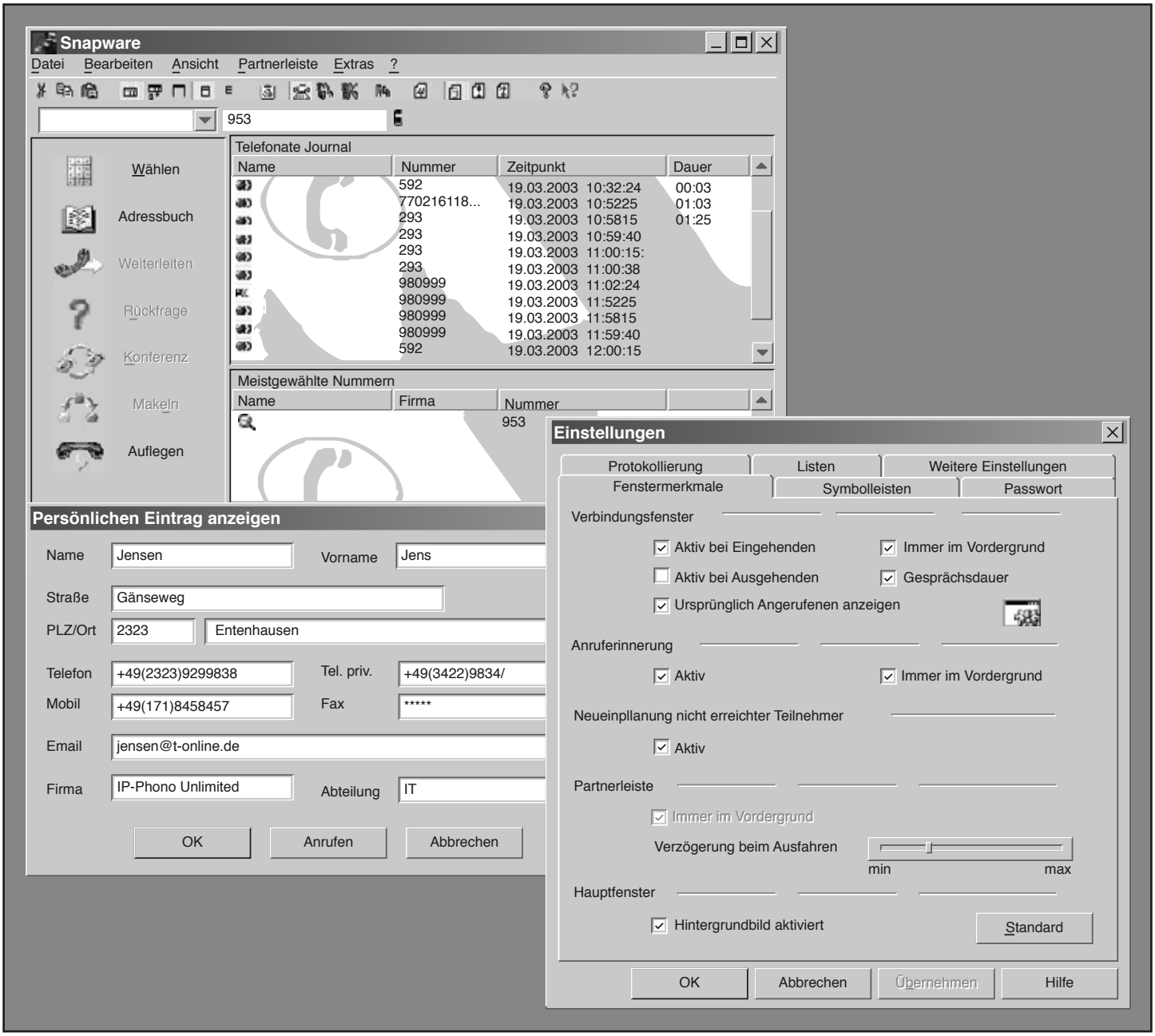


Bild 10

Für Mitarbeiter von Hotlines, großen, im Firmengebäude verteilten Teams, kleinen Call-Centern oder auch für Vieltelefonierer bietet die Snapware zahlreiche Funktionen die das Telefongeschäft sinnvoll unterstützen und die Effizienz steigern.

Die Snapware besteht aus mehreren Komponenten. Ein Snapware-Client umfasst ein Komfort-Telefon, das eigentliche Hauptfenster des Snapware-Systems, eine so genannte Partnerleiste, die am oberen oder seitlichen Bildschirmrand eingeblendet wird, den Presence-Manager und eine WEB-Komponente.

Das Komfort-Telefon kann wahlweise versteckt oder auf dem Bildschirm sichtbar betrieben werden (Bild 10). Es ermöglicht die Einstellungen der Anwendungseigenschaften, bietet Telefonjournale, automatische Erinnerungsfunktionen, die Einrichtung der Partnerleiste, bietet den Zugang zum Presence Manager, zur Verwaltung eines persönlichen Adressbuchs und verfügt über Schaltflächen zur Bedienung des Telefons. Aus dem Adressbuch, dem Telefonjournal und einer Liste der meist gewählten Rufnummern kann selbstverständlich direkt per Doppelklick gewählt werden.

Eine nach kurzer Zeit geliebte Funktion ist das Wählen einer Telefonnummer direkt aus einem beliebigen Dokument oder einer Anwendung über einen frei definierbaren Hotkey. Einzige Voraussetzung ist, dass die Nummer mit dem Mauszeiger markiert werden kann. Die Snapware filtert aus einer markierten Zeichenkette alle Zahlen heraus, erkennt ob es ein internes oder externes Gespräch ist und initiiert die Anwahl automatisch an dem Telefon des Benutzers. Kombiniert mit der XML-Funktion für Privatgespräche kann so jede Telefonnummer, egal wo sie auf dem Bildschirm steht, sowohl dienstlich als auch privat über den PC gewählt werden.

Anwenderbericht: IP-Telefonie

Bild 11

Mit der Partnerleiste (Bild 11) kann der Benutzer u.a. die Telefone seiner Teamkollegen, wichtige Telefonfunktionen, einen Kalender und Kurzwahlziele auf seinem PC abbilden. Die Farbe der Icons zeigt dabei an, ob das Telefon eines Teamkollegen frei oder besetzt ist und ob gerade intern oder extern telefoniert wird. An den kleinen Symbolen, neben den Telefonen erkennen Snapwarebenutzer an welchen Telefonen Rufumleitungen gesetzt sind, ein Rückruf initiiert ist oder ob der Kollege überhaupt am System angemeldet ist. Über die Snapware kann parallel zu einem Gespräch ein Chat zu einem Kollegen aufgebaut werden. Wird der Mauszeiger über eines der Symbole bewegt, so wird zudem angezeigt wer gerade anruft, wohin eine Rufumleitung führt etc. Gezieltes Heranholen von Gesprächen, man kann erst nachsehen wer beim Kollegen anruft, weiterleiten von Gesprächen, Konferenzen oder das einfache Anrufen werden per „drag and drop“ oder Mausklick unterstützt.

Der Umfang des Monitorings muss selbstverständlich sowohl vom Administrator als auch vom Benutzer freigegeben werden. Ohne entsprechende „Erlaubnis“ ist es nicht möglich die beschriebenen Funktionen uneingeschränkt zu nutzen.

Alternativ zu den dargestellten Möglichkeiten der Anrufverteilung auf Basis des Call Managers bietet auch die Telesnap in der Partnerleiste Hotlinefunktionen an. (Bild 12) Ein Hotline- Mitarbeiter kann sich mit einer speziellen Funktion, ohne seinen Telefonstatus zu verändern, an einer Hotline an- oder abmelden und einen Pause- oder Nachbearbeitungsstatus setzen. Auch die Integration der Telesnap eigenen Voice-Mail ist möglich. Beide Varianten bieten umfangreiche Möglichkeiten. Die Entscheidung für die Cisco- oder Telesnap-Variante hängt sicherlich von der Zahl der geplanten Snapware Clients im Unternehmen ab.

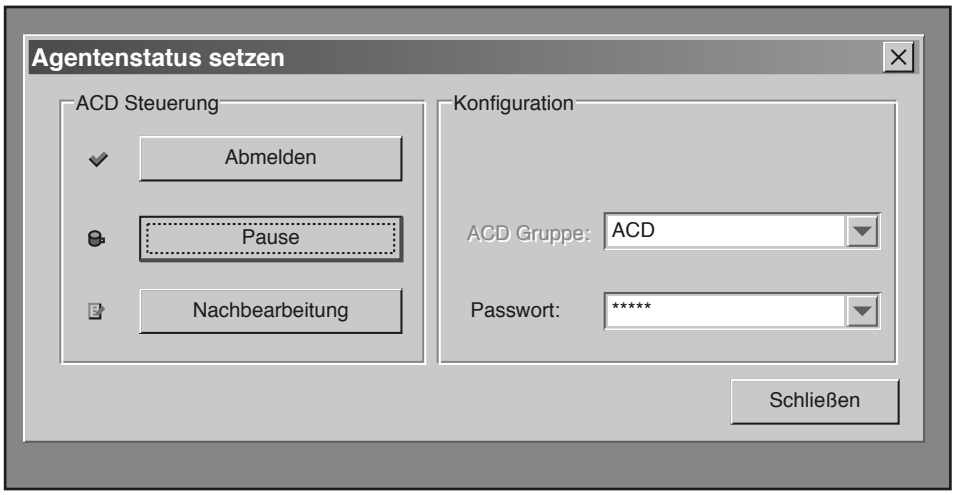
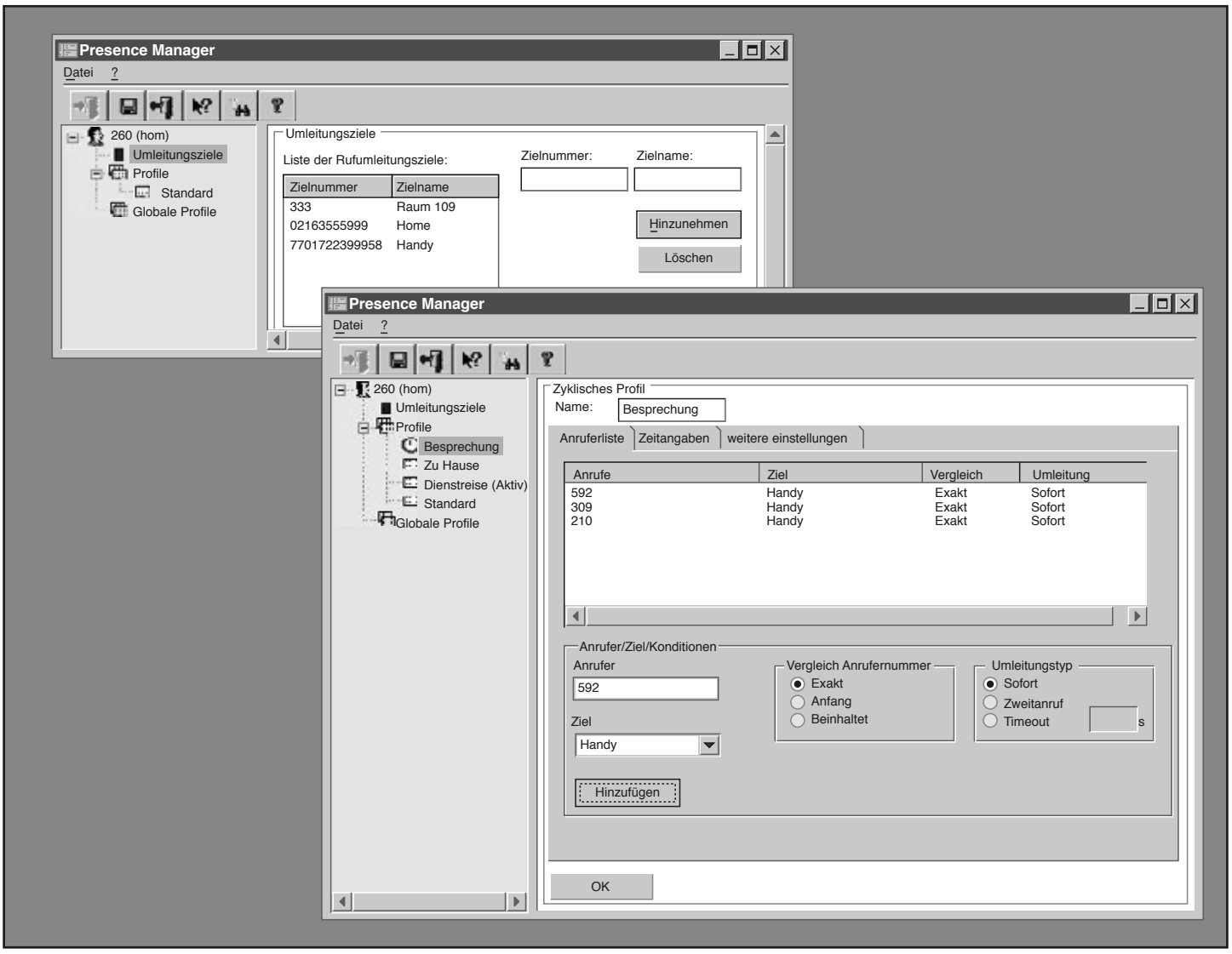


Bild 12

Zuletzt sei noch der Presence-Manager erwähnt (Bilder 13 - 14). Er ermöglicht dem Benutzer sein Telefon in Abhängigkeit vom Anrufer oder von der Uhrzeit gezielt umzuleiten.

Bild 13



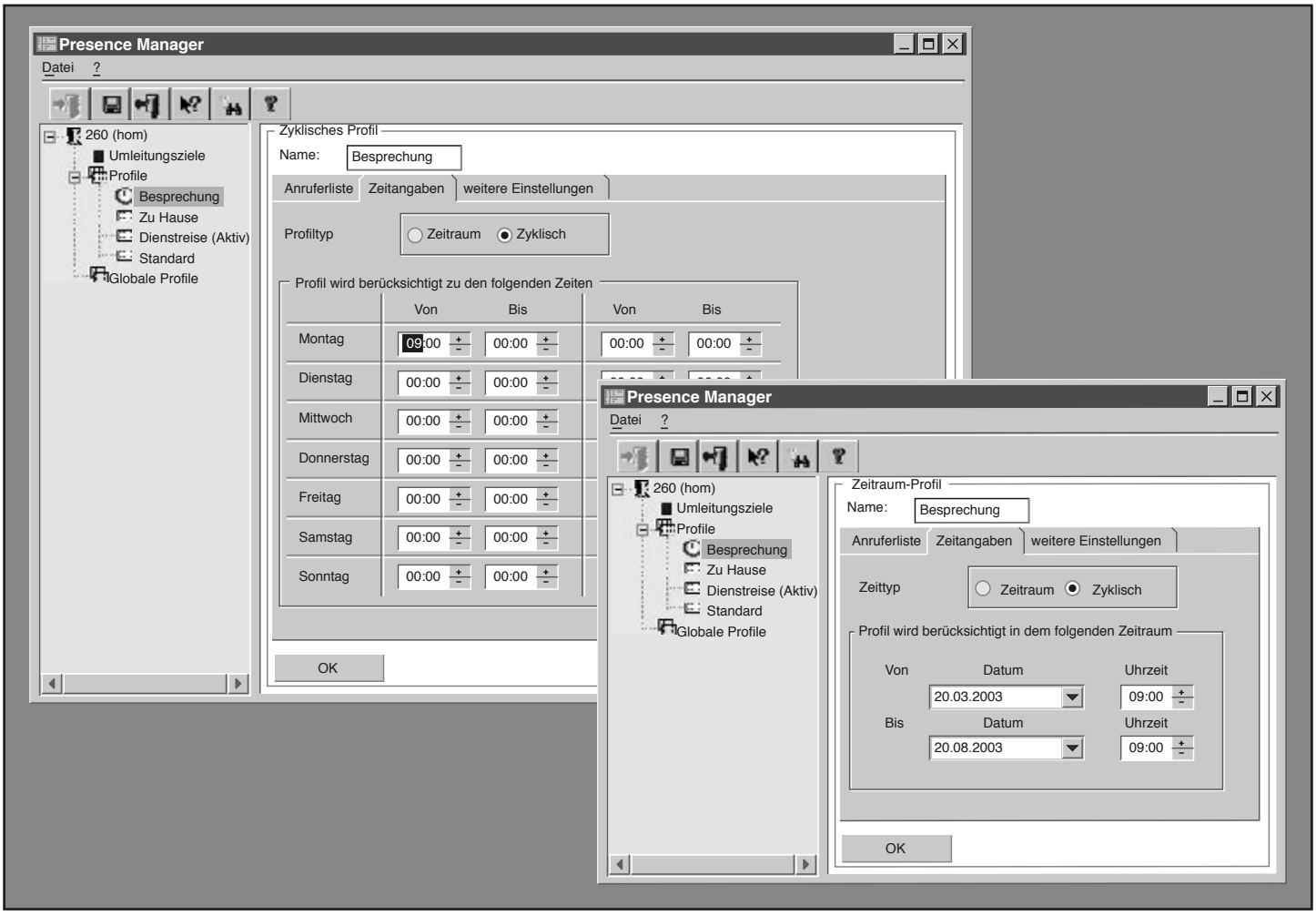


Bild 14

Zunächst definiert ein Anwender seine persönlichen Umleitungsziele, danach kann er mehrere statische oder zyklische Profile einrichten. Zuletzt definiert er bei welchen Anrufen und wann welche Profile gelten.

Richtet man sich zum Beispiel ein Profil „Besprechungen“ für eine täglich von 9 bis 9:30 Uhr stattfindende Statusbesprechung ein, so kann dieses Profil per Mausklick aktiviert werden und die Anrufe mit den hinterlegten Rufnummern werden in dieser Zeit automatisch zum Handy weitergeleitet. Alle anderen Gespräche gelangen zum Beispiel zur Voice-Mail. So kann sichergestellt werden, dass bestimmte Anrufe den Anwender immer erreichen, wenn er dies möchte.

Der Presence Manager, Telefonjournale, Adressbuch und einige andere Funktionen sind auch mittels WEB Snapware über den Internet-Explorer für den Anwender remote zugänglich.

Fazit

Die beschriebenen Funktionen geben nur einen geringen Teil der Leistungsfähigkeit des Cisco Call Managers in Kombination mit Unity und den Produkten der Firma Telesnap wider. Sie machen jedoch deutlich, dass dieses, rein in Software gegossene IP-Telefonsystem, den Vergleich mit einer klassischen TK-Lösung nicht scheuen muss.

In den Punkten Skalierbarkeit, Administration und Flexibilität hat diese Architektur klare Vorteile. Durch den Einsatz marktgängiger Server wird eine kontinuierliche Leistungssteigerung automatisch erzielt. Das Remote-Management ist durch die weitestgehend über den Internet-Explorer realisierte Administrationsoberfläche möglich und Sicherungs- und Backupverfahren entsprechen denen der vorhandenen Datenserver. Da alle Funktionen in Software gegossen sind und die Schnittstellen zugänglich sind, lassen sich gewünschte Funktionen leicht implementieren.

Ein erhebliches Einsparungspotential bietet ein Konzept mit zentralen Call Managern im Cluster-Verbund. In den Niederlassungen werden IP-Telefone und Gateways installiert, die Server stehen in der Zentrale des Unternehmens. Eine wesentliche Voraussetzung für dieses Konzept ist jedoch ein ausfallsicheres Weitverkehrsnetz mit Backup und entsprechender Bandbreite.

Die in diesem Bericht beschriebenen Anwendungen befinden sich im Rechenzentrum des Landes Nordrhein Westfalen im produktiven Betrieb. Seit Herbst 2002 wurden die Produkte der Telesnap erprobt. Die besonderen Schwerpunkte lagen in der blindengerechten Ausstattung der Telefonzentrale und in der Implementation von Anwendungen zur Unterstützung von Hotlines. Die Vollaustattung mit über 650 IP-Telefonen konnte nach dem erfolgreichen Einsatz der Telesnap-Anwendungen und der aktuellen Version des Call Managers im Laufe des dritten Quartals 2003 abgeschlossen werden.

Aktueller Kongress

Wireless LAN Forum 2003

Das Wireless LAN Forum 2003 vom 17.11. - 19.11.03 in Königswinter greift das momentan aktuellste Netzwerk- und Infrastrukturthema auf. Er analysiert den Einsatz von Wireless-Netzwerken in der Praxis, stellt Planungs-Methoden gegenüber, vergleicht die heutigen und zukünftigen Wireless-Varianten, bewertet die Produkt- und Marktsituation und gibt Empfehlungen zum Betrieb und zum Trouble Shooting.

Eine begleitende Ausstellung mit ausgewählten Themenschwerpunkten und Produktpräsentationen gibt parallel die Möglichkeit des Gesprächs mit wichtigen Herstellern.

Jeder Teilnehmer erhält kostenlos die neue Studie von ComConsult Research über „Sicherheit im Wireless LAN“ (Listenpreis: 298 Euro), die Anfang November erscheint und die neuesten Ansätze für ein sicheres WLAN analysiert und bewertet.

Auf diesem Forum erfahren Sie:

- wie Wireless-Technologien arbeiten, welche Alternativen es dabei gibt
- welche neuen Technologien in den nächsten 3 Jahren auf den Markt kommen und wie weit diese rückwärtskompatibel sind
- wie der Markt aussieht und wie er sich entwickelt
- was die neuen Produktansätze der Wireless Switches bringen, ob sie besser sind als der traditionelle Ansatz
- was sie über Funk- und Codierungs-Technik wissen müssen
- wie die verschiedenen Normungsansätze 11a, 11b, 11g zu bewerten sind

- wann und warum welche Produkte mit welcher Technologie zwischen den Herstellern interoperabel sind und wo dies zur Zeit nicht gesichert ist
- wie Sie erfolgreich eine flächendeckende Versorgung planen und realisieren können
- welche verschiedenen Planungsmethoden es gibt und welche für Sie am besten geeignet ist
- wie Sie eine Antenne technisch und wirtschaftlich optimal für Ihren Einsatzzweck auswählen
- wie die häufig diskutierten Sicherheits-Bedenken zu bewerten sind und wie Sie Ihre Installation sicher machen können
- was bei einer Installation in speziellen Umgebungen wie medizinische Bereiche oder Personalverwaltung oder Schule besonders zu beachten ist
- welchen hohen Stellenwert das Distribution-Netzwerk für eine flächendeckende Installation hat und wie Sie dabei die sehr häufig gemachten Auslegungsfehler vermeiden können
- warum sich Produkte im Preis zum Teil erheblich unterscheiden und welche Produkte besonders empfehlenswert sind
- wie sich typische Produkte des Marktes im Labortest verhalten und was das für die tägliche Praxis bedeutet
- in welchem Umfang eine kabelbasierte Lösung durch ein WLAN abgelöst werden kann und wie weit das sinnvoll ist
- ob Telefonie im WLAN eine echte Perspektive ist und warum dieses Thema spannend ist

Die Themenschwerpunkte und Livepräsentationen der begleitenden Ausstellung gehen auf folgende Themen ein:

- Wireless Switches: wie sie arbeiten, was sie leisten
- Zentrale Konfiguration großer Mengen an Access Points
- Messtechnik und Trouble Shooting: was leisten Messgeräte
- Sicherheits-Risiko WLAN: Live-Hack im WLAN, Diskussion und Präsentation der neuesten Studie von ComConsult Research
- Kabel kontra WLAN: Kostenszenarien und Trendanalyse
- IP-Telefonie im WLAN

Versäumen Sie nicht, sich jetzt noch einen Platz auf dieser herausragenden Sonder-Veranstaltung zu sichern.

Die Referenten sind Dr. Franz-Joachim Kauffels, Dr. Jürgen Suppan (ComConsult-Research), Peter Mohn, Dr. Simon Hoff, Dr.-Ing. Behrooz Moayeri und Dr. Joachim Wetzlar (ComConsult Beratung und Planung GmbH) Andreas Schlechter (TGS Telonik/Trapeze Network) und Mathias Wietrychowski (Cisco Systems Deutschland).

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Wireless LAN Forum

☐ Ich melde mich an zum
Wireless LAN Forum 2003
in Königswinter vom 17.11. - 19.11.03
zum Preis von € 1.690,-- zzgl. MwSt.

☐ Buchen Sie für mich ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Wireless LAN Forum 2003: Die Inhalte

Motivation, Bedarf und Wirtschaftlichkeit
- Typische mobile Nutzungssituationen
- WLAN-Technologie heute: wo stehen wir, was sind die Alternativen
- Das Notebook im WLAN
- Flächendeckung kontra Spot-Anwendung
- Kabel kontra Wireless: wie weit kann der WLAN-Einsatz gehen
- Anforderung an eine Lösung
- Typische Probleme beim Einsatz von WLAN
- WLAN und die Übertragung von Personaldaten

WLAN-Technologie: neueste Entwicklungen und Grenzen des bisherigen Verfahrens
- Grundlagen
- HTSG und die Konsequenzen für die Zukunft
- Die besondere Bedeutung der a-Variante
- Welcher Durchsatz ist in Zukunft erreichbar
- OFDM: Arbeitsweise und Konsequenzen für die Praxis
- Der Medienzugang CSMA/CA und seine Grenzen im Betrieb mit vielen Teilnehmern
- Ausblick

Sicherheit in Wireless LANs: Alternative Lösungsansätze, pro und kontra
- Analyse der Sicherheitsrisiken
- Das Sicherheitskonzept von IEEE 802.11
- Beispiele für typische Angriffsszenarien
- Life-Hack des WEP-Schlüssels
- Alternative Lösungen und ihre Bewertung
- WPA, 802.11i: jetzt nutzbar?
- VPN: der richtige Weg?
- IEEE 802.1x
- Server-Infrastruktur kontra einfache Lösung
- Wo hoch sind die Betriebsaufwände
- Gibt es eine komplett sichere Lösung?
- Wie sicher ist CISCOs LEAP, was ist zu tun
- Ausblick und Empfehlungen

Rahmenbedingungen für die erfolgreiche Nutzung von WLANs
- Reichweiten
- Störpotenziale
- Störungen und Instabilitäten im WLAN: Ursachen und Vermeidung
  – Warum WLANs unstabil sein können
  – Wie das durch eine gute Planung vermieden werden kann
- Messergebnisse
- Tuning und Optimierung: was leisten die diversen Protokoll-Parameter, sollten sie in der Praxis genutzt werden oder nicht
- Empfehlungen für die erfolgreiche Nutzung von WLANs

WLAN-Technologien im Vergleich: was sie leisten, wo welche Variante optimal ist, wo die Zukunft liegt
- 11a, b, g, h: wo liegen die Unterschiede
- Was bedeuten die Auflagen der RegTP
- Für wen und für welche Anwendung ist welche Variante geeignet
- Wie weit sind die Varianten kompatibel zueinander

Architektur-Varianten und Planungsmethoden im Vergleich
- Flächendeckung kontra Hot-Spot
- Anbindung/Erweiterung bestehender Kabel-LANs
- Integriert oder separat: wie sieht das optimale Distribution Netzwerk aus
- K.O.-Kriterium Layer-3-Mobility
- Planungsansätze:
  – Capacity
  – Coverage
  – Quality
- Worin unterscheiden sich Planungsansätze
- Von der Nachrichtentechnik zur Realität: Einmessung- und Berechnungsverfahren für WLAN-Planungen

Antennenauswahl und Montage von Access Points
- Ergebnisse eines Labortests mit gängigen Antennen
- Einfache Dipolantenne kontra Spezial-Richt-/Verstärker-Antenne: was leisten sie? Wie hoch ist die Mehrleistung?
- Wie hoch sind Leistungs- und Qualitätsunterschiede zwischen den angebotenen Antennen
- Worauf bei der Installation an Access Points zu achten ist, welche typischen Fehler bis zu 80% der Leistung vernichten können
- Hinweise und Empfehlungen zur Montage

Einmessung, Abnahme, Trouble Shooting: Methoden, Werkzeuge, Erfahrungen
- Messmethoden
- Welche Werkzeuge bietet der Markt, was kosten sie, was ist sinnvoll
- Welche Parameter sollten gemessen werden
- Wie kann die Stabilität einer Flächenversorgung messtechnisch unterstützt werden
- Betrieb eines WLAN: welche Parameter sollten überwacht werden, wie aussagekräftig sind die Status-Anzeigen von Access Points und Adapterkarten
- Was kann aus den WLAN-typischen Protokoll-Parametern und Countern geschlossen werden

WLANs in der Fertigungs- und Automatisierungstechnik
- Anforderungen der Industrie: Fertigungs- und Automatisierungstechnik im Fokus
- Was ist anders, wie sieht die Umgebung aus
- Typische Anwendungen und Applikationen
- Kundennutzen
- Wie sehen geeignete Lösungen aus

Markt- und Produktsituation
- Was leisten die Produkte
- Welche Produkttypen gibt es
- Welche Neuentwicklungen und Trends gibt es
- Schlüsselfrage Interoperabilität: wie kann diese erreicht werden
- QoS, VLAN: wird das wirklich gebraucht
- Markt- und Produktübersicht
- Wie positionieren sich die Hersteller
- Wie entwickeln sich die Preise

Wireless Switches kontra traditionelle Access Points: wer leistet mehr, wohin entwickeln sich Produkte?
- Wie arbeiten Wireless Switches, welche Varianten gibt es, was leisten sie
- Wireless Switches kontra Access Punkt mit zentraler Konfigurations-Software: was ist besser?
- Betrieb und Sicherheit einer Wireless-Installation in der Praxis

Von der Konfiguration zum Betrieb großer Mengen an Access Points: WLANs beherrschen mit WLSE von Cisco
- Was ist WLSE
- Warum wird eine zentrale Konfiguration benötigt
- Wie sieht ein typisches Einsatzszenario aus
- Wo liegen die Unterschiede zum Wireless Switch

Wireless-Switches: Optimierter Betrieb von Wireless-Netzwerken durch Einsatz neuer Technologien
- Nachteile traditioneller Access Points
- Neue Architekturen
- Integration Switch- und Wireless-Technologie
- Arbeitsweise der Produkte
- Vorteile für den Kunden

Mobile Clients im WLAN
- Virtualisierungstrend
- Mit WLAN möglich: standortunabhängige Kommunikation
- Lösung für Gäste-Notebooks
- Lösung für eigene mobile Clients
- Erforderliche Sicherheitsmechanismen

Der Veranstalter behält sich Änderungen im Programm vor.

Studie des Monats

Voice over IP: Zeitverzug (Delay)

Aus dem ComConsult Research Voice over IP Report*

Auch die originalgetreue Wiedergabe eines Sprachsignals wird von Menschen als qualitativ schlecht bewertet, wenn sie erst nach einem zu großen Zeitverzug erfolgt. Die dabei maßgebliche Grenze ist bei jedem Menschen individuell unterschiedlich. Die Feststellung dieser Grenze ist Gegenstand aufwendiger Studien (z. B. des ITU-Dokuments G.114, „One Way Transmission Time). Nach diesen Studien empfinden die meisten Benutzer Verbindungen mit Round-Trip-Delays von mehr als 300 ms als eine Art „Wechselsprechen“ und nicht als interaktives Gespräch. Bei empfindlichen Benutzern liegt diese Grenze bei 150 ms oder gar niedriger, während weniger empfindliche Benutzer auch Verzögerungen von 300 bis 800 ms als nicht störend empfinden.

Maßgeblich für die Aufstellung eines so genannten Delay Budgets für einen Netzbetreiber ist jedoch die Grenze 300 ms für die Signalumlaufzeit, d. h. 150 ms für den Weg vom Sprecher zum Hörer.

Dies bedeutet, dass innerhalb dieser 150 ms folgende Schritte durchgeführt werden müssen:

1. Das Signal muss abgetastet und der Bitstrom generiert werden. Die dazu erforderliche Zeit ist vernachlässigbar, so dass man von einer reinen Digitalisierung in Echtzeit ausgehen kann.

2. Das Signal muss komprimiert werden. Einige Kompressionsalgorithmen verzögern das Signal bei der Kompression, um Korrelationseffekte auszunutzen. Diese Verzögerung wird „look-ahead delay“ genannt.

3. Die Paketbildung ist mit einer weiteren Verzögerung verbunden, da so viele Bits abgewartet werden müssen, wie es für die Bildung eines Paketes erforderlich ist.

4. Die Übertragung des Paketes auf das Netz ist mit einer weiteren Verzögerung verbunden.

5. Im Netz wird das Paket durch die reine physikalische Signallaufzeit verzögert. Dieser Parameter ist entfernungsabhängig. Es gilt die Näherungsformel „pro 200 km eine Millisekunde“.

6. Die Warteschlangen in den Netzkomponenten tragen in Abhängigkeit von der Netzauslastung zusätzlich zum Zeitverzug bei.

7. Da die Laufzeit der Pakete in einem Netz unterschiedlich lang ist, muss auf der Empfängerseite ein Puffer dafür sorgen, dass dem Decoder ein kontinuierlicher Bitstrom übergeben wird. Ansonsten würde der Decoder ein verzerrtes akustisches Signal generieren. Die Puffertiefe ist von der Laufzeitschwankung der Pakete im Netz abhängig und trägt wiederum zur Gesamtverzögerung bei.

8. Aus den empfangenen Paketen wird ein kontinuierlicher Bitstrom erzeugt. Dieser Schritt beinhaltet bei komprimierter Übertragung auch eine Dekompression.

9. Aus dem Bitstrom wird das akustische Signal gewonnen. Die dazu erforderliche Zeit ist vernachlässigbar, so dass man von der Signalgenerierung in Echtzeit ausgehen kann.

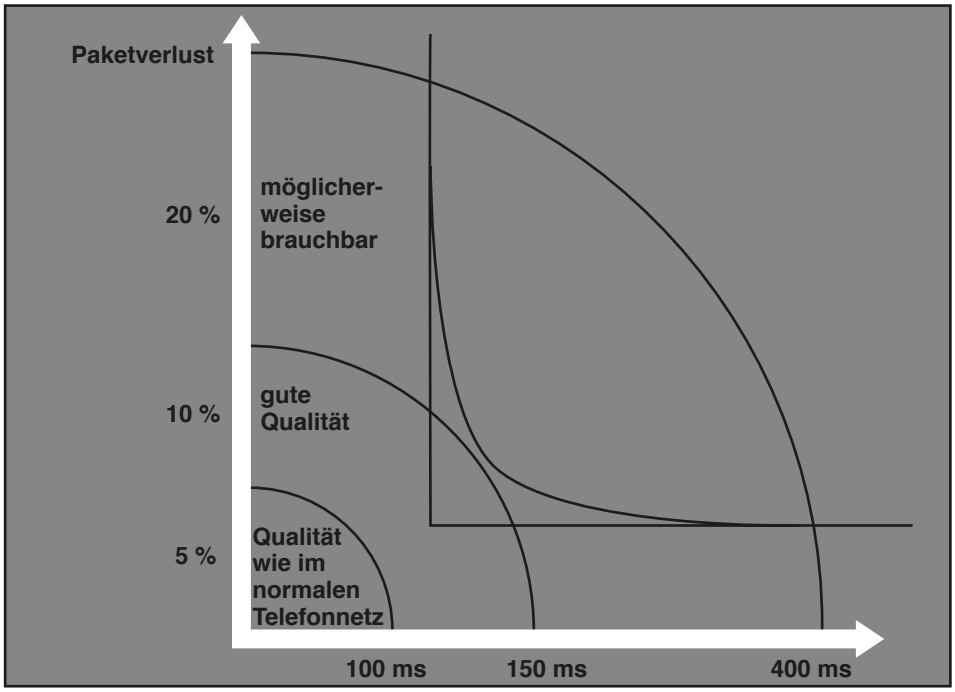
Die Schritte 2, 3 und 8 sind vom Kompressionsalgorithmus abhängig. Bei der Diskussion verschiedener Codec-Standards werden die entsprechenden Werte erwähnt.

Der Schritt 4 ist in einem geswitchten Netz, das zur Übertragung von VoIP vorausgesetzt wird, auf die interne Verarbeitungszeit im sendenden Endgerät beschränkt (Zugriffszeiten beim internen Bussystem etc.). Der Schritt 5 ist entfernungsabhängig und exakt quantifizierbar.

Allein die Schritte 6 und 7 erzeugen einen variablen, schwer vorzubestimmenden Anteil an Verzögerung (Delay). Dieser Anteil ist im Wesentlichen von der Auslastung der Netze auf der Strecke vom Sender zum Empfänger abhängig. Je höher die Auslastung, desto größer die Paketlaufzeit. Aber der Schritt 6 ist selbst bei einer Auslastung von 0% mit einem endlichen Verzögerungsanteil verbunden, da jede Netzkomponente auch bei 0% Auslastung eine nicht infinitesimale Zeit für die Verarbeitung des Paketes benötigt. Man kann von der Faustregel ausgehen, dass pro Netzkomponente (Switch oder Router) eine Millisekunde als Verzögerung zu berücksichtigen ist.

Es gibt einen Zusammenhang zwischen Delay, Paketverlust und Sprachqualität. Dieser Zusammenhang ist in Bild 1 schematisch dargestellt.

Bild 1: Zusammenhang zwischen Delay, Paketverlust und Sprachqualität



* Voice over IP, ComConsult Research Technologie Report,
zu beziehen über den Verlag ComConsult Technologie Information (weitere Informationen unter **www.comconsult-research.com**)

Voice over IP: Zeitverzug (Delay)

Auf der horizontalen Achse ist der Delay dargestellt, auf der vertikalen Achse die prozentuale Verlustrate bei den Paketen. Je nach Kombination dieser beiden Werte ist die Sprachqualität sehr gut, gut oder bedingt brauchbar. Ist die Laufzeit des Signals sehr klein, können mit aufwändigen Dekodierungsmaßnahmen die Paketverluste ausgeglichen werden, so dass auch bei relativ hohen Paketverlusten eine gute Qualität des Sprachsignals sicherzustellen ist. Dieser Spielraum sinkt mit steigenden Delay-Werten.

Andererseits ist bei sehr niedrigen Paketverlustraten eine aufwändige Kodierung nicht erforderlich, sodass mehr Spielraum für Netzdelay übrig bleibt. Dieser Spielraum sinkt mit steigender Paketverlustrate, die vom Codec ausgeglichen werden muss.

Nun stelle man sich vor, man arbeite mit einem Netz, das in der Lage ist, 97% der Pakete innerhalb einer Zeit von 110 ms zu befördern. Die „Koordinaten" dieses Punktes N, der von den Eigenschaften des Netzes abhängt, sind in der Abbildung 11 dargestellt. Zusätzlich zu dem vom Netz verursachten Delay und Paketverlust können andere Komponenten wie Codec bis zu bestimmten Grenzen Delay und Paketverlust verursachen. Im dargestellten Beispiel kann z. B. ein Codec eingesetzt werden, der für Kodierung und Dekodierung insgesamt circa 30 ms brauchen würde, ohne die gute Sprachqualität zu beeinträchtigen.

Bestimmte Bestandteile der Verzögerung sind fest, und zwar in der Regel jene Bestandteile, die mit der Kodierung und Dekodierung zusammenhängen. Die durch das Netz verursachte Verzögerung ist jedoch variabel. Das führt dazu, dass die vom Kodierer erzeugten Pakete unterschiedlich schnell beim Dekodierer ankommen. Der Dekodierer ist jedoch auf einen quasi kontinuierlichen Paketstrom angewiesen, um auch einen kontinuierlichen Bitstrom als Voraussetzung für ein nicht verzerrtes Audiosignal generieren zu können. Daher müssen zum Ausgleich der Laufzeitschwankungen im Netz Puffer an Empfängern implementiert werden. Beispiel: Beträgt die Laufzeitschwankung im Netz 10 ms, müssen die ankommenden Pakete für genau diese Zeit zwischengespeichert werden. Man stelle sich vor, auf ein besonders „schnelles" Paket folgt ein besonders „langsames" Paket. Die Ankunftszeit dieser beiden Pakete wird dann um maximal 10 ms länger auseinander liegen als die Zeit zwischen der Generierung des ersten und der Generierung des zweiten Paketes. Das erste Paket muss daher künstlich um 10 ms verzögert werden, wofür der Zwischenspeicher sorgt.

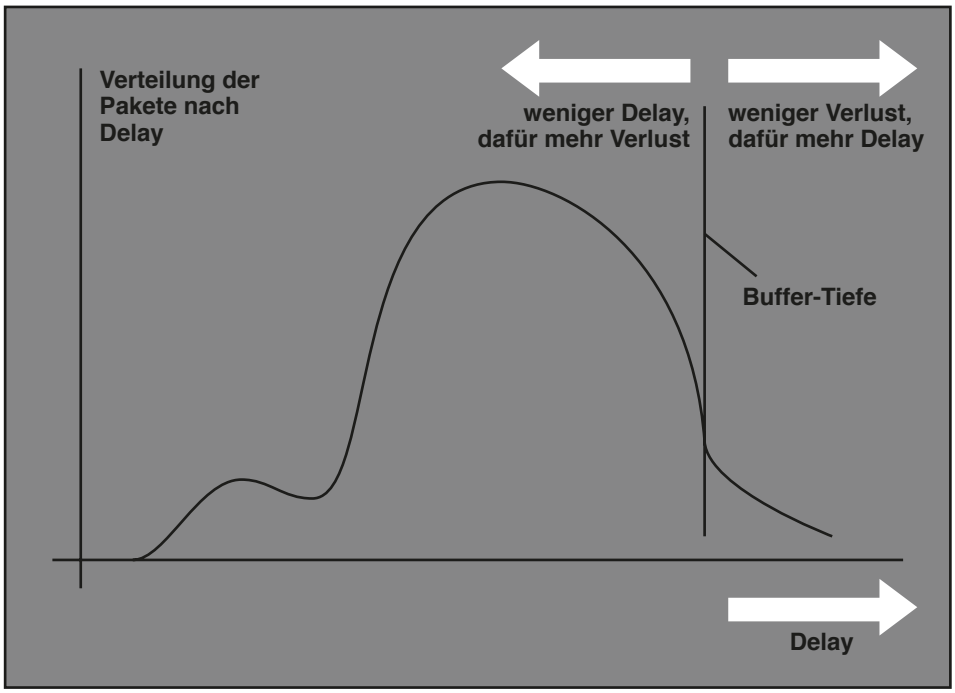


Bild 2: Wechselwirkung der Zwischenspeicherung und der Paketverlustrate

Zwischenspeicher können daher Jitter (Laufzeitschwankung) ausgleichen, aber nur auf Kosten der gesamten Verzögerung. Nun gibt es einen gewissen Spielraum für die Dimensionierung des Zwischenspeichers dadurch, dass die gängigen Kodierungsverfahren eine gewisse Paketverlustrate tolerieren. Wird diese Rate nicht überschritten, kann das Sprachsignal noch mit akzeptabler Qualität dekodiert werden. Codecs müssen in diesen Fällen die Paketverluste ausgleichen (loss concealment). Zum Beispiel wird beim Kodierungsverfahren gemäß dem Standard G.723.1 bei einem Paketverlust der letzte Frame in gedämpfter Form wiederholt. Tests zeigen, dass bei hinsichtlich loss concealment besonders ausgereiften Kodierungsverfahren bis zu 10% unkorrelierter Verlust wenig Einfluss auf die Qualität der Sprachübertragen hat. Unkorrelierter Verlust liegt dann vor, wenn z. B. keine längeren Paketverlustphasen (loss bursts) vorkommen.

Daher kann man den Zwischenspeicher kleiner dimensionieren als die größte annehmbare Laufzeitschwankung und somit die wenigen „langsamsten" Pakete ignorieren. Pakete, die später ankommen als der eingestellte Jitter-Ausgleich erlaubt, gelten als verloren. Ist der Zwischenspeicher zu klein, führt eine zu hohe Verlustrate zur Beeinträchtigung der Signalqualität.

Die Wechselwirkung der Zwischenspeicherung der Pakete und der Verlustrate ist in der Bild 2 dargestellt.

Aus dieser Darstellung geht ein Histogramm hervor, das die Verteilung der Pakete nach Delay zeigt. Links im Bild ist die Häufigkeit der Pakete dargestellt, die einen kürzeren Weg durch das Netz nehmen und schneller am Ziel ankommen, rechts im Bild die Häufigkeit solcher Pakete, die langsamer sind. Würden alle Pakete ohne Delay ankommen, bräuchte man keinen Zwischenspeicher. Da die Laufzeitunterschiede der Pakete jedoch ungleich Null ist, wird ein Zwischenspeicher benötigt. Ab einer bestimmten Tiefe dieses Speichers empfängt der Dekodierer alle Pakete. In der Abbildung 12 würde dies bedeuten, dass der senkrechte Strich ganz rechts im Bild platziert wird und somit alle Pakete (dargestellt als die Fläche unterhalb der Kurve) dem Dekodierer zugeführt werden. Dies ist gleichbedeutend mit minimalem Paketverlust, jedoch einem großen Delay durch Jitter-Ausgleich.

Bewegt man den senkrechten Strich nach links, verkleinert man den Zwischenspeicher, wodurch man den Delay minimiert. Damit geht jedoch der Verlust aller Pakete einher, deren Anteil mit dem Anteil der Fläche unterhalb der Kurve und rechts vom senkrechten Schritt korrespondiert. Dieser Anteil darf den maximal vom Dekodierer tolerierbaren Verlust nicht überschreiten.

Einige Codecs können diese Tuningmaßnahme dynamisch vornehmen und somit einen optimalen Ausgleich zwischen Verlustminimierung und Delay-Minimierung finden

Neben dem Jitter-Ausgleich trägt die Synchronisation zur Erhöhung des Gesamtdelays bei. Eine Synchronisation ist deshalb erforderlich, weil nicht sichergestellt ist, dass die Uhren von Sender und Empfänger mit dem absolut gleichen Takt arbeiten. Ohne Synchronisation würde ein Empfänger, der mit einer langsameren Uhr als die des Senders arbeitet, von den ankommenden Paketen „überrollt" werden. Ein Empfänger mit einer schnelleren Uhr als die Uhr des Senders würde die Pakete zu schnell verarbeiten und das Problem von zeitweise ausbleibenden Paketen verursachen, was wiederum zu einem verzerrten Audiosignal führen würde.

Zur Vermeidung solcher Situationen wird die Synchronisation gemäß Bild 3 implementiert.

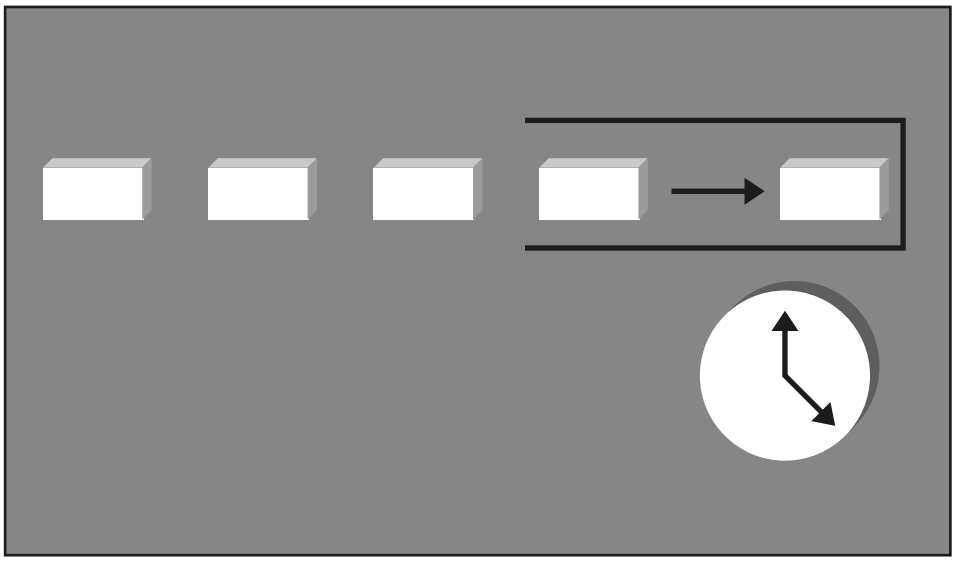


Bild 3: Synchronisation durch Zwischenspeicherung

Damit muss sich der Empfänger mit dem Sender synchronisieren. In den Paketen ist dazu ein Zeitstempel vorhanden, der mit der eigenen Uhr verglichen wird. Kommen die Pakete schneller an, werden sie zwischengespeichert. Die Entnahmegeschwindigkeit der Pakete aus diesem Zwischenspeicher richtet sich danach, ob der Füllungsgrades des Zwischenspeichers bestimmte Schwellwerte unter- bzw. überschreitet.

Jitter-Ausgleich und Synchronisation tragen somit zum Gesamtdelay bei und müssen beim Delay-Budget berücksichtigt werden. Ein beispielhaftes Verzögerungsbudget ist in der Bild 4 dargestellt:

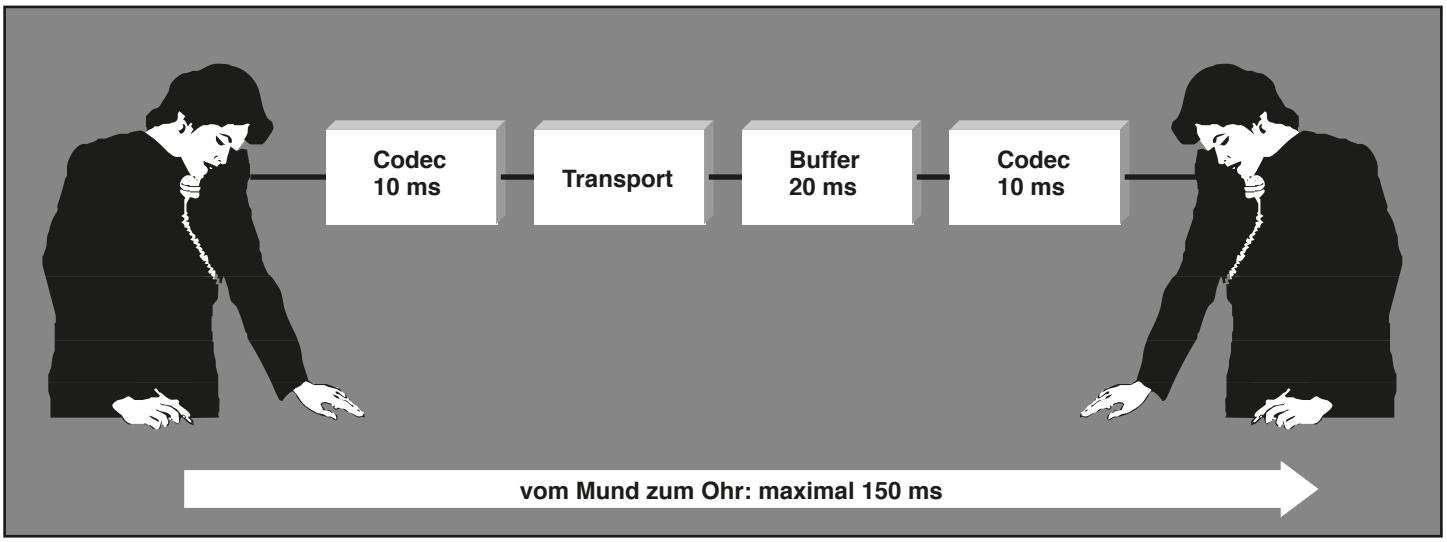
Werden die Pakete verschlüsselt übertragen (z. B. über ein Virtual Private Network – VPN), müssen die Ver- und Entschlüsselungszeiten zusätzlich berücksichtigt werden.

Um die einzigen variablen und schwer planbaren Anteile, nämlich die Wartezeit in den Netzkomponenten und im Zwischenspeicher des Empfängers, als konstante Anteile erfassen zu können, sind zwei Methoden denkbar:

- Die VoIP-Pakete werden priorisiert und von jeder Netzkomponente vor allen anderen Anwendungsdaten übertragen. Somit ist die Verweildauer der VoIP-Pakete in den Warteschlangen der Netzkomponenten gleich der minimalen Verarbeitungszeit eines IP-Paketes. Die Laufzeitschwankungen werden ebenfalls auf ein Minimum reduziert.
- Die Netzkapazität wird auf ein solches Maß erhöht, dass sich keine Warteschlangen in den Netzkomponenten bilden.

Die Vor- und Nachteile der beiden Ansätze werden in der QoS-Diskussion seit Jahren gegenübergestellt. Als Ergebnis dieser Diskussion (Voice over IP Report, Abschnitt 3.14) kann festgehalten werden, dass solange mit vertretbarem Aufwand Netzkapazität im Überfluss bereitgestellt werden kann, der zweite Ansatz zu empfehlen ist, ansonsten der erste Ansatz. In der Regel ist der erste Ansatz in WANs erforderlich, während in LANs der zweite Ansatz angewandt wird.

Bild 4: Exemplarisches Delay Budget



Aktueller Report

Studie des Monats: Voice over IP – Anforderungs-Katalog und Evaluierung

Der Markt ist reif für VoIP:

- Fast alle TK-Hersteller haben ihre Produkte mit VoIP-Fähigkeiten versehen.
- Viele der zukünftigen Multimedia-Anwendungen werden auf VoIP-Diensten basieren.
- Mehr und mehr Anwender integrieren VoIP in ihr Lösungs-Portfolio.
- Die Produkte schwenken auf SIP um, eine wesentliche Voraussetzung für eine genormte TK-Funktionalität.
- Die Kosten für VoIP-Lösungen sinken.

Trotzdem ist eine Entscheidung für Voice over IP nicht leicht. Immer noch gibt es eine Reihe ernstzunehmender Kriterien, die auch gegen einen Voice-over-IP-Einsatz sprechen können. Hier setzt der Report "Voice-over-IP: Evaluierung" an. Dieser Report zeigt Ihnen:

- was hinter Voice-over-IP steckt
- nach welchen Kriterien eine Entscheidung für eine neue TK-Lösung fallen sollte
- wie sie bei der Auswahl einer neuen TK-Lösung vorgehen können
- wie eine VoIP-Lösung nach diesen Kriterien zu bewerten ist
- wo die Schwachstellen einer VoIP-Lösung liegen
- was hinter dem Normungsstreit SIP kontra H.323 steckt
- wie der Markt einzuschätzen ist
- wie die Kosten einer traditionellen TK-Lösung gegenüber VoIP zu bewerten sind
- wo wichtige Hersteller wie Avaya, Alcatel, CISCO, Nortel und Siemens stehen

Dabei wird auch auf folgende Fragen eingegangen:

Mit welchen Vor- und Nachteilen sind IP-PBX-Lösungen zum jetzigen Zeitpunkt hinsichtlich Leistungsmerkmale, Sicherheit, Verfügbarkeit, Skalierbarkeit etc. verbunden?

Welche Vorteile bieten IP-PBX-Systeme für Unified Messaging und Call-Center-Anwendungen?

Stellt das Ersetzen des Zweidrahttelefons mit einem kleinen Display und einer numerischen Tastatur durch ein IP-Telefon mit einem etwas größeren Display und einer numerischen Tastatur für den Anwender eine ausreichende Motivation dar, zu VoIP zu migrieren?

Was muss die Zielsetzung der VoIP-Migration sein?

Wie weit sind wir von einer offenen, standardisierten Welt im Bereich VoIP entfernt?

Was ist der Migrationspfad zum Erreichen der offenen, standardisierten Umgebung?

Ausblick auf Signalisierungsstandards und Verbesserung der Leistungsmerkmale der IP-PBX-Lösungen, z. B. durch Verfügbarkeit neuer Applikationen, deren Einsatz im Unternehmen sinnvoll und vorgesehen sind.

Dieser Report setzt sich kritisch mit dem Thema Voice over IP auseinander. Er zeigt, wann ein Einsatz sinnvoll ist und wann sie mit ihrer Entscheidung noch warten sollten.

Für jeden, der in der Entscheidung für eine neue TK-Lösung steht, ist dieser Report ein unverzichtbares Hilfsmittel.

Der Autor, Dr. Behrooz Moayeri ist Mitglied der Geschäftsleitung der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrungen zurück. Er verfügt über mehr als 10 Jahre Beratungspraxis für Netzwerk-Technologien und ist spezialisiert auf Integration von Sprache und Daten, Redesign bestehender Netzwerke und Fehlersuche.

Fax-Antwort an ComConsult 02408/955-399

Bestellung Voice over IP

☐ Ich bestelle den Research Report
Voice over IP
(Preis € 398,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Bestellen Sie auf unsere Web-Seite
www.comconsult-research.com

Schwerpunktartikel November 2003, Thema 1

Problematische VPN-Aspekte – Redundanz

1. Teil der Fortsetzung von Seite 1

Dipl.-Inform. Andreas Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

„Ausfallsichere VPNs: zuverlässig und kostengünstig“

Je stärker sich Unternehmen auf IT-basierte Arbeitsabläufe stützen, desto essentieller wird die Frage nach der Verfügbarkeit der dazu notwendigen Ressourcen. Diese Frage stellt sich naturgemäß auch bei der Realisierung von VPNs.

Dieser Artikel versucht, Anregungen zur Klärung der VPN-seitigen Aspekte zu geben. Natürlich ist eine zuverlässige Weitverkehrsverbindung aus Sicht der Geschäftsprozesse nur die halbe Miete: auch die im Zugriff befindlichen Ressourcen und das lokale Netzwerk, in dem sich diese Ressourcen befinden, muss hinreichende Verfügbarkeitswerte aufweisen.

Alle diese Aspekte zu behandeln würde jedoch den Rahmen dieses Artikels bei weitem sprengen – inhaltlich als auch mit Blick auf den Umfang. Eine recht ausführliche Diskussion ausfallsicherer IT-Strukturen, insbesondere mit Blick auf Server-Systeme, findet sich z.B. in einem entsprechenden aktuellen Report der ComConsult Technologie-Information*.

Will man seine VPN-basierten WAN-Verbindungen weitestgehend ausfallsicher gestalten, so sind hierzu verschiedenste Ansätze denkbar, die sich zum Teil auch unmittelbar in den Features marktverfügbarer Produkte widerspiegeln. Hierunter fallen Cluster-Lösungen für VPN-Gateways ebenso wie die Nutzung von IP-Routing-Mechanismen wie HSRP. Unabhängig von den letztlich implementierten Mechanismen ist jedoch zunächst ein wesentlicher Grundsatz des Designs ausfallsicherer IT-Strukturen zu berücksichtigen:

Da jede Kette maximal nur so stark ist wie ihr schwächstes Glied, reicht es nicht aus, punktuelle Maßnahmen zu ergreifen, sondern die Kommunikationskette in ihrer Gesamtheit muss durch entsprechende Maßnahmen abgesichert werden. Der Gewinn einer einzelnen Maßnahme – gemessen als Steigerung der Verfügbarkeitswerte der Gesamtlösung – ist dabei umso größer, je anfälliger das Zielobjekt der Maßnahme ist. Es empfiehlt sich daher, das Augenmerk primär auf diejenigen Elemente der Kommunikationskette zu richten, die das höchste Ausfallrisiko aufweisen.

* Serverfarmen, ComConsult Research Technologie Report,
zu beziehen über den Verlag ComConsult Technologie Information (weitere Informationen unter **www.comconsult-research.com**)

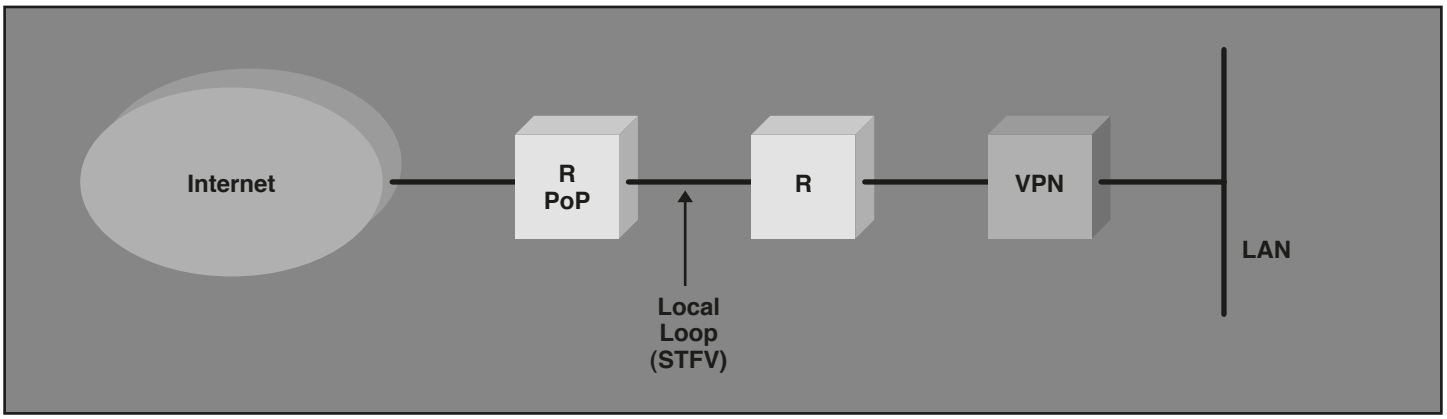


Bild 1: VPN-Anbindung ans Internet

Der Local Loop als Ansatzpunkt

Im Fall von VPN-Lösungen sind dies in aller Regel die physikalischen WAN-Strecken zwischen dem eigenen Netz und dem Trägernetz des VPNs, bei Internet-gestützten VPNs also die Verbindung zum PoP des ISPs (Local Loop). Die zugesicherte Verfügbarkeit einer Standard-Festverbindung der Deutschen Telekom liegt beispielsweise bei ca. 98%, das entspricht einer durchschnittlichen Ausfallzeit von 7 Tagen und 7 Stunden pro Jahr. Demgegenüber erreichen z.B. hardwarebasierte Netzwerk-Systeme (Router, VPN-Boxen, etc.) deutlich höhere Verfügbarkeitswerte (ein Ansatz von 99,9% erscheint hier eher zu konservativ als zu mutig...).

Die Gültigkeit des Grundsatzes „Je unzuverlässiger ein Bestandteil der Gesamtlösung ist, desto effektiver wirken sich Maßnahmen zur Verfügbarkeitssicherung aus“ verdeutlicht ein einfaches Beispiel:

Wir betrachten die Verfügbarkeit einer VPN-Anbindung; der Einfachheit halber betrachten wir nur eine Seite der Kommunikationsbeziehung und vernachlässigen die Providerstruktur im IP-Trägernetzwerk vollständig. Diese Anbindung bestehe vereinfacht dargestellt aus einem VPN-Gateway, einem WAN-Router und einer Standard-Festverbindung zur Anbindung an den nächsten PoP des Providers (Bild 1).

Für die so skizzierte VPN-Anbindung an den ISP ergeben sich auf Basis obiger Verfügbarkeitsannahmen folgende jährliche Netzausfallzeiten:

- Jährliche Ausfallzeit (je Lokation): ca. 184 h
- Redundantes VPN-Gateway verringert Ausfallzeiten auf ca. 175 h (= ca. 5% Reduktion)
- Redundanter WAN-Link verringert Ausfallzeiten auf ca. 12 h (= ca. 93% Reduktion)
- Vollredundante Auslegung verringert Ausfallzeiten auf ca. 3,5 h (= ca. 98% Reduktion)

Man erkennt leicht, dass die redundante Hardware die Ausfallzeiten nahezu überhaupt nicht, der redundante WAN-Link hingegen deutlich spürbar verringert. Insofern sollten Redundanzmaßnahmen bevorzugt im Bereich der Anbindung an das VPN-Trägernetz ansetzen, d.h. dass beispielsweise der Local Loop zum PoP des Internet-Providers durch geeignete Maßnahmen redundant ausgelegt werden sollte.

Problematische VPN-Aspekte – Redundanz

Redundanzmaßnahmen

In der Regel sollen VPNs aus den eingangs angeführten Gründen mit hohen Verfügbarkeitswerten aufwarten können. VPN-Knotenpunkte mit zentraler Bedeutung für die IT-Gesamtstruktur – etwa der Standort des unternehmenszentralen Rechenzentrums – bedürfen in jedem Fall Anbindungen, die mittels geeigneter Redundanzmechanismen hochverfügbar ausgelegt sind. Für sonstige Standorte kommen – je nach Bedeutung einer Lokation und daraus ableitbarer Verfügbarkeitsanforderung – neben vergleichbaren Hochverfügbarkeitslösungen auch Backup-Ansätze in Betracht. Hierunter sind in aller Regel leistungsschwächere bedarfsweise aktivierte Verbindungen zu verstehen (z.B. Dial-Backup per ISDN), die zumindest eine Notfall-Versorgung der wichtigsten Anwendungen sicherstellen.

Für die Gewährleistung einer hohen Verfügbarkeit von VPN-Gateways existieren verschiedene Ansätze:

- Einsatz von Cluster-Lösungen
- Einsatz von Failover-Lösungen
- Einsatz von Routing-Mechanismen
- Einsatz von Load-Balancern
- Bereithaltung von vorkonfigurierten Reservegeräten
- Wartungsvertrag mit zugesicherten Fehlerbehebungszeiten

Offenbar (s.o.) bedarf insbesondere der vergleichsweise fehleranfällige WAN-Link ebenfalls einer ausreichenden Ausfallsicherung.

Hierzu sind folgende Varianten denkbar:

- Redundanter WAN-Link
- Wählbackup für den WAN-Link
- Wählbackup „Around the Cloud“

Im Folgenden sollen nun die einzelnen Ansätze kurz betrachtet und insbesondere deren jeweilige wesentliche Vor- und Nachteile beleuchtet werden.

Absicherung der VPN-Geräte mittels Cluster

Dieser Lösungsansatz verwendet entweder eine im VPN-Gateway eingebaute Cluster-Option oder eine zusätzliche Software. Dabei stellt sich das Cluster nach außen als ein einziges virtuelles VPN-Gateway dar; die Verteilung der Datenströme auf die realen Gateways wird durch die Cluster-Steuerung vorgenommen.

Vorteile dieses Ansatzes liegen vor allem im Bereich Load-Sharing bzw. Load-Balancing; neben der dadurch möglichen Erhöhung der Leistungsfähigkeit kann – variable Cluster-Größe vorausgesetzt – hierüber zusätzlich eine gute Skalierbarkeit des VPN-Gateways erzielt werden.

Von Nachteil sind allerdings die meist hohen Kosten: in der Regel stehen entweder hochpreisige Systeme mit integrierter Clusterfunktion zur Verfügung oder preisgünstige VPN-Lösungen müssen mit Hilfe teurer Cluster-Software aufgerüstet werden. Auch die Stabilität solcher Lösungen – insbesondere unter hoher Last – sollte unter den konkret vorliegenden Rahmenbedingungen sorgfältig untersucht werden: hier hat es in der Vergangenheit nicht selten Fälle gegeben, in denen das Cluster die Systemverfügbarkeit eher negativ als positiv beeinflusst hat.

Zu beachten ist auch, dass naturgemäß ein VPN-Gateway-Cluster den Local Loop nicht mit absichern kann, sondern lediglich die VPN-Gateway-Funktion.

Absicherung der VPN-Geräte mittels Failover

Dieser Lösungsansatz verwendet eine im VPN-Gateway eingebaute Failover-Option. Hierbei erscheinen die miteinander gekoppelten Gateways nach außen als ein einziges virtuelles VPN-Gateway. Anders als beim Cluster ist aber stets nur ein Gateway aktiv; dieses bewältigt die gesamte Kommunikationslast. Erst im Fehlerfall erfolgt ein Umschalten auf ein anderes Gateway, das daraufhin zum aktiven Gateway wird.

Vorteile dieses Ansatzes liegen in der gegenüber „vollwertigen“ Cluster-Lösungen oft günstigeren Lizenzierung: die jeweiligen Standby-Systeme sind meist preiswerter, da ein Parallelbetrieb beider Systeme ausgeschlossen ist. In der Vergangenheit haben sich solche Lösungen als recht stabil erwiesen.

Nachteilig ist hier sicherlich die fehlende Load-Sharing-Option, die gleichzeitig eine Skalierung des VPN-Gateways ausschließt.

Auch dieser Ansatz schließt den Local Loop nicht mit ein.

Problematische VPN-Aspekte – Redundanz

Absicherung der VPN-Geräte mittels Routing-Mechanismen

Dieser Lösungsansatz verwendet Standard-Routing-Mechanismen. Im Backup-Fall wird der Datenverkehr auf einem alternativen Weg, d.h. über ein anderes Gateway, zum Ziel transportiert. Dazu müssen die betroffenen Remote VPN-Gateways typischerweise entweder den Aufbau mehrerer paralleler Tunnel zu verschiedenen Gateways unterstützen oder es kommen alternativ mehrere Gateways zum Einsatz. In letzterem Fall wären beide VPN-Lokationen hochverfügbar ausgelegt...

Vorteile des Ansatzes liegen neben dem Kostenaspekt (keine Cluster-Software notwendig) und den Load-Sharing und Skalierungs-Möglichkeiten (jeweils in Abhängigkeit vom Routing-Mechanismus, der zum Einsatz kommt) vor allem in den Bereichen Stabilität und Flexibilität.

Nachteilig kann eine eventuelle kurze Kommunikationsunterbrechung sein, die durch die notwendige Konvergenzzeit des Routing-Mechanismus und einen ggfs. notwendigen VPN-Tunnelaufbau verursacht wird. In den meisten Szenarien ist die auftretende Verzögerung jedoch so gering, dass dies nicht auf die Anwendungen durchschlägt.

Bei diesem Ansatz ist es problemlos möglich, auch den Local Loop mit abzusichern.

Absicherung der VPN-Geräte mittels Load-Balancer

Dieser Lösungsansatz verwendet Load-Balancer (LB); diese Systeme sind ursprünglich zur Lastverteilung in Server-Farmen gedacht, eignen sich aber auch für HV-Lösungen. Das LB-System stellt sich nach außen als ein einziges virtuelles VPN-Gateway dar und leitet Kommunikationsbeziehungen jeweils auf dasjenige reale Gateway um, das aktuell am wenigsten ausgelastet ist. Fällt ein Gateway aus, wird dies wie eine Vollauslastung interpretiert, so dass der Datenverkehr auf andere Gateways umgeleitet wird.

Vorteile dieser Lösung finden sich in den Bereichen Load-Balancing und damit auch Skalierbarkeit; außerdem arbeiten gute Load-Balancer sehr stabil und sind, da es sich um völlig eigenständige Komponenten handelt, für alle VPN-Techniken nutzbar.

Von Nachteil sind allerdings die hohen Kosten: es werden vor- und nachgeschaltete Balancer benötigt, die ebenfalls wiederum redundant ausgelegt sein müssen.

Die Lösung deckt – wie alle Ansätze, die sich auf die Gateways konzentrieren – den Local Loop nicht mit ab, so dass dieser separat abgesichert werden muss.

Absicherung der VPN-Geräte mittels vorkonfigurierter Reservegeräte

Die Absicherung mittels fix-und-fertig konfigurierter Austausch-Systeme (mitunter auch gern als Cold-Standby-Lösung bezeichnet) weist als gravierenden Nachteil die Notwendigkeit eines manuellen Eingreifens seitens des Betriebspersonals auf. Um die notwendige Qualität der entsprechenden Arbeitsschritte zu gewährleisten sind regelmäßige Übungen unumgänglich, zumal die Reservesysteme auch hinsichtlich ihrer einwandfreien Funktion in festen Zeitabständen überprüft werden sollten. Auch die kontinuierliche Aktualisierung der Standby-Systeme hinsichtlich deren Hard- und Software-Ausstattung sowie der Parametrierung ist eine nicht zu unterschätzende Aufgabe, insbesondere in Umgebungen mit einer überdurchschnittlichen Änderungsdynamik. Schließlich ist zu beachten, inwieweit detailliertere Verfügbarkeitsanforderungen jenseits prozentualer Angaben – etwa maximale Ausfallzeiten – mit den jeweiligen Betriebszeiten überhaupt realisierbar sind: lassen sich solche Anforderungen beispielsweise auch Nachts oder an Wochenenden erfüllen?

Als einzige Vorteile verbleiben die vergleichsweise geringen Kosten – die Reservegeräte benötigen in aller Regel keine Lizenz, da sie nicht aktiv sind – und die geringe Komplexität: Im Fall eines Versagens der aktiven Systeme werden letztere einfach 1:1 gegen die Reservesysteme getauscht.

Absicherung der VPN-Geräte durch Wartungsvertrag

Alternativ zur selbst realisierten Bevorratung von Reservesystemen kann auch – soweit angeboten – ein geeigneter Wartungsvertrag abgeschlossen werden. Für eine solche Lösung gelten im wesentlichen die gleichen Anmerkungen wie für die zuvor diskutierte Lösung; im Zweifel verlängern sich die Ausfallzeiten sogar noch weiter, da das Wartungspersonal erst anreisen muss...

Absicherung des WAN-Links

Wie bereits mehrfach angesprochen, stellt der WAN-Link zum Provider das schwächste Glied des Kommunikationspfades dar und bedarf daher in besonderem Maße einer adäquaten Absicherung. Alle zuvor angesprochenen Redundanzmechanismen – mit Ausnahme des Einsatzes von Routingverfahren – decken ausschließlich das VPN-Gateway ab; der Local Loop ist daher mit separaten Mechanismen abzusichern.

Dabei stehen grundsätzlich 3 gängige Ansätze zur Verfügung:

- Der WAN-Link wird mehrfach (i.d.R. doppelt) ausgelegt – in diesem Fall kann mittels Load-Sharing eine entsprechend hohe Bandbreite realisiert werden und auch im Fehlerfall normalerweise ohne wesentliche Einschränkungen weiter kommuniziert werden. Allerdings entstehen hohe Kosten, die nur dann unmittelbar zu einem Mehrwert führen, wenn die zusätzliche Bandbreite auch tatsächlich sinnvoll in Anspruch genommen werden kann: Reicht beispielsweise ein E1-Link (2 Mbps) zur Aufnahme der Kommunikationslast aus, so führt ein redundanter zweiter Link bestenfalls zu einer spürbaren Verbesserung bei extremen Lastspitzen, nicht aber bei „normalem“ Kommunikationsaufkommen.

- Der WAN-Link wird mit einem Wähl-Back-up versehen – diese Lösung ist im Vergleich zum redundanten WAN-Link kostengünstiger, da nur die monatlichen Grundgebühren für den Wählanschluss sowie die sporadisch anfallenden Gesprächsgebühren zu berücksichtigen sind – letztere sind obendrein meist vergleichsweise niedrig, da es sich um einen lokalen Link handelt. Es entstehen allerdings in der Regel Leistungseinbußen gegenüber dem Primärlink im Fehlerfall; andernfalls muss der Wählanschluss sehr großzügig dimensioniert werden, was den Kostenvorteil großenteils wieder aufzehrt. Auch eine Bandbreiten-skalierung ist bei üblicher Auslegung des Wählanschlusses nur in sehr engen Grenzen möglich: die über diesen Link nutzbare Bandbreite ist gering und außerdem wegen der zeitbezogenen Tarifierung bei dauerhafter Nutzung teuer. Ein solcher Ansatz eignet sich allenfalls zum Abfangen gelegentlicher Lastspitzen.

- Es erfolgt ein Wähl-Backup mit direkter Einwahl in der VPN-Gegenstelle - diese Lösung (mitunter auch als „Backup Around the Cloud“ bezeichnet) ist im Vergleich zum redundanten WAN-Link relativ kostengünstig, da nur die monatlichen Grundgebühren für den Wählanschluss sowie die sporadisch anfallenden Gesprächsgebühren zu berücksichtigen sind.

Letztere können allerdings bei internationalen Verbindungen durchaus signifikant werden. Ein weiterer nicht zu unterschätzender Vorteil dieses Ansatzes ist die Abdeckung auch von Störungen innerhalb des VPN-Trägernetzes, da der komplette Backup-Pfad von der Netzstruktur des Providers unabhängig ist. Hinsichtlich zu erwartender Leistungsein-bußen gegenüber dem Primärlink wie auch zur Skalierungsmöglichkeit gilt das gleiche wie schon zuvor dargelegt. Die anfallenden Kosten für diese Lösung können insbesondere bei internationalen Standorten recht schnell in unangenehme Größenordnungen vorstoßen, wenn die Backup-Verbindung – z.B. bei schlechter Qualität des Primärlinks oder Konfigurationsfehlern – sehr oft oder für längere Zeiträume in Anspruch genommen werden muss. Zu berücksichtigen ist auch das entsprechend auszulegende Dial-In-System in der VPN-Gegenstelle, welches ebenfalls Kosten für Planung, Realisierung und Betrieb nach sich zieht.

Zwischenbilanz

Welche der angesprochenen Varianten eignen sich nun grundsätzlich für einen Einsatz in Umgebungen mit hohen Verfügbarkeitsanforderungen?

Die Varianten mit manuellem Eingreifen scheiden in aller Regel aus, da sie zu große Unwägbarkeiten hinsichtlich der Erfüllung hoher Anforderungen mit sich bringen. Ebenfalls auszuschließen ist in den meisten Fällen der Load-Balancer-Ansatz; dieser ist deutlich teurer als andere Lösungen, ohne entsprechend mehr zu leisten.

Der Cluster-Ansatz eignet sich vor allem dann, wenn aus anderen Gründen ohnehin eine solche Lösung implementiert werden muss – etwa mit Blick auf zukünftige HV-Anforderungen an die Internet-Firewall; bei einer VPN-Lösung auf Firewall-Basis würde sich hier natürlich eine Nutzung des ohnehin einzusetzenden Firewall-Clusters auch zur Verfügbarkeitssicherung des VPN anbieten. Ansonsten bieten andere Varianten mehr Vorteile.

Aus Sicht des Autors sind im Grundsatz die Varianten „Routing-Mechanismus“ und „Fail-Over“, letzteres in Verbindung mit routingbasierender Redundanz für den Local Loop, zu bevorzugen.

Alternative Varianten sollten normalerweise nur dann in Betracht gezogen werden, wenn die präferierten sich im Zuge der Detailkonzipierung der VPN-Gesamtlösung als nicht hinreichend geeignet erweisen sollten, bzw. sich eine alternative Variante aus sonstigen Gründen (s.o.) anbietet.

Dabei stellt in den meisten Fällen die Routing-Variante nach Einschätzung des Autors die Methode der Wahl dar, soweit nicht ungünstige Randbedingungen dem entgegenstehen.

Gründe hierfür sind vor allem:

- Kosten
- Verfügbarkeit für praktisch alle VPN-Lösungsansätze
- Einbeziehung des WAN-Links
- Load-Sharing-Möglichkeit, einschließlich WAN-Link

In Bezug auf die Art der Absicherung des WAN-Links kann keine eindeutige pauschale Empfehlung ausgesprochen werden. Diese Entscheidung ist jeweils auf der Basis der konkreten Detail-Konzipierung zu treffen, wenn alle relevanten Rahmenbedingungen festliegen.

Redundanz – aber auf welcher Ebene?

Bisher haben wir die Verfügbarkeitsfrage punktuell, d.h. bezogen auf entweder die VPN-Box oder den Local Loop betrachtet. Da aber – wie ganz zu Anfang bereits angesprochen – stets die Gesamtlösung im Auge zu behalten ist, muss noch die Frage gestellt werden, wie die punktuellen Lösungen miteinander in Einklang zu bringen sind.

Fassen wir nochmals zusammen: Die üblicherweise geforderte Ausfallsicherheit wird durch Redundanz erreicht; dabei müssen nicht nur das VPN-Equipment sondern auch das Trägernetzwerk entsprechend ausgelegt sein. Da das Trägernetzwerk (meist das Internet, das im Folgenden als Basis angenommen wird – die jeweiligen Argumentationen lassen sich auch im Fall eines speziellen Provider-Netzwerks übernehmen) in dessen Core-Bereich in aller Regel als ausreichend redundant angesehen werden kann, konzentrieren sich Maßnahmen in diesem Bereich sinnvollerweise auf die Anbindung an diesen Internet-Core, d.h. die ISP-Anbindung und hier insbesondere den WAN-Link zum ISP-PoP.

Problematische VPN-Aspekte – Redundanz

Eine Ausfallsicherheit dieser Core-Anbindung kann durch Redundanzmaßnahmen in zwei unterschiedlichen Bereichen gewährleistet werden:

- Innerhalb des Trägernetzwerks selbst
- Auf der VPN-Ebene

Der Ansatz der Redundanz im Trägernetzwerk basiert auf der Bereitstellung redundanter WAN-Links mit automatisierter Umschaltung innerhalb des Trägernetzwerks im Fehlerfall.

Ist diese Voraussetzung gegeben, so sind auf der VPN-Ebene keinerlei Maßnahmen zur Verfügbarkeitssicherung für die Internetanbindung mehr erforderlich; die Redundanzmechanismen für das VPN-Equipment können daher mit größtmöglicher Flexibilität gestaltet werden.

Mögliche Lösungen (unter Berücksichtigung der zuvor gezogenen Zwischenbilanz) für die VPN-Redundanz sind dann:

- Fail-Over
- Routing-Mechanismen (VRRP/HSRP)
- Routing-Mechanismen (dynamisches Routing)

Allerdings ist zu berücksichtigen, dass für diesen Ansatz ein internes Transitnetz zwischen den VPN-Komponenten und den WAN-Routern notwendig ist (vgl. Bild 3). Dies hat zur Folge, dass eine Vereinigung der Funktionen WAN-Routing und VPN-Tunneling in einem einzigen Gerät nicht möglich ist; die Kosten sind bei diesem Ansatz somit potenziell höher.

Der alternative Ansatz stellt die Ausfallsicherheit der Internetanbindung über entsprechende Mechanismen auf der VPN-Ebene her. Dies ist u.a. dann sinnvoll, wenn eine Redundanz innerhalb des Trägernetzwerks nicht geeignet bereitgestellt werden kann oder entsprechende Lösungen zu komplex oder unflexibel ausfallen würden.

Der Lösungsansatz lässt sich wie folgt beschreiben:

Es werden mehrere (in der Regel zwei) redundante Pfade aufgebaut, bestehend aus jeweils einem VPN-Gateway und einem WAN-Link zum ISP-PoP. Über jeden Pfad wird je ein VPN-Tunnel aufgebaut; diese Tunnel werden wie virtuelle WAN-Links zur VPN-Gegenstelle behandelt. Die Umschaltung zwischen den beiden möglichen Pfaden erfolgt durch dynamisches Routing innerhalb der Tunnel: Fällt ein Tunnel aus – egal aus welchem Grund – so betrachtet das Routing-Protokoll den virtuellen WAN-Link als „down" und schaltet auf den alternativen Link um.

Redundanz auf der VPN-Ebene

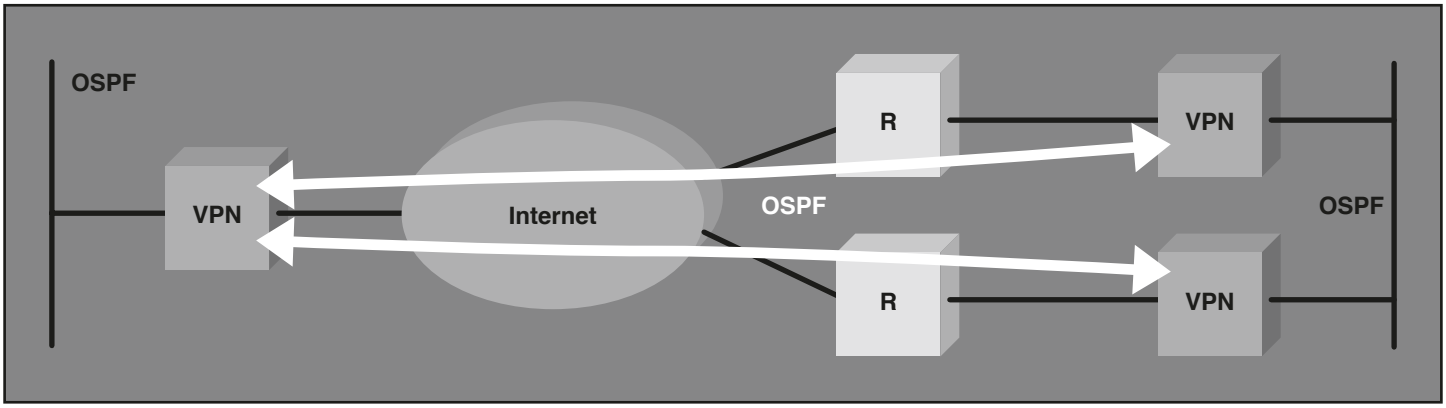
Dieser Ansatz (vgl. oben und Bild 2) setzt den durchgängigen Einsatz eines Routing-Protokolls innerhalb der gesamten VPN-Infrastruktur voraus. Ein Einsatz von alternativen lokalen Mechanismen wie z.B. VRRP scheitert bei dem dargestellten Ansatz in der Regel daran, dass diese Verfahren das Wegbrechen des VPN-Tunnels nicht detektieren können. Fällt ein Gateway aus, so schaltet VRRP auf das alternative Gateway um; dieser Fall ist aber infolge der üblicherweise recht hohen Verfügbarkeitswerte für Netzinfrastrukturkomponenten der weitaus seltenere gegenüber Fehlern innerhalb des Trägernetzwerks. Treten letztere auf, so bleibt das betroffene Gateway aktiv und eine Umschaltung des Traffics auf den alternativen Pfad erfolgt nicht. Außerdem gestaltet sich bei Verwendung von VRRP ein ansonsten mögliches Load-Balancing komplizierter; mit der skizzierten, einfachen Verschaltung der Komponenten ist dies überhaupt nicht möglich.

Bei der Wahl eines geeigneten Routing-Protokolls sollte OSPF bevorzugt werden, da es schnelle Konvergenz und (bei Bedarf) sichere gegenseitige Authentifizierung bietet und insbesondere ein gesteuertes Load-Balancing ermöglicht. Dennoch ist auch der Einsatz von Distance-Vektor-Protokollen, z.B. RIP, prinzipiell möglich.

Bei höheren Verfügbarkeitsanforderungen kann der zweite Standort ebenfalls redundant ausgelegt werden. In diesem Fall stellt er sich als Spiegelbild des ersten Standorts dar.

Diese Lösung bietet eine Reihe von vorteilhaften Aspekten – insbesondere können problemlos zwei unabhängige Provider genutzt werden, um im Sinne einer möglichst umfassenden Entkopplung der beiden redundanten Pfade die Ausfallsicherheit nochmals zu erhöhen; auch ein Wechsel eines Providers ist jederzeit machbar. Weiterhin erfasst dieser Ansatz sämtliche Fehlerszenarien (Gateway und Local Loop), ohne zusätzlicher Mechanismen zu bedürfen. Allerdings ist die Funktionalität des dynamischen Routings innerhalb des VPN-Tunnels eine Forderung, die derzeit noch die Produktauswahl einschränkt. Am besten fährt man hier nach Erfahrung des Autors mit VPN-Routern; solche können ggfs. dann auch die Funktion des WAN-Routers mit übernehmen und so die Komponentenkosten reduzieren, wobei allerdings in der Regel die Nutzung eines vom Provider gestellten und betriebenen Routers – der zudem meist in den Kosten des Internetzugangs bereits enthalten ist – Vorteile bringt, insbesondere mit Blick auf eine saubere Schnittstellendefinition (in diesem Fall die LAN-Schnittstelle des Provider-Routers).

Bild 2: Redundanz durch dynamisches Routing im VPN



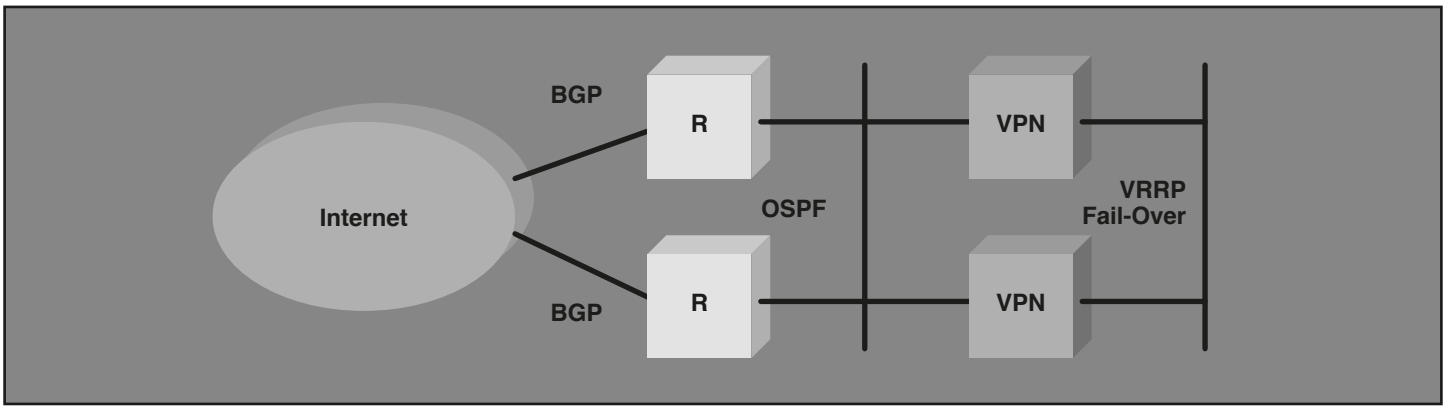


Bild 3: Dynamisches ISP-Routing mit BGP

Redundanz im Trägernetzwerk

Alternativ kann die Redundanz auch auf Ebene der Trägernetzwerks bereitgestellt werden.

Am elegantesten geschieht dies über ein dynamisches Routing zwischen dem Provider und dem eigenen Netz. Dies erfordert allerdings entsprechende Bereitschaft seitens des Providers, die nicht zwangsläufig in allen Fällen gegeben sein muß. Spielt der Provider nicht mit, muss man sich mit anderen Mitteln behelfen...

Die resultierenden Varianten sind im folgenden dargestellt. Dabei wird in der Illustration stets davon ausgegangen, dass aus Sicherheitserwägungen kein dynamisches Routing in Richtung Firewall eingesetzt wird.

Grundsätzlich kann natürlich auch bei diesen Ansätzen z.B. OSPF eingesetzt werden, was insgesamt Vorteile bringt, etwa mit Blick auf Lastverteilung zwischen den VPN-Gateways.

Dynamisches Routing

Bild 3 illustriert diesen Ansatz; hier erfolgt ein Peering mit dem Provider via BGP. Die propagierten Routen werden intern mittels OSPF weitergegeben; die Gateways können mit einem beliebigen Mechanismus gegen Ausfall geschützt werden.

Bei dieser Lösung lassen sich, ähnlich wie bei der weiter oben dargestellten Redundanz auf VPN-Ebene, alle Fehlerszenarien abdecken, allerdings muss ggfs. ein zusätzlicher Mechanismus für die VPN-Gateways eingesetzt werden (z.B. eine Failover-Lösung). Außerdem kann selbst bei Ausfall eines Gateways immer noch ein Load-Sharing stattfinden. Nachteilig ist in jedem Fall, dass man auf die Mitarbeit des/der Provider angewiesen ist – dadurch werden insbesondere Providerwechsel erschwert – und in vielen Fällen ausreichender registrierter IP-Adressraum sowie eine AS-Nummer für das BGP-Routing benötigt wird. Alternativ kann ein IGP (z.B. OSPF) eingesetzt werden, allerdings ist diese Lösung zumindest in Mehr-Provider-Szenarien unüblich und dürfte nicht selten an der fehlenden Bereitschaft des Providers zur Mitwirkung scheitern.

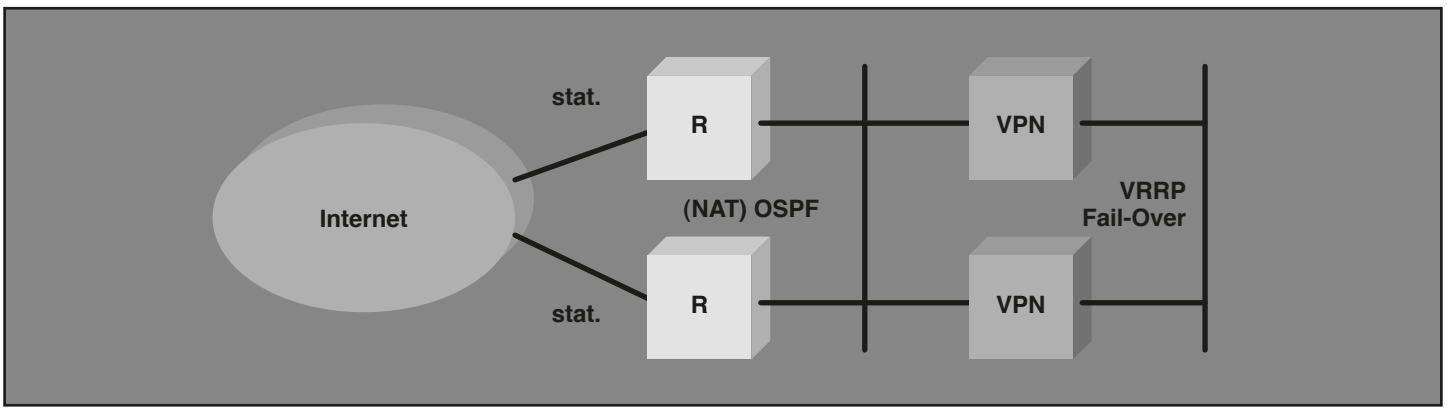
Statisches Routing

Bild 4 illustriert diesen Ansatz; hier werden für die VPN-Peers auf den WAN-Routern statische Routen eingerichtet. Diese statischen Routen werden intern mittels OSPF-Redistribution weitergegeben; die Steuerung des Datenverkehrs erfolgt über gezielte Kostenzuweisung für diese externen Routen.

Die Gateways können mit einem beliebigen Mechanismus gegen Ausfall geschützt werden.

Bei diesem Ansatz ist eine Mitwirkung des Providers nicht notwendig, wodurch die oben angesprochenen Einschränkungen/Probleme nicht auftreten. Ansonsten entspricht er in seiner Funktionalität dem dynamischen Ansatz, allerdings mit einer nicht unwesentlichen Einschränkung: Es ist keine vollständige Redundanz gegeben; eine Umschaltung auf den alternativen Pfad erfolgt nur bei Ausfall des WAN-Links oder des WAN-Routers, nicht bei sonstigen Problemen auf der ISP-Seite.

Bild 4: Statisches ISP-Routing



Problematische VPN-Aspekte – Redundanz

Dieses Konstrukt ist grundsätzlich auch mit mehr als einem Provider möglich. Üblicherweise werden ISP-Adressen unter Ver-wendung von NAT eingesetzt; alternative Lösungen setzen in der Regel das Vorhan-densein eines eigenen offiziellen IP-Adressraums voraus und sind mit den beteiligten Providern abzustimmen. Es ist allerdings fraglich, ob die beteiligten Provider gewillt und in der Lage sind, solche Alternativlösungen zu realisieren. Erfahrungsgemäß verursachen Sonderlösungen zumindest Probleme, sowohl in technischer als auch in organisatorischer Hinsicht. Auch Providerwechsel sind nicht trivial, da die bestehende Lösung von einem neuen Provider adaptiert oder ggfs. eine neue Lösung gefunden werden müsste.

Dezentrale Redundanzmechanismen

Alle dargestellten Redundanzlösungen generieren einen nicht unerheblichen Aufwand; daher stellt sich die Frage, ob etwa auch kleinere dezentrale Außenstellen in gleicher Weise wie etwa der zentrale Hauptstandort eines VPN-basierten Netzwerk-Verbunds hochverfügbar an diesen Verbund angeschlossen werden sollen.

Grundsätzlich sind für die Anbindung dezentraler Liegenschaften an das VPN – je nach Verfügbarkeitsanforderung – drei Varianten möglich:

- Hochverfügbarer VPN-Anschluss analog zur Zentrale
- Hochverfügbarer WAN-Link

  Bei dieser Variante erfolgt die ISP-Anbin-dung im wesentlichen analog zur zentralen Anbindung, allerdings wird auf Hardware-Redundanz verzichtet. Dies vereinfacht das Konstrukt – auch im Hinblick auf die LAN-Infrastruktur – und reduziert die Kosten.

  Die Gesamtverfügbarkeitsbilanz ist demgegenüber immer noch gut, da die Hauptursache für Ausfälle der WAN-Link zum ISP-PoP ist (vgl. Grobkonzept). Nimmt man realistische Werte für die Verfügbarkeit der Hardware an, so ist die Verlängerung der mittleren Ausfallzeiten kaum spürbar (bei angenommenen 99,99% Verfügbarkeit für die Hardware – ein durchaus konservativer Wert – beträgt diese Verlängerung ca. 50 Minuten p.a.).
- Normalverfügbarer VPN-Anschluss

  Bei dieser Variante existiert nur eine einfache Anbindung an den ISP. Die geforderte Absicherung des Zugriffs auf die zentralen Ressourcen wird mittels eines Dial-In-Backup erreicht.

Hierbei sind zwei Alternativen zu betrachten:

- Direkter Dial-In in der Zentrale, wahlweise mit oder ohne VPN-Tunnel – dies stellt einen Backup für den gesamten VPN-Tunnel dar (Variante „Around the Cloud“)
- Dial-In beim ISP, mit VPN-Tunnel – hierbei handelt es sich um einen Backup für den WAN-Link

Die zweite Alternative benötigt keine zentrale Dial-In-Infrastruktur und entspricht einer etwas schwächeren Variante des hochverfügbaren WAN-Links; allerdings werden Ausfälle im Bereich des ISP-Netzes nicht mit abgedeckt. Sofern die zentrale Dial-In-Lösung mit vertretbarem Aufwand realisiert werden kann und stabile zuverlässige Wählverbindungen aus der jeweiligen Niederlassung zur Zentrale möglich sind, empfiehlt sich daher die erste Alternative. Allerdings muss dazu eine Detektion des Ausfalls des Tunnels und Verwendung dieses Tunnelausfalls als Trigger für den Dial-Vorgang erfolgen können. Hierzu bietet sich z.B. der Einsatz eines Routing-Protokolls und das Setzen einer (routingtechnisch „teuren“) statischen Route über das Dial-Interface an – ein Verfahren, das auch als „Floating Static Route“ bezeichnet wird.

Redundanzmechanismen für Mobile Clients

Neben der Anbindung von remote Standorten an eine Zentrale eignet sich eine VPN-Lösung in besonderem Maße auch zur Bereitstellung eines Remote-Zugriffs für mobile Clients. Es stellt sich die Frage, inwieweit hier die skizzierten Redundanzmechanismen ebenfalls wirksam werden können.

Je nach Redundanzmechanismus auf zentraler Seite sind Maßnahmen auf der Client-Seite nicht erforderlich – dies gilt dann, wenn sich die Identität des zentralen VPN-Knotens bei Greifen der Redundanzmechanismen nicht ändert, was beispielsweise bei Failover-Lösungen typischerweise der Fall ist.

Falls sich die Identität ändern kann – davon ist bei der Mehrzahl der skizzierten Lösungen auszugehen – muss der Client in der Lage sein, verschiedene Gegenstellen (Peers) zu kontaktieren. Der Client-Mechanismus arbeitet dann bei Verlust eines VPN-Tunnels diese Peer-Liste im Round-Robin-Verfahren ab, bis ein neuer Tunnel aufgebaut werden konnte.

Unterstützt der Client derartige Mechanismen nicht (z.B. bei Einsatz des nativen W2K-VPN-Clients), so kann alternativ eine Definition verschiedener VPN-Verbindungen erfolgen, aus denen der Anwender manuell (nach dem Trial-and-Error-Prinzip) eine funktionsfähige auswählt.

Fazit

Die Bereitstellung der Redundanz auf der VPN-Ebene stellt bei einer Gesamtbetrachtung aller Vor- und Nachteile aus Sicht des Autors die günstigste Lösung dar.

Wesentliche Gründe für diese Bewertung sind:

- Unabhängigkeit von der Mitwirkung der Provider und den damit verbundenen Unwägbarkeiten
- Problemlose Einbindung aller dezentralen Mechanismen in dieses Konzept
- Kostenersparnis und Verringerung der Komplexität der Architektur beim Einsatz von VPN-Routern

Daraus resultiert unmittelbar die Verwendung von Routing-Mechanismen als Redundanzverfahren; als optimales Protokoll bietet sich hier OSPF an. Innerhalb der LANs kann – falls OSPF nicht eingesetzt werden kann oder soll – alternativ VRRP verwendet werden. Für einen solchen Ansatz sind VPN-Router erfahrungsgemäß am besten geeignet.

Die Client-Redundanz wird dann über entsprechende Peer-Listen, bzw. ersatzweise die Definition mehrerer VPN-Verbindungen, hergestellt.

Die konkrete Auslegung zentraler bzw. dezentraler Standorte richtet sich nach den Anforderungen an die Verfügbarkeit; in den meisten Fällen ist von einer vollredundanten Lösung, wie skizziert, in zentralen und einer entsprechend abgespeckten Lösung in dezentralen Standorten auszugehen.

Problematische VPN-Aspekte – NAT

2. Teil der Fortsetzung von Seite 1

Das NAT-Problem

Diverse Mechanismen von IPSec und NAT vertragen sich nicht miteinander. Insofern handelt es sich eigentlich nicht um ein einziges NAT-Problem sondern um diverse NAT-Probleme. Wir wollen im folgenden sukzessive diese Problembereiche untersuchen und beginnen bei dem offensichtlichen: dem Authentication Header.

Der Authentication Header (AH) generiert eine kryptographische Prüfsumme über den Inhalt des IPSec-Pakets in Form eines MD-5 oder SHA-Hashwerts, zu dessen Berechnung ein geheimer symmetrischer Schlüssel erforderlich ist. Dieser Hashwert umfasst alle im Paket befindlichen Daten mit Ausnahme des AH-Prüfsummenfelds und der nicht-statischen Informationen des IP-Headers. Da der Hashwert ohne Kenntnis des Schlüssels nicht gezielt gefälscht und der Schlüssel seinerseits aufgrund der Eigenschaften der Hash-Funktion nicht aus dem Hashwert zurückberechnet werden kann, wird jegliche Manipulation am Datenpaket bei der Verifikation der Prüfsumme aufgedeckt und ein solches Paket vom Empfänger als ungültig verworfen. Der AH dient somit dem Erhalt der Integrität der übertragenen Datenpakete.

Soweit, so gut...

Unglücklicherweise basiert jedoch der NAT-Mechanismus bekanntermaßen genau auf einer gezielten Manipulation der IP-Adressen der Datenpakete: In der Regel wird die Absenderadresse durch eine andere Adresse ersetzt. Diese Manipulation wird vom AH äußerst wirksam unterbunden – er kann an dieser Stelle nicht zwischen erwünschten (NAT) und unerwünschten (IP-Spoofing) Manipulationen unterscheiden. Ein Einsatz des AH in NAT-Szenarien ist somit ausgeschlossen.

Dies allein scheint nicht weiter dramatisch, wird doch der AH in vielen Szenarien gar nicht verwendet bzw. kann meist darauf verzichtet werden, da das zweite IPSec-Protokoll, ESP, ebenfalls eine – wenn auch nicht ganz so weitreichende – Integritätsprüfung beinhaltet. Löst also der Verzicht auf den Authentication Header das NAT-Problem?

Leider nein, denn auch ESP (Encapsulating Security Payload) verursacht Probleme im Zusammenspiel mit NAT. Ein generelles Problem sind hier gemultiplexte NAT-Kommunikationsbeziehungen.

Multiplexing ist bei NAT dann vonnöten, wenn mehrere interne Adressen auf eine (oder wenige) externe Adresse abgebildet werden müssen – das Standard-Szenario etwa bei der Verwendung von DSL-Routern im SOHO-Bereich. Üblicherweise kommt hier NAPT (Network Address and Port Translation) zum Einsatz – dieser Mechanismus ist auch unter der Bezeichnung PAT (Port Address Translation) bekannt. NAPT/PAT multiplexen durch gezielte Manipulation des Client-Ports (bei UDP bzw. TCP) oder anderer aus Sicht des Empfängers frei wählbarer Parameter (z.B. ICMP-Identifier). Durch eine eindeutige Zuordnung der jeweiligen internen Adresse zu einem solchen Parameter lassen sich die Antwortpakete gezielt demultiplexen.

Unglücklicherweise verschlüsselt ESP den Teil des IP-Pakets, in dem sich diese manipulierbaren Parameter befinden. Somit ist eine sinnvolle Manipulation nicht mehr möglich und das Verfahren scheitert. Einzige Chance – für entsprechend ausgestattete NAT-Geräte – wäre eine Nutzung des IPSec-Headers zum Multiplexen. Hier steht allerdings lediglich der SPI (Security Parameter Index) zur Verfügung, der wegen der in ESP integrierten Integritätsprüfung nicht manipulierbar ist. Freilich bestünde grundsätzlich die Möglichkeit, den originalen ISP zu verwenden – immerhin ist die Wahrscheinlichkeit einer Kollision aufgrund der 32 Bit Länge des SPI extrem gering – allerdings besteht hier ein grundsätzliches Problem: der SPI wird für jede der beiden Kommunikationsrichtungen zwischen den beteiligten Partnern separat vereinbart. Die Folge davon ist, dass zwischen dem SPI der gesendeten Pakete und dem der empfangenen nicht notwendigerweise eine Korrelation besteht.

Anders ausgedrückt: der Empfänger eines Antwortpakets kann aus dem darin enthaltenen SPI nicht mit Sicherheit die korrekte Adreßabbildung ermitteln, da dieser SPI mit dem zuvor gesendeten in keinem erkennbaren Zusammenhang stehen muss. Daher ist diese Methode nicht allgemein verwendbar; es gibt allerdings Produkte (beispielsweise von Cisco), die in der Lage sind, identische SPIs auf beiden Seiten der Kommunikationsbeziehung sicherzustellen, und somit ein NAPT/PAT ermöglichen, solange die VPN-Lösung homogen bleibt.

NAPT/PAT geht also üblicherweise auch nicht – dann aber doch zumindest statisches NAT, oder? Nun, auch mit statischem NAT bleiben Probleme, nämlich zumindest dann, wenn ESP im Transport-Modus verwendet wird (dies ist beispielsweise bei der in Windows2000/2003 integrierten IPSec-VPN-Lösung der Fall). Ursächlich hierfür ist der Prüfsummenmechanismus in TCP (teilweise auch in UDP), der neben den Source- und Destination-Ports auch die jeweiligen IP-Adressen von Sender und Empfänger berücksichtigt. Ändert ein NAT-Gerät eine IP-Adresse, so muss der TCP-Header, d.h. das Prüfsummenfeld, entsprechend angepasst werden. Ohne ESP stellt dies kein Problem dar, mit ESP jedoch sehr wohl, da das Prüfsummenfeld verschlüsselt ist. Eine Korrektur ist somit nicht möglich – sie würde von der Integritätsprüfung von ESP sofort entdeckt werden – was dazu führt, dass die Prüfsummenverifikation beim Empfänger scheitert und dieser derartige Pakete verwirft.

Dieses Problem tritt allerdings nur im Transport-Modus auf: Im Tunnel-Modus bezieht sich die TCP-Prüfsumme auf den inneren IP-Header, während die Manipulation am äußeren, dem Tunnel-IP-Header vorgenommen wird. Da dieser auch von der ESP-Integritätsprüfung nicht erfasst wird, kann in diesem Fall NAT eingesetzt werden.

Somit bliebe also ESP im Tunnel-Modus mit statischem NAT als mögliches Einsatzszenario, wenn – ja, wenn nicht auch IKE Probleme mit NAT hätte.

IKE (Internet Key Exchange) handelt die IPSec-Sicherheitsbeziehungen (Security Associations, SA) zwischen den beiden Kommunikationspartnern aus. Leider wird es ebenfalls von NAT beeinträchtigt. Hierfür gibt es gleich mehrere mögliche Ursachen:

- IKE verwendet, abhängig von Einsatzform und Implementierung, IP-Adressen zur Identifizierung der Kommunikationspartner. Diese befinden sich als Parameter innerhalb des IKE-Protokolls. Stimmen diese Parameter mit den tatsächlichen IP-Adressen nicht überein, so wird ein entsprechendes Paket meistens verworfen.

- IKE verwendet selbst ebenfalls SAs, um einen geschützten Kommunikationspfad („IKE-Tunnel“) für das Aushandeln der IPSec-SAs bereitzustellen. Die zugehörigen IKE-SAs bestehen in aller Regel recht lange, um beispielsweise ein regelmäßiges Rekeying (dabei werden in bestimmten Zeitabständen die Schlüssel für die ESP-Verschlüsselung neu vereinbart) mit größtmöglicher Effizienz zu gestalten. Demgegenüber sind die NAT-Timeouts für UDP, dem von IKE genutzten Transportschicht-Protokoll, in der Regel erheblich kürzer. Da über IKE nur bei Bedarf Informationen ausgetauscht werden, kommt es häufig zu langen Idle-Perioden, die dazu führen, dass das Adress-Mapping aus der NAT-Table gelöscht wird, was zur Unzustellbarkeit der betroffenen IKE-Pakete führt.

- Nicht alle IKE-Implementierungen akzeptieren Client-Ports, die vom Standard-Port (UDP 500) abweichen. Verändert ein NAT-Gerät den Source-Port eines abgehenden Pakets und der Empfänger akzeptiert nur den Port 500, so kommt keine Kommunikation zustande – die Aushandlung des IKE- und damit auch des IPSec-Tunnels scheitert.

Somit verbleibt oftmals nur die manuelle SA-Konfiguration, wenn NAT im Einsatz ist – ein Ansatz, der zumindest in umfangreicheren Szenarien absolut nicht praktikabel ist.

Dieses Problem wurde natürlich schon vor geraumer Zeit erkannt und es existieren diverse Lösungen dafür, die jedoch allesamt proprietärer Natur sind. Allen derartigen Techniken ist gemeinsam, dass sie Encapsulation als Lösungsansatz verwenden, was naheliegt, da sich damit – man sieht es beim ESP-Tunnel-Modus – einige Probleme quasi von selbst lösen.

Die meisten Hersteller generieren einen zusätzlichen UDP-Tunnel unter Verwendung verschiedenster Portnummern; eine etwas ausgefallenere Lösung bot die (mittlerweile strategisch durch die XSR-Router ersetzte) Aurorean-VPN-Lösung der Fa. Enterasys: Hier kam eine Verkapselung in HTTPS zum Einsatz, in der Hoffnung, auf dieser Basis aus vielen Netzwerken heraus ohne Anpassung einer etwaigen Firewall per VPN kommunizieren zu können.

NAT-Traversal – Das Prinzip

Problematisch bei diesen Ansätzen war neben der Inkompatibilität zwischen unterschiedlichen Herstellern die nicht selten sehr aufwendige manuelle Konfiguration des Encapsulation-Mechanismus. Ziel der IPSec-Arbeitsgruppe innerhalb der IETF war es daher, nicht nur einen Standard-Mechanismus zu entwickeln, der IPSec und IKE weitestgehend NAT-Kompatibel macht, sondern dies auch möglichst ohne manuellen Konfigurationseingriff.

Die aktuellen Ergebnisse für den „NAT-Traversal“ (NAT-T) getauften Mechanismus haben immer noch Draft-Status (derzeit in der Version 6 bzw. 7 für die beiden grundlegenden Mechanismen) und können unter www.ietf.org eingesehen werden. Die jeweiligen Drafts waren und sind immerhin bereits Basis für vereinzelte Implementierungen (beispielsweise für Microsofts Windows2000/2003/XP-VPN); das spricht dafür, dass die Drafts bereits einen recht hohen Qualitäts- und Stabilitätsgrad aufweisen.

Das Grundprinzip von NAT-T lässt sich leicht wie folgt beschreiben:

- Erkenne, ob NAT im Einsatz ist
- Verkapsele, falls nötig

Das Verfahren verfügt somit nicht nur über hinreichende Encapsulation-Techniken, sondern darüber hinaus über einen Lern-Mechanismus, der manuelle Konfiguration im Wesentlichen überflüssig machen soll.

Wie funktioniert NAT-T?

Betrachten wir zunächst das Erkennen eventueller NAT-Geräte. Diese Detektion erfolgt in der ersten IKE-Phase (Main Mode oder Aggressive Mode) und liefert gleichzeitig Informationen darüber, ob die fragliche Gegenstelle überhaupt NAT-T unterstützt.

Letzteres wird durch den Austausch von sog. Vendor-ID-Payloads im Rahmen der ersten beiden Nachrichten der ersten IKE-Phase festgestellt. Bei der dabei übermittelten ID handelt es sich um den MD5-Hash des Strings „RFC xxxx“, wobei xxxx für die Nummer des jeweils unterstützten RFCs steht. Stellt ein Kommunikationspartner fest, dass sein Gegenüber nicht NAT-T-kompatibel ist, d.h. ein „passender“ Hash-Wert wird nicht übermittelt, so bricht er die NAT-T-Prozedur ab.

Verstehen beide sich auf den NAT-T-Mechanismus, so prüfen sie den Kommunikationspfad auf das Vorhandensein etwaiger NAT-Geräte. Dazu untersuchen sie, ob sich IP-Adressen oder Ports auf dem Pfad zwischen ihnen ändern. Dies geschieht mit Hilfe spezieller NAT-D-Payloads (NAT-Discovery), die mit der dritten und vierten (im Main Mode) bzw. zweiten und dritten (im Aggressive Mode) Nachricht ausgetauscht werden. Eine solche NAT-D-Payload enthält den Hash-Wert der IP-Adresse und des Ports, jeweils für die Sender- und Empfängerseite. Der Ablauf ist wie folgt: Beide Partner berechnen über die eigene Adresse und den eigenen Port sowie über Adresse und Port des jeweils anderen je einen Hash-Wert; dazu bedienen sie sich des in den vorangegangenen IKE-Nachrichten ausgehandelten Hash-Verfahrens. Die beiden Hash-Werte übertragen sie in Form zweier NAT-D-Payloads an den Partner. Beide vergleichen die selbst berechneten (lokalen) Hash-Werte mit dem Inhalt der NAT-D-Payloads. Stimmen die jeweiligen Informationen überein, so befand sich kein NAT-Gerät im Pfad; bei Abweichungen muss mindestens ein NAT-Gerät existieren.

In diesem Fall geschieht Folgendes:

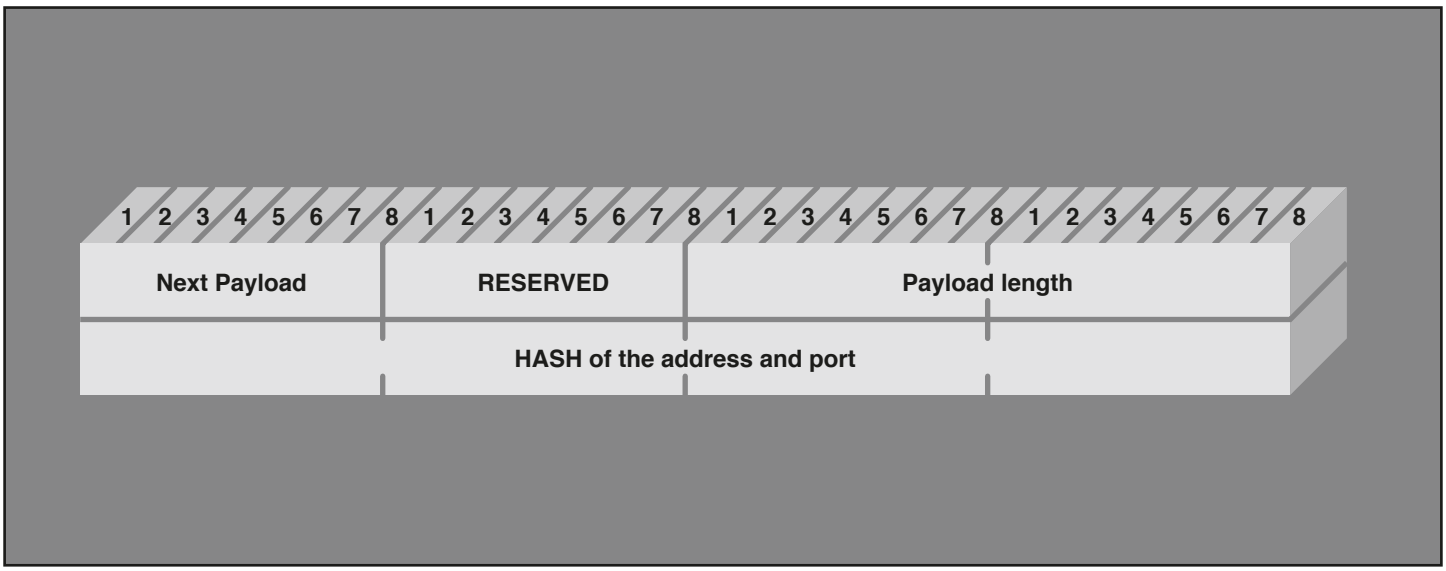
- Beide Kommunikationspartner ändern den IKE-Port auf UDP 4500 – dies soll eventuelle Störungen des NAT-T-Mechanismus durch NAT-Geräte mit „IKE-Unterstützung“ verhindern.

- Derjenige Kommunikationspartner, der feststellt, dass sich die Hashwerte für seine eigene Adresse unterscheiden, sendet sog. IKE-Keepalives – dies soll NAT-Timeouts verhindern und ist notwendig, da der besagte Kommunikationspartner sich offenkundig „hinter“ einem NAT-Gerät befindet.

- Die beiden Kommunikationspartner wenden die NAT-T-Kapselung an – dies wird in IKE-Phase 2 (Quick Mode) vereinbart.

Es versteht sich von selbst, dass ein NAT-T-kompatibles IKE zwingend auch IKE-Pakete von anderen Ports als UDP 500 akzeptieren muss. Anderenfalls kämen die für das Funktionieren von NAT-T notwendigen Informationsaustausche ja gar nicht zustande.

Bild 5: NAT-D-Payload



Zur Kapselung wird ein UDP-Header zwischen IP- und ESP-Header eingefügt (UDP-ESP) (Bild 6). Dieser verwendet die IKE-Ports, deshalb ist es notwendig, ein Unterscheidungsmerkmal zwischen IKE und UDP-ESP festzulegen. Dieses Merkmal ist der so genannte Non-ESP-Marker, der dem ursprünglichen IKE-Paketformat hinzugefügt wird; das neue, erweiterte IKE-Format wird als „Floated IKE“ (Bild 7) bezeichnet. Der Non-ESP-Marker befindet sich im übrigen exakt an der selben Position wie der SPI im UDP-ESP-Header. Da der Wert „0“ des Non-ESP-Markers als Kennzeichen für Floated IKE definiert ist, muss der SPI in ESP-SAs Werte ≠ 0 annehmen.

Das so beschriebene Paketformat wird der Einfachheit halber auch noch für die IKE-Keepalive-Pakete (Bild 8) verwendet. Diese sind durch eine Payload von 0xFF gekennzeichnet und sollen vom Empfänger kommentarlos ignoriert werden.

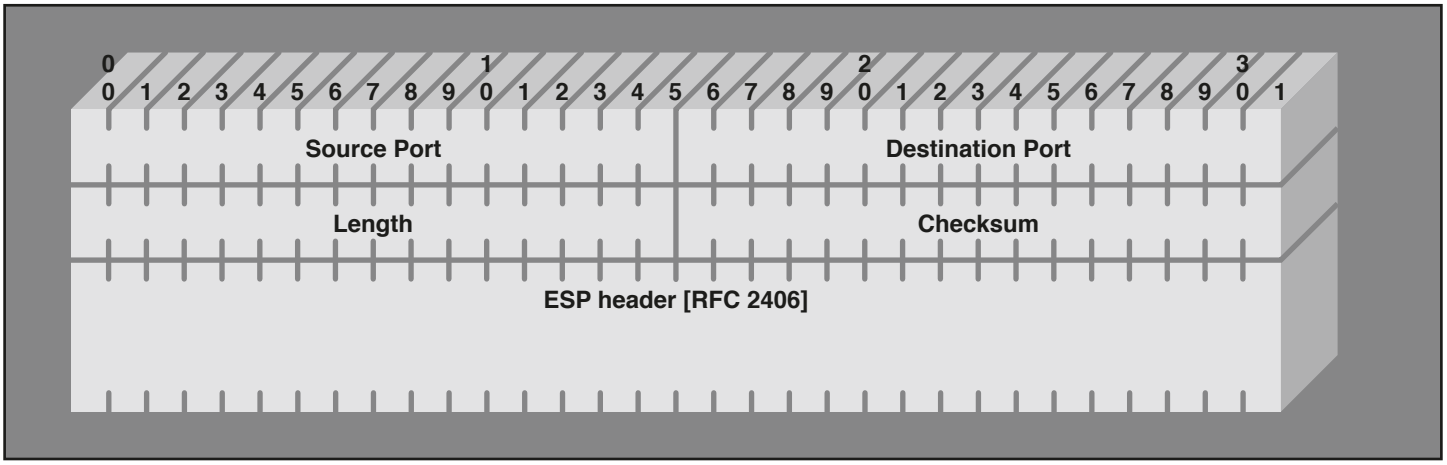


Bild 6 (oben): UDP-ESP

Bild 7 (Mitte): Floated IKE

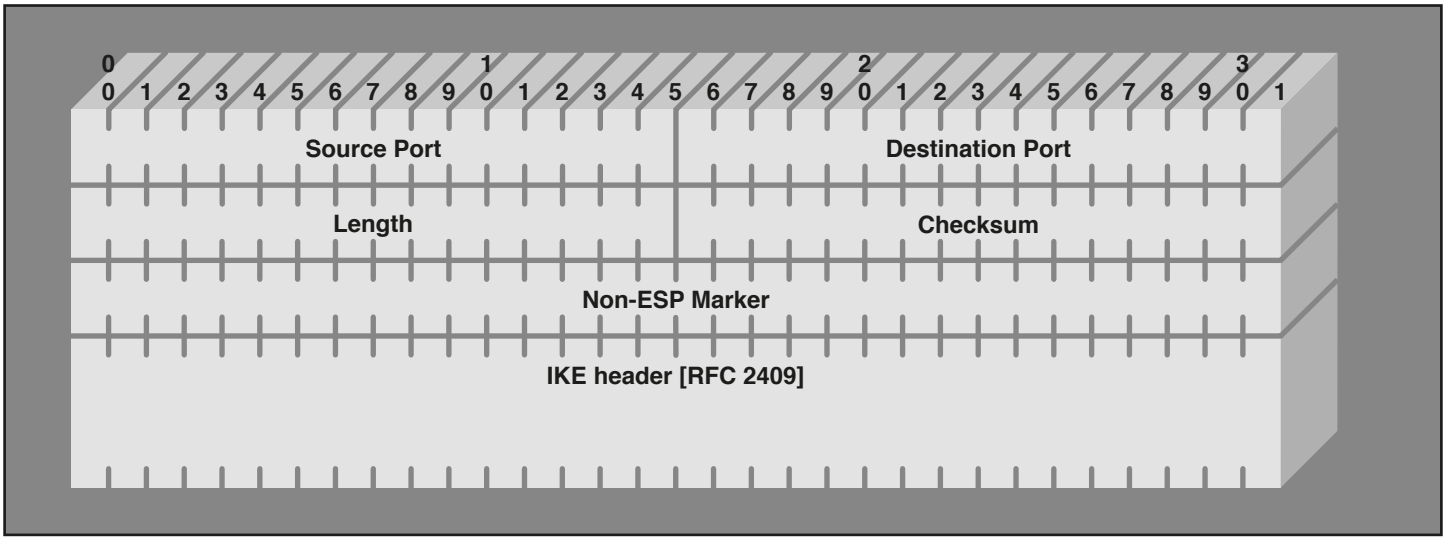
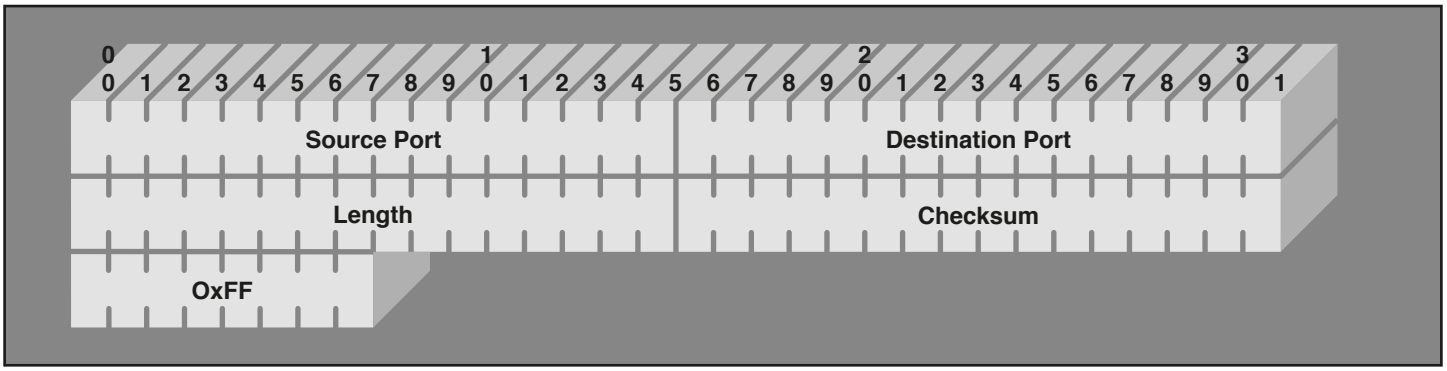


Bild 8 (unten): IKE-Keepalive



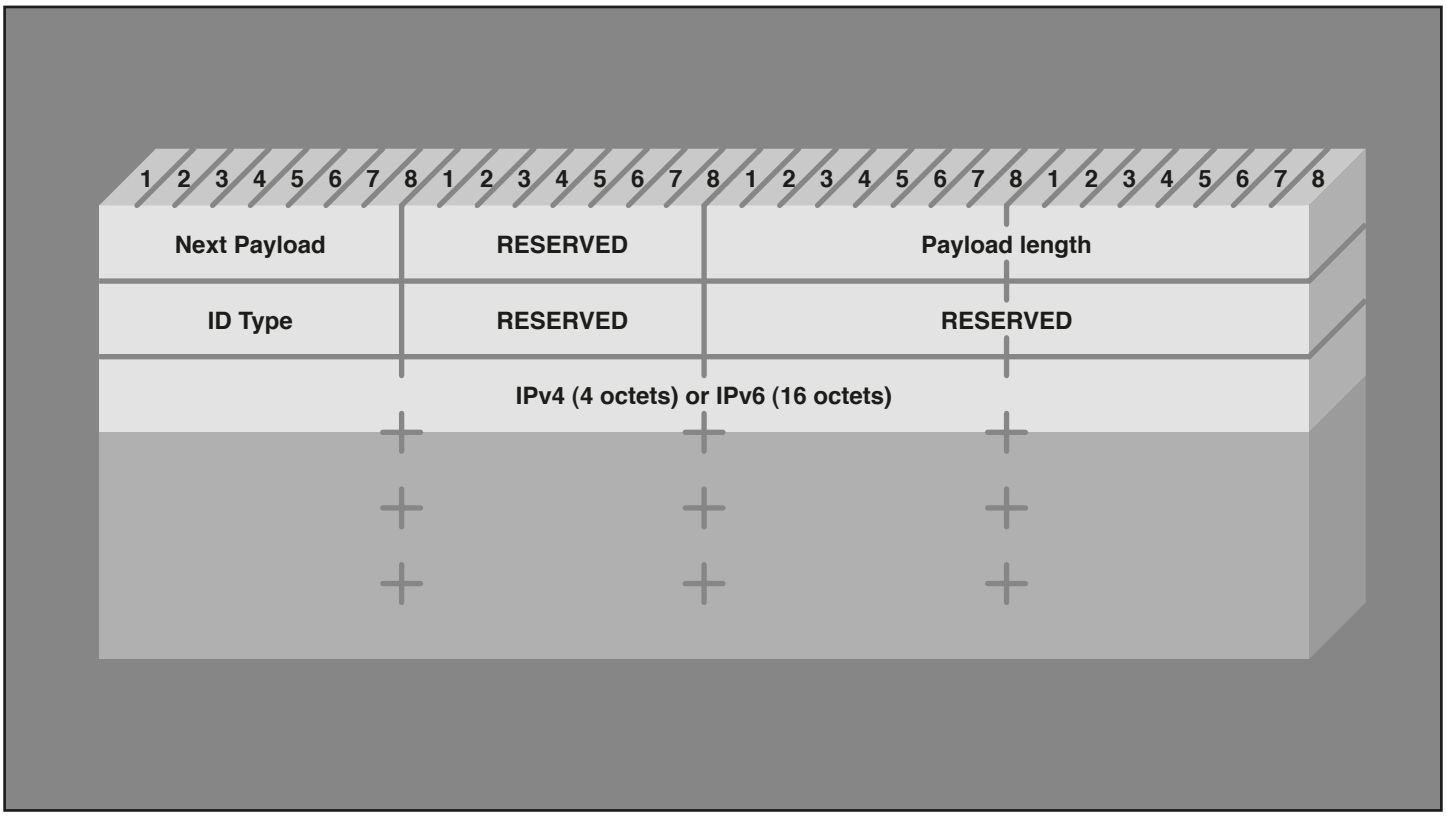


Bild 9: NAT-OA-Payload

Neben der für die IKE-Phase 1 vorgesehenen NAT-D-Payload ist mit der NAT-OA-Payload ein weiterer Nachrichten-Typ definiert. OA steht für „Original Address" und erlaubt die Information der Gegenstelle über die ursprünglichen Original IP-Adressen. Diese sind wichtig, falls der Kommunikationspartner bei ESP im Transport-Modus die Korrektheit der TCP-Prüfsumme auch nach erfolgter NAT verifizieren soll. Dazu werden die entsprechenden Adressinformationen in IKE-Phase 2 genau dann übermittelt, wenn ein Partner ESP im Transport-Modus als Proposal vorschlägt bzw. sich für diesen Vorschlag entscheidet. In einem sochen Fall werden dem Partner (in zwei getrennten Payloads) sowohl die eigene als auch die Partner-Adresse mitgeteilt, jeweils in der Form, in der sie lokal wahrgenommen wird, da sie in dieser Form in die lokale Prüfsummenberechnung Eingang gefunden haben.

Die jeweilige Partner-Adresse kann dabei u.U. durch ein vorhandenes NAT manipuliert sein – an dieser Stelle spielt dies keine Rolle, es muss nur sichergestellt sein, dass der Empfänger dieselben Adressen zur Prüfsummenkalkulation verwendet wie der Sender...

Fazit: Was geht und was bleibt offen?

Welche der festgestellten Probleme im Zusammenspiel von IPSec und NAT werden nun durch NAT-T – zumindest teilweise – gelöst?

Die IKE-Problematik wird im Wesentlichen durch entsprechende Erweiterungen / Anpassungen des Protokolls („IKEv2") gelöst: NAT-T-kompatible IKE-Implementierungen müssen mit abweichenden Source-Ports umgehen können, da NAT-T sonst gar nicht funktionieren kann. Ebenso muss IKE Abweichungen zwischen den protokollinternen IP-Adressen und den äußeren Adressen auf der Netzwerk-Ebene tolerieren. Die ebenfalls im Zusammenhang mit IKE stehende NAT-Timeout-Problematik wird durch die Verwendung der IKE-Keep-alives behoben. Diese sorgen dafür, dass das Adressmapping in der NAT-Table stets aufrechterhalten bleibt.

Das Multiplexing-Problem bei dynamischem NAT (NAPT/PAT) wird durch die Verkapselung mittels UDP-ESP gelöst, da der zusätzliche Header von den IPSec-Mechanismen nicht erfasst, d.h. weder in seiner Integrität geschützt noch verschlüsselt wird. Die UDP-Client-Ports können somit gezielt zum Multiplexen genutzt werden.

Die mit Hilfe der NAT-OA-Payload übertragenen ursprünglichen IP-Adressen ermöglichen die korrekte Verifikation der TCP-Prüfsumme im Transport-Modus.

Und schließlich entfällt die bei den bisherigen proprietären Ansätzen notwendige manuelle Konfiguration durch die Selbstlernfähigkeit von NAT-T.

Aber nicht alle Probleme sind damit gelöst: Der Einsatz des Authentication Headers scheitert nach wie vor, da NAT-T den äußeren IP-Header nicht kapselt und somit dieser nicht manipuliert werden darf. Unausgeräumt sind auch noch einige Sicherheitsbedenken im Zusammenhang mit der Verwendung von Klartextmechanismen in IKE-Phase 1.

Dennoch scheint man – dies darf abschließend festgestellt werden – hier seitens der IETF auf einem guten Weg zu sein, zumal der Authentication Header ja ohnehin in vielen Fällen als nicht notwendig oder doch zumindest notfalls verzichtbar eingestuft wird. Wenn jetzt noch das Verfahren endlich Serienreife erlangt und dann auch sauber implementiert wird, steht einem weitestgehend ungehinderten VPN-Einsatz auch in NAT-Umgebungen eigentlich kaum noch etwas im Wege.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
- **10.11. - 14.11.03 Aachen**
- **02.02. - 06.02.04 Aachen**

TCP/IP und SNMP
- **08.12. - 12.12.03 Berlin**
- **02.02. - 06.02.04 Bonn**

Internetworking
- **08.12. - 12.12.03 Aachen**
- **02.02. - 06.02.04 Aachen**

Ethernet Technologien – neuester Stand
- **08.12. - 12.12.03 Aachen**
- **08.03. - 12.03.04 Aachen**

Paketpreis für alle vier Seminare: € 6.690,-- zzgl. MwSt.
(Einzelpreise: € 1.990,--/€ 1.990,--/€ 2.290,--/€ 1.990,--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
- **17.11. - 21.11.03 Aachen**
- **02.02. - 06.02.04 Aachen**

Trouble Shooting in geswitchten Ethernet-Umgebungen
- **10.11. - 14.11.03 Aachen**
- **01.03. - 05.03.04 Aachen**

Trouble Shooting für TCP/IP-und Windows-Umgebungen
- **03.11. - 07.11.03 Aachen**
- **19.01. - 23.01.04 Aachen**

Paketpreis für alle 3 Seminare mit Sniffer-Lizenz:
€ 7.500,-- zzgl. MwSt. (Seminar-Einzelpreise: je € 2.490,--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
- **24.11. - 28.11.03 Berlin**
- **01.03. - 05.03.04 Köln**

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
- **08.12. - 10.12.03 Bonn**
- **22.03. - 24.03.04 Bonn**

Sicherheitslösungen III: Planung und praktische Konfiguration
- **01.12. - 05.12.03 Aachen**
- **19.04. - 23.04.04 Aachen**

Paketpreis: € 4.990,-- zzgl. MwSt.
(Einzelpreise: € 1.990,-- / € 1.690,-- / € 2.290,--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Impressum

Verlag:
Dr. Suppan International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland, Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich, 12 Ausgaben im Jahr

Bezug:
Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie