Dr. Suppan International Institute

Der Netzwerk Insider

Februar 2004

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Voice-over-IP Management

von Dipl.-Inform. Petra Borowka

Mit zunehmender Verbreitung von Telefonie in IP Netzen wurden neue Tools oder Module für existierende Tools mit Funktionen zur Analyse, Überwachung und Verwaltung von Sprachkomponenten in IP Netzen entwickelt. Dies betrifft nicht nur Enterprise sondern auch Carrier Netze und die Schnittstelle zwischen beiden.

Was sollte gemessen werden? Was leisten die Tools? Welche Kombinationen sind sinnvoll?

Der nachfolgende Beitrag gibt einen Überblick über Management-Anforderungen und -Möglichkeiten für den Voice over IP Betrieb.

Dieser Beitrag setzt ein grundsätzliches Verständnis der Funktionsweise von IP Telefonie sowie der Protokolle und Verfahren, die hier zum Einsatz kommen, voraus.

Für eine Einführung in Voice over IP wird auf die Netzwerk Insider vom September und November 2000 verwiesen.

"Quo vadis, VoIP? Der Voice-Markt ist da – aber wo läuft er hin?"

"Quo vadis, VoIP? Der Voice-Markt ist da – was tun die Hersteller?"

weiter Seite 21

...

Zweitthema

Sicherheitsaspekte beim Einsatz von Industrial Ethernet

von Dipl.-Inform. Dietlind Hübner, Dipl.-Ing. Hartmut Kell, Dr.-Ing. Behrooz Moayeri und Dipl.-Ing. Thomas Simon

Mit der Einführung von Industrial Ethernet geht im Industriebereich das Zeitalter kleiner Inselnetze ohne jegliche Online-Verbindung zur Außenwelt zu Ende. Gerade die Möglichkeit, die Offenheit von Ethernet als Standard für Unternehmensnetze zu nutzen und zwischen dem Industriebereich und anderen Bereichen einen Informationsaustausch „in Echtzeit" zu realisieren, birgt jedoch Risiken für die Sicherheit der Industrieprozesse in sich.

Den Autoren sind aus den letzten Monaten zahlreiche Fälle bekannt, in denen der kombinierte Einsatz von Ethernet, IP und marktüblichen Betriebssystemen bei Missachtung der erforderlichen Sicherheitsmechanismen zu ernshaften Sicherheitsvorfällen und erheblichen Beeinträchtigungen von Industrienetzen führte.

Vor dem Einsatz jeder Industrial-Ethernet-Lösung ist zu prüfen, welche Auswirkungen diese Lösung auf die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der ausgetauschten Nachrichten und der betroffenen Daten und Systeme hat.

Durch die Umstellung auf Industrial Ethernet erfolgt ein vollständiger Technologiewechsel, der aus dem Blickwinkel der Sicherheit eingehend zu untersuchen ist.

weiter Seite 6

Top-Event

Das ComConsult IT-Sicherheits-Forum 2004

auf Seite 4

Zum Geleit

Trends 2004: WLAN und Voice

auf Seite 2

Studie des Monats

IP-Telefonie – Cisco versus Siemens

auf Seite 16

Zum Geleit

Trends 2004: WLAN und Voice

Das Jahr 2004 wird viele Veränderungen im Netzwerk-Bereich mit sich bringen. So viel wie seit Jahren nicht mehr. Dabei kommt die wesentliche Motivation für diese Änderungen aus den Bereichen Wirtschaftlichkeit und Umsetzung neuer Applikationen. Doch häufig wird die Tragweite dieser Änderungen unterschätzt. Bei näherer Analyse zeigt sich, dass Änderungen im Kerndesign unserer Netzwerke, veränderte Betriebskonzepte und ein modifiziertes Sicherheits-System die natürliche Folge dieser Entwicklung sind.

Im Bereich Voice gibt es nach wie vor einen erheblichen Investitions-Stau. Viele TK-Verträge sind ausgelaufen oder laufen aus. Doch die Anwender schwanken bisher. Zu deutlich ist, dass die Zukunft des TK-Marktes IP-Telefonie heißt. Aber vielen Anwendern ist unklar, wann, wie und mit wem sie den Einstieg realisieren sollen:

- die Frage des „wann“ wird primär bestimmt von den Faktoren Preisgestaltung und Produktreife. Hier zeigen aktuelle Analysen von ComConsult-Research (siehe die Top-brisante Studie: Cisco versus Siemens), dass die Produktreife einen akzeptablen Stand erreicht hat. Die Preise sind in den letzten Monaten massiv gefallen, mit dem niedrigen Dollar-Kurs haben die amerikanischen Produkte häufig einen Preisvorteil gegenüber europäischen Produkten. Auch weiterhin sind sinkende Preise speziell auf der Endgeräte-Seite zu erwarten

- für viele Einsatzszenarien lässt sich eine erhebliche Wirtschaftlichkeit von IP-Telefonie nachweisen. Das wirtschaftliche Problem ist dabei nicht die IP-Telefonie selbst sondern der Umfang der Umbaukosten für das bestehende Netzwerk und auch das Sicherheits-System

- die Fragen „wann“ und „mit wem“ gehören im deutschen Markt untrennbar zusammen. Die Kernfrage des Marktes ist die Rolle von Siemens im Spagat zwischen traditioneller TK-Technik auf der einen und moderner IP-Technik auf der anderen Seite. Da viele Kunden, gerade mit großen Installationen, den sanften Migrations-Weg anstreben werden (Risiko-Minimierung, Nutzung vorhandener Investitionen), hat Siemens den Vorteil der besseren Alt-Integration auf seiner Seite. Dem steht aber die Ungewissheit der zukünftigen IP-Lösung gegenüber. Hier zeigt gerade die aktuelle Studie von ComConsult-Research, dass mit der HiPath 8000 auch im Hause Siemens ein großer Softswitch zunehmend im Enterprise-Markt positioniert wird. Parallel steht mit der Version 2 der HiPath-Software ein wesentlicher Funktionswechsel ins Haus, der auch Rückwirkungen auf IP-Telefonie hat. Die Kunden stellt das vor die Frage: weiter warten, jetzt einsteigen, bei Siemens bleiben, doch einen Wechsel zu einem anderen Hersteller wagen.

In Summe wird das Jahr 2004 ein Voice-Jahr werden. Bereits jetzt gibt es erhebliche Mengen an Projekten, speziell in den mittelständischen Umgebungen, die mit deutlichen wirtschaftlichen Vorteilen rechnen können (zum Beispiel: Filialorgansiationen).

Der zweite Motor des Netzwerk-Marktes 2004 sind WLANs. Hier boomt das Geschäft. Spannend sind dabei aber nicht die vielen kleinen WLAN-Inseln sondern die großen Projekte, die im Rahmen neuer Nutzungsformen deutliche Kostenvorteile sowohl in der Beschaffung als auch im Betrieb bieten. Typische Beispiele für wirtschaftliche Vorteile mit ROI-Zeiten von deutlich unter einem Jahr sind:

- Installation von WLANs in Filialorganisationen. WLANs als Basis eines Filialnetzes haben erhebliche Vorteile: kein Change-Aufwand, gute Möglichkeiten der Remote-Administration, geringe Installationskosten auch in komplexen Umgebungen. Man kann allgemein sagen: WLAN-Technik ist eine fast perfekte Netzwerk-Technik für kleine Filialen, Vertriebsbüros, Niederlassungen etc.

- Installation im Logistik und Produktionsbereich: Ersatz von Bündelfunk-Syste-men, Vermeidung aufwendiger Verkabelungen in teuren Produktionsumgebungen, jede Menge Sonder-Projekte mobiler Kommunikation. Hier schaffen WLANs einen deutlichen Mehrwert

- Neue Service- und Betriebs-Abläufe im Gesundheitswesen. Mobile Endsysteme ermöglichen erhebliche Rationalisierungen im Gesundheitssystem

- Großraumflächen oder allgemein Flächen mit schwieriger und teurer Verkabelung: keine Change-Kosten, geringe Investkosten und seit der Verfügbarkeit von 54 Mbit/s ein deutlich verringerter Bedarf an Access Points führen zu sehr wirtschaftlichen Lösungen

Doch kein Licht ohne Schatten. Diese Entwicklung hat Rückwirkungen auf unsere bestehenden Netzwerke. Diese müssen auch bei der wirtschaftlichen Berechnung berücksichtigt werden. Speziell betroffen davon sind:

- das Design- und Strukturprinzip. Mit immer neuen Anwendungen entsteht die Frage, in welchem Umfang diese voneinander geschützt werden müssen. Dies betrifft Sicherheitsfragen aber auch Themen wie Sabotage, Auswirkung von Fehlern. Wie stark muss ein bestehendes Design angepasst werden, um diesen Anforderungen gerecht zu werden?

- mit neuen Anwendungen und insbesondere der Übertragung von Sprache entstehen neue Sicherheits-Themen. Wie kann ein Abhören eines Telefon-Gesprächs verhindert werden, in wie weit muss ein unerlaubter Zugang zum Netzwerk generell verhindert werden, wie relevant sind Verfahren wie 802.1x oder Weiterentwicklungen (siehe UPN von Enterasys).

- reicht die Kapazität bestehender Netzwerke aus? Vergleicht man das Design neuer Netzwerke unter Nutzung der Eigenschaften moderner Switch-Systeme (zum Beispiel 4 statt 2 GBIC/LWL-Ports, Einsatz von LACP) mit älteren Netzwerken, dann sieht man doch deutliche Unterschiede. Wenn aber ein neues Design so viel anders ist, ist dann das alte noch tragfähig oder muss nachgebessert werden?

- Netzwerk-Betrieb wird deutlich aufwendiger. Auf der einen Seite steht die deutliche Ausweitung der Betriebszeiten. 5/7x24 Stunden ist der klare Trend. Auf der anderen Seite die zunehmende Komplexität gerade durch die Integration völlig anders strukturierter Verkehrsströme. Wie passt das übereinander? Hier muss der bestehende Betrieb und auch die Toolsausstattung in Frage gestellt werden, neue Betriebskonzepte sind gefordert

Als Fazit bleibt festzustellen, dass 2004 ein Netzwerk-Jahr werden wird. Derartig massive Veränderungen hat es seit Jahren nicht gegeben. Positiv sind die wirtschaftlichen und applikatorischen Vorteile, die damit geschaffen werden. Der Preis besteht in der Notwendigkeit, die Tragfähigkeit der bisherigen Netzwerke zu prüfen.

Alle diese Themen diskutieren wir auf dem Netzwerk-Redesign-Forum 2004 Ende März in Königswinter. Ich freue mich auf eine lebhafte und kontroverse Diskussion.

Ihr Dr. Jürgen Suppan

drsuppan@comconsult-research.com

Top-Event

Netzwerk-Redesign Forum 2004

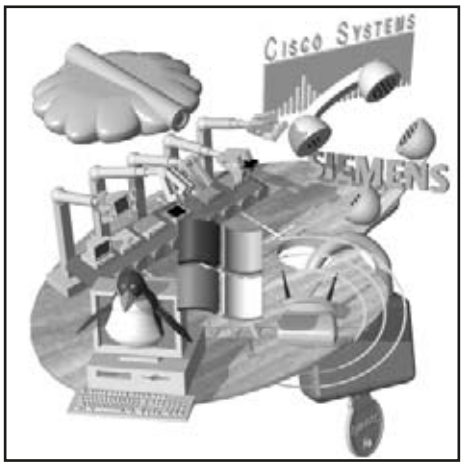
Vom 29. März bis 1. April veranstaltet die ComConsult Akademie im Maritim Hotel Königswinter das Netzwerk-Redesign Forum 2004.

Wie in jedem Jahr so wird sich hier auch 2004 die Branche treffen. Die Mischung aus herstellerneutralen Top-Referenten, den neuesten Technologie-Entwicklungen, hochaktuellen Projekterfahrungen und direkt umsetzbaren Empfehlungen aus der Praxis, einer hochaktuellen Ausstellung, der gleichzeitigen Anwesenheit vieler relevanter Hersteller hat diesen Kongress zum jährlichen Treffpunkt der Branche gemacht.

Dieser Spitzenkongress bietet auch in diesem Jahr wieder hochaktuelle Themen:

Standardisierung und Technologie-Entwicklung:
- Was passiert hinter den Kulissen, was ist neu, wie relevant ist es?
- Welche neuen Standards sind verabschiedet, welche stehen vor der Tür?
- Was passiert in den Labors der Hersteller?

Optimierung des Netzwerk-Betriebs:
- Wie kann ein Netzwerk besser betrieben werden?
- Welche neuen Management-Konzepte gibt es?
- LAN-Analyse im Umbruch



Netzwerk-Redesign Forum 2004:
Analyse und Übersicht der aktuellsten Netzwerk-Technologien und Marktentwicklungen

Hersteller und Produkte:
- Wie positionieren sich die Hersteller?
- Wie entwickeln sich wichtige Netzwerk-Produkte?
- Welche Vorteile können genutzt werden?

Sicherheit und Netzwerke:
- Welchen Stellenwert haben Sicherheits-Lösungen im Netzwerk?
- Netzwerk, Server, Applikation: wo wird Sicherheit am besten umgesetzt?
- Effizienter SmartCard-Einsatz: vom VPN zur Mail-Verschlüsselung

RZ-Strukturen 2004:
- Integration Server und Netzwerk
- Neue Anforderungen an IP-Management
- Welche Anforderungen an Verzeichnis-dienste und IP-Ma-nagement generiert die neue Generation von Active Directory?
- Integration der Benutzer-Verwaltungen von Windows und Linux

Auch in diesem Jahr besteht die Möglichkeit, die Veranstaltung 3-tägig oder 4-tägig zu buchen. Am 4. Tag bieten wir den Teilnehmern Spezial-Workshops zu ausgesuchten Top-Themen. Dabei wird der Stand der Technik und der optimale Betrieb wichtiger Technologien intensiv über den ganzen Tag evaluiert. Die Teilnehmer können dabei zwischen den Workshops wechseln. Zurzeit sind folgende Workshops geplant:

Workshop IP-Telefonie

Workshop Sicherheit

Workshop Wireless LAN

Netzwerk-Redesign Forum 2004
29.03. - 01.04.04 in Königswinter

Fax-Antwort an ComConsult 02408/955-399

Kongress-Anmeldung

Ich melde mich an für das
Netzwerk-Redesign Forum 2004

☐ **vom 29.03. - 01.04.04 mit Workshop**
zum Preis von € 1.990,-- zzgl. MwSt.

☐ **vom 29.03. - 31.03.04 ohne Workshop**
zum Preis von € 1.690,-- zzgl. MwSt.

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Thema

ComConsult IT-Sicherheits-Forum 2004

Vom 10. bis 13. Mai veranstaltet die ComConsult Akademie im Maritim Hotel Königswinter das IT-Sicherheits-Forum Forum 2004.

In den letzten Jahren hat sich diese Veranstaltung zu einem unbedingten „MUSS" für jeden Sicherheitsinteressierten entwickelt. An insgesamt vier Tagen werden angeboten:

- Hintergründe zu aktuellen Sicherheitsvorfällen
- Trends und Marktentwicklungen bei Sicherheitstechnologien
- Produktvergleiche und Fallstudien
- Tutorien und Workshops

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei Tutorien (IT-Sicherheit im Überblick, zwei Fachthemen). Am 2. und 4. Tag werden durch erfahrene

Referenten aktuelle fachliche Entwicklungen und Praxisbeispiele vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu speziellen Themen vorbehalten. Da diese parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Das ComConsult IT-Sicherheits-Forum zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit Live durchgeführten Produktvergleichen hat einen hohen praktischen Wert für die Teilnehmer. Daneben werden aber auch neue Entwicklungen aufgezeigt, die sowohl Bedrohungen als auch Gegenmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in interne Geschäftsabläufe, da hier nach aller Erfahrung immer noch die größten Defizite anzutreffen sind. Damit spricht das ComConsult IT-Sicherheits-Forum sowohl Techniker als auch Manager an.

10 % Frühbucherrabatt bis 31.03.04

IT-Sicherheits-Forum 2004

10.05. - 13.05.04 in Königswinter

4 Tage IT-Sicherheits-Forum 2004 mit Tutorium zum Preis von € 1.750,-- statt regulär € 1.990,-- zzgl. MwSt.

3 Tage IT-Sicherheits-Forum 2004 ohne Tutorium zum Preis von € 1.485.-- statt regulär € 1.690,-- zzgl. MwSt.

Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Kongress-Anmeldung

Ich melde mich an für das
ComConsult IT-Sicherheits-Forum 2004

☐ **vom 10.05. - 13.05.04 mit Tutorium**
zum Preis von € 1.750,-- zzgl. MwSt.*

☐ **vom 11.05. - 13.05.04 ohne Tutorium**
zum Preis von € 1.485,-- zzgl. MwSt.*

*Frühbucherpreise gültig bis 31.03.04

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

IT-Sicherheits-Forum 2004

ComConsult IT-Sicherheitsforum 2004 – Die Themen

Sicherung der Netzgrenzen
- Firewalls allein reichen nicht, was sollte man noch einsetzen?
- Einsatz von VPN/RAS mit unterschiedlichen Techniken
- Kritischer Übergang zwischen DMZ und LAN
- Sicherung von „inbound“ und „outbound“ Verbindungen

Sichere Nutzung von WLANs
- Neue Sicherheitsstandards im WLAN-Bereich
- Strategien für "offene" und abgeschirmt betriebene WLANs
- Wie behandelt man unterschiedliche Nutzergruppen (Interne, Externe etc.)

Mobility unter Sicherheitsaspekten
- Sicherung des mobilen Endgerätezoos: Notebook, PDA, MDA, Handy
- Wie geht man mit dem Wunsch nach Hot-Spot-Nutzung um?
- Wie sichert man WLAN- und Bluetooth-Schnittstellen?
- Integrierte Produkte mit Personal Firewall, AV und Dateiverschlüsselung

Webanwendungen mit gravierende Risiken
- Neueste (katastrophale) Ergebnisse von Security-Audits
- Sicherheitshinweise für Entwickler von WA
- Proxy-Ansatz zur externen Sicherung von WA
- Ist der Einsatz von XML Web Services überhaupt zu vertreten?

Content-Security: Umgang mit gefährlichen Inhalten
- Anatomie neuer Viren und Würmer
- Zentrale und dezentrale Sicherheitsmaßnahmen
- Wie kann man auch verschlüsselte Verbindungen kontrollieren?

Mailverschlüsselung
- Warum wird sie bisher eher selten eingesetzt?
- Erfolgt jetzt der Schwenk auf serverbasierte Mailverschlüsselung?
- Neue Sicherheitsstandards (Bundesregierung, VDEW etc.)
- Neue Produkte (PGP Enterprise, S/MIME-Gateways etc.)

Sicherheitsstrukturen für interner Netze
- Kann man aus Sicherheitssicht noch transparente Konzernnetze vertreten?
- Konzepte zum Aufbau interner Segmentierung
- Einbindung von Rechenzentren
- Wie bindet man externe Gäste temporär in das interne Netz ein?

Patch- und Updatemanagement
- Wie kann man mit Informationsflut und Verteilproblematik begegnen?
- Warum es nicht immer sinnvoll ist, Patches sofort einzuspielen
- Patchverteilung im Windowsumfeld (SUS oder was?)
- Wie behandelt man Server? Freigabeproblematik bei Kaufanwendungen

Linux und Windows
- Ist Open Source sicherer als Closed Source?
- Kann Linux im Client -/ Server -Bereich empfohlen werden?
- Sind kombinierte Lösungen sinnvoll?

Security Awareness und Governance
- Einbeziehung der IT-Prozesse in das interne Kontrollsystem
- Bekanntmachung und Durchsetzung einer SecPol im Konzernumfeld
- Durchführung einer Security Awareness-Kampagne

Kosten/Nutzen-Betrachtungen zur IT-Sicherheit
- Mit welchen Argumenten sind Geldgeber zu überzeugen?
- Qualitative vs quantitative Ansätze zur Kostenrechtfertigung
- Lässt sich ein Return-of-Security-Investment (RoSI) berechnen?

Security Management
- Welche übergreifenden Lösungen gibt es?
- Integration von Frühwarnsystemen
- Korrelation von Events über Herstellergrenzen
- Aufgaben einer Alarmzentrale

Weitere vorgesehene Themen
- Intrusion Detection / Prevention
- Security Outsourcing
- Auditierung, Zertifizierung
- Security Policy, Risikoanalyse

Der Veranstalter behält sich Änderungen im Programm vor

Zweitthema

Sicherheits-aspekte beim Einsatz von Industrial Ethernet

Fortsetzung von Seite 1

Das Autorenteam:

Dipl.-Inform. Dietlind Hübner,
huebner@comconsult.com

Dipl.-Ing. Hartmut Kell,
kell@comconsult.com

Dr.-Ing. Behrooz Moayeri,
moayeri@comconsult.com

Dipl.-Ing. Thomas Simon
simon@comconsult.com

Um die Sicherheit von Industrial Ethernet korrekt bewerten zu können, muss man berücksichtigen, dass jede IT-Lösung auf die drei Komponenten Applikation, Systeme und Netz angewiesen ist. Auf allen diesen drei Ebenen können Sicherheitsmechanismen implementiert werden. Im Folgenden wird auf die Sicherheitsmechanismen für Industrial Ethernet auf allen diesen drei Ebenen eingegangen.

Applikationsebene

Die Applikationsebene im Bereich Industrial Ethernet ist sehr vielfältig und vielschichtig. Daher kann nachfolgend nur exemplarisch auf wenige (auch im industriellen Bereich mittlerweile verbreitete) Anwendungsplattformen eingegangen werden, darunter Web, SQL und Terminalserver.

Web-Sicherheit

Die Web-Technologie wird immer wichtiger. Die Web-Nutzung überwiegt im weltweiten Internet und ist die Grundlage von unternehmensweiten Intranets, die zunehmend in den Industriebereich Einzug finden. Dabei ist die Web-Technologie zum Teil unausgereift, zumindest was die Sicherheit betrifft.

Das HTML-Format wird auch in E-Mails verwendet, d.h. E-Mails können potenziell gefährliche Inhalte beinhalten, so dass der E-Mail-Client ohne Rückfrage beim Benutzer einen Code ausführen kann, der in einer empfangenen E-Mail enthalten ist. Beispiele für die Gefährdungsquellen sind Makros, ActiveX-Objekte, schadensstiftende Scripts und Trojanische Pferde.

Die Bestandteile der Web-Sicherheit sind die Sicherheit des Web-Servers und seiner Inhalte, die Sicherheit des Datenstroms zwischen Server und Browser vor Preisgabe, Manipulation und Zerstörung, die Sicherheit des Computers, auf dem der Browser läuft, die Authentifizierung des Benutzers dem Server gegenüber und umgekehrt und die Unbestreitbarkeit der Transaktionen (insbesondere wichtig bei revisionspflichtigen Vorgängen).

Die ganze Kette ist so stark wie das schwächste Glied. Die stärkste Verschlüsselung bei der Transaktion nutzt wenig, wenn die Daten vom Server entwendet werden können. Ein gut abgesicherter Web-Server nutzt wenig, wenn das darunter liegende Betriebssystem Sicherheitslücken aufweist.

Der Zustand der Web-Sicherheit hat sich in den letzten Jahren ständig verbessert. Die Web-Server-Sicherheit und die sichere Übertragung der Daten im Rahmen der Web-Nutzung mittels Secure Socket Layer (SSL) ist nunmehr eine etablierte Technik, die zumindest bei nicht-zeitkritischen Web-Anwendungen im Industriebereich genutzt werden sollte, wenn die Anforderungen an die Integrität der Systeme und Daten und/oder Vertraulichkeit der übertragenen Informationen hoch sind.

Seminar zum Thema

Sicherheits-Lösungen: Von den Einzelbausteinen zur Integrierten Lösung

Seminar

01.03. - 05.03.04 Köln
03.05. - 05.05.04 Zürich
24.05. - 28.05.04 Köln

Dieses Seminar vermittelt, aus welchen Bausteinen eine effiziente Sicherheits-Lösung aufgebaut wird, welche Bausteine unverzichtbar sind und wie diese Bausteine konfiguriert werden. Jeder einzelne Baustein wird detailliert erklärt und in seinen Potenzialen beschrieben. An vielen typischen Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.
Referenten: Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hans-Peter Mohn,
Einzelpreis: € 2.290,-- zzgl. MwSt.

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

Sicherheitsaspekte beim Einsatz von Industrial Ethernet

In den letzten Jahren blieben nur diejenigen Systeme von Vorfällen wie wiederholten Verbreitungen von Viren und Würmern verschont, auf denen eine sichere Konfiguration eingestellt ist.

Aktive Web-Inhalte können den Client gefährden, indem sie auf lokale Dateien und Ressourcen zugreifen, Sicherheitslücken von Helper-Applikationen ausnutzen, ohne Beteiligung des Benutzers sich auf der lokalen Maschine einnisten, ohne Wissen des Benutzers im Speicher der lokalen Maschine verbleiben, Programme auf der lokalen Maschine manipulieren, auf andere Browserfenster auf der lokalen Maschine zugreifen, neue Prozesse auf der lokalen Maschine kreieren oder mit Drittrechnern kommunizieren. Diese umfangreiche Funktionalität wird heute durch die Web-Browser ermöglicht. Je mehr von dieser Funktionalität aktiviert wird, desto größer sind die Risiken für die Sicherheit des Clients. Daher lautet die Grundregel auch bei der sicheren Konfiguration von Web-Clients: Sicherheit durch Vereinfachung und Verzicht auf nicht dringend benötigte Funktionalität.

Mobile Code bedeutet, dass Programme von unbekannter Quelle auf den Maschinen der Benutzer ausgeführt werden. Diese Ausführung erfolgt ohne explizites Handeln (und Wissen) des Benutzers. Die Vorteile bestehen darin, dass maschinenunabhängiger und portierbarer Code zum Einsatz kommen kann. Aus der Sicht der Sicherheit entsteht jedoch der Nachteil, dass man einer unbekannten Quelle vertraut.

Das zu empfehlende Sicherheitskonzept für Web Clients basiert auf einer Klassifizierung der Web Sites in unterschiedlich zu behandelnde Kategorien. Zum Beispiel kann ein Administrator mithilfe eines solchen Konzeptes bestimmen, dass innerhalb des Industriebereiches die Web-Server vertrauenswürdig sind und Mobile Code auf den Clients zur Ausführung bringen können, während den Web-Servern außerhalb dieses Bereiches diese Möglichkeit entzogen wird.

Sicherheit von SQL-Servern

Im Januar 2003 startete einer der bis dahin größten Angriffe auf das Internet und der daran angeschlossenen Windows-basierenden Server. Der als „Slammer“ bzw. „Sapphire“ bekannt gewordene Internet-Wurm legte durch exzessives Versenden einer Vielzahl von Paketen einige wichtige Internet-Knoten für Stunden lahm. Tausende Rechner, auf denen der Microsoft SQL Server 2000 oder MSDE 2000 (Microsoft Data Engine) installiert waren, wurden von dem Wurm befallen und sendeten Pakete an weitere Rechner. Dabei handelte es sich um Systeme, die einen zum Zeitpunkt des Angriffs ungefähr ein halbes Jahr alten Patch von Microsoft noch nicht eingesetzt hatten.

Dieser Angriff machte im großen Maßstab deutlich, dass einige sehr weit verbreitete Standardanwendungen und –dienste weitgehend ungeschützt sind. Dabei sind Angriffe über SQL (Structured Query Language, Abfragesprache für den Zugriff auf Datenbanken) schon seit Jahren bekannt. SQL-Server dürfen nicht auf Windows Domain Controllern installiert werden, da so genannte Extended Store Procedures (XPs) für Zugriffe auf das Betriebssystem missbraucht werden können; bei Domain Controllern gefährdet dies die Authentifizierungsinformationen.

Auf allen SQL-Servern sollten unnötige, jedoch mächtige XPs gelöscht werden (z. B. xp_cmdshell, der eine Verzweigung zum Standardbefehlsinterpreter des Betriebssystems und damit die Ausführung beliebiger Befehle ermöglicht).

SQL Server sind möglichst mit eingeschränkten Rechten zu installieren. Ein eigenes Benutzerkonto sollte für einen SQL-Server eingerichtet werden.

Terminalserver

Eine auch im Industriebereich verbreitete Anwendung ist der Terminalserver (TS). Er wird für den Fernzugriff auf Windows-Rechner eingesetzt. Diese Funktionalität wurde bereits für einige Angriffe missbraucht.

Um solche Angriffe abzuwehren, sind Maßnahmen erforderlich, auf die im Folgenden eingegangen wird:

- Die Bezeichnung des Standard-Web-Formulars für die TS-Authentifizierung (TSWeb\default.htm) ist zu ändern und dafür zu sorgen, dass diese Standardbezeichnung nirgendwo in untrusted-Umgebungen auftaucht.
- Die Portnummer des TS muss geändert werden (Standard ist 3389).
- Auf dem TS selbst sollte man das Konto des lokalen Administrators umbenennen.
- Der Zugang der Benutzer ist mittels Appsec-Tool auf bestimmte Applikationen zu beschränken.
- Der TS sollte in der Verzeichnisstruktur als eigene OU implementiert werden.

Seminar zum Thema

Sicherheits-Lösungen: IP-VPNs, der Kern einer Sicherheits-Infrastruktur

Seminar

22.03. - 24.03.04 Bonn
28.06. - 30.06.04 Köln

Das Seminar beschäftigt sich mit den Nutzungsformen, den Realisierungs-Alternativen und der Integration in bestehende Netzwerk-Infrastrukturen von VPN-Technologie, wie z.B. die optimale Kombination eines VPN-Servers mit Firewall/Routing/NAT oder die Klärung der Microsoft-spezifischen Fragen auf den Client-PCs (Interoperabilität, Anmeldung, Namensauflösung)
Referenten: Dipl.-Inform. Andreas Meder, Alexander Zarenko
Einzelpreis: € 1.690,-- zzgl. MwSt.

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

Sicherheitsaspekte beim Einsatz von Industrial Ethernet

Systemebene

Bei den bisherigen Felbussen sind die Möglichkeiten eines potenziellen Angreifers, auf die Systeme von außen zuzugreifen, äußerst eingeschränkt. Die Situation bei Industrial Ethernet ist völlig anders. Ethernet/IP-Netze sind universal nutzbare Kommunikationsmedien, die auch für Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systeme auf vielfältige Weise missbraucht werden können. Daher muss bei jeder Ethernet/IP-Komponente der erforderliche Schutz vor Angriffen über das Netz implementiert werden.

Die im Folgenden dargestellten Maßnahmen sind nur ein Ausschnitt aus dem Mindestumfang an Sicherheitsmechanismen, die bei Systemen mit Anschluss an Ethernet/IP-Netze implementiert werden müssen. Ausführlichere Maßnahmenkataloge müssen Gegenstand entsprechender Sicherheitskonzepte jedes Unternehmens sein.

Benutzerrechte

Auf allen im Prinzip offenen Systemen im Industriebereich (Windows, Unix, Linux) sind Benutzer einzurichten. Dabei gelten die bei allen offenen Systemen zwingend erforderlichen Maßgaben für die Benutzer, u. a.:

- Es ist zu klären, welche Mitarbeiter unter welchen Voraussetzungen und Umständen auf welche Systeme physikalischen Zugriff haben dürfen (namentliche Bestimmung).
- Der Zugriffsbereich jedes Benutzers ist möglichst einzuschränken.
- Jeder Benutzer darf nur so viele Rechte wie nötig und so wenige Rechte wie möglich erhalten.

Passwörter

Jeder Benutzer, der auf ein System zugreift, muss sein eigenes, durch ein eigenes Passwort abgesichertes Konto haben. Gruppen- oder Funktionskonten sind zu vermeiden. Statt dessen sollten Gruppen eingerichtet werden, wenn mehrere Benutzer auf die selben Ressourcen zugreifen müssen.

- Alle Konten sind durch Passwörter zu schützen.
- Passwörter dürfen nicht in Automatismen eingebaut werden.
- Es sind Regeln für starke, nicht-triviale Passwörter aufzustellen und allen Benutzern mitzuteilen. Die Benutzer sind über bewährte Methoden für die Wahl von nicht trivialen Passwörtern aufzuklären, z. B. über die Bildung von Passwörtern unter Verwendung der Anfangsbuchstaben der Wörter eines Satzes.
- Das Notieren von Passwörtern auf Papier ist zu untersagen.
- Passwort-Aging ist einzuführen.

Härten von Systemen

An Industrial Ethernet angeschlossene Knoten basieren oft auf Standardbetriebssystemen mit den einschlägig bekannten Sicherheitsschwächen und –lücken. Diese Systeme sind durch eine „Härtung“ abzusichern. Zu den Härtungsmechanismen gehören folgende Maßnahmen:

- Jeder nicht benötigte IP-Service auf einem System ist zu deaktivieren.
- Security-Scanner sind zur Prüfung von innen und außen (über das Netz) einzusetzen, um ggf. die Präsenz von Sicherheitslücken festzustellen.
- TCP-Wrapper und Systembasierende Firewalls zum besseren Schutz der TCP-Services können optional eingesetzt werden.
- Zur Prüfung von Systemdateien und anderen kritischen, keinen schnellen Änderungen unterliegenden Dateien und Verzeichnissen können prüfsummenbildende Programme eingesetzt werden.
- Eine manuelle und automatische Log-Auswertung ist zwingender Bestandteil der Sicherheitsmechanismen auf den Systemen.

Der Prozess der Entfernung nicht benötigter Dienste und Funktionen ist einer der wichtigsten Bestandteile der Phase nach der Grundinstallation. Diese Phase wird als die Phase der Härtung der Systeme bezeichnet. Wichtige Aspekte bei der Härtung von Systemen sind u. a.:

- Entfernung unnötiger Dateien und Features
- Physikalischer Schutz (Zutrittsschutz etc.)
- Konto- und Passwortrichtlinien
- Entfernung unnötiger Dienste
- SNMP: Die SNMP-Standardeinstellung bei Servern ist sehr unsicher und muss geändert werden (Änderung der Default Community Strings etc.).

Seminar zum Thema

Sicherheits-Lösungen: Planung und praktische Konfiguration

Praxis-Seminar

19.04. - 23.04.04 Aachen
19.07. - 23.07.04 Aachen

Dieses Praxis-Seminar vermittelt den praktischen Umgang mit Firewall, VPN, Windows-Sicherheit und WLAN-Sicherheit. Im Rahmen von praktischen Live-Übungen werden typische Konfigurationen analysiert und vermittelt. Als Übungsbasis stehen typische Produkte des Marktes zur Verfügung
Referenten: Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hans-Peter Mohn, Christian Osterbrink und Alexander Zarenko
Einzelpreis: € 2.290,-- zzgl. MwSt.

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

Sicherheitsaspekte beim Einsatz von Industrial Ethernet

Mehrstufiges Backup-Konzept

Bei Entdecken von Angriffen ist die Verfügbarkeit von Backups außerordentlich wichtig. Alle Daten aller Systeme sind regelmäßig einem Daten-Backup zu unterziehen.

Darüber hinaus sind Papier-Ausdrucke wichtiger Konfigurationsdateien vorzuhalten.

Die Regeln eines sachgerechten Backups sind einzuhalten, wie z.B. abwechselnde Nutzung von mehreren Bändern, Nutzung von Bändern nur bis zur maximalen Anzahl von Überschreibungen, Durchführung von regelmäßigen Restore-Tests, physikalischer Schutz für Backup-Bänder, Auslagerung der Bänder auf einen anderen Standort als der Rechner-Standort, sicherer Transport der Bänder derart, dass nur vertrauenswürdiges Personal auf die Bänder Zugriff hat etc.

Zusatzwerkzeuge

Alle Infektionswege für die Ausbreitung von Viren und sonstiger schadensstiftender Software sind auch auf Systemen zu kontrollieren, die an Industrial Ethernet angeschlossen werden. Dazu gehören Datenträger, Mail-Services etc. Die notwendigen Scanner sind auf Servern und Clients vorzusehen. Zusätzlich sind sichere Systemeinstellungen für die Verhinderung der Ausbreitung von schadensstiftender Software unerlässlich.

Unverzichtbarer Bestandteil der Sicherheitsmechanismen sind Virenscanner. Zurzeit gibt es über 80.000 unterschiedliche Computerviren, Trojanische Pferde und gefährliche Internetprogramme. Tausende Angreifer versuchen heimlich in Computersysteme einzudringen. Angesichts der Verschärfung der Problematik in den letzten Jahren und der Tatsache, dass pro Woche bis zu 200 neue Viren erscheinen, ist eine IT-Umgebung ohne Virenschanner aus der Sicht der Security nicht zu verantworten, auch nicht im Bereich Industrial Ethernet.

Im Zusammenhang mit der Ereignisüberwachung sind Tools für die Log-Auswertung von großer Bedeutung, da die manuelle Auswertung von Ereignisprotokollen einen großen Aufwand verursacht. Zu den Werkzeugen für die automatische Auswertung von Ereignisprotokollen gehören die folgenden Produkte:

- NTLast von Foundstone (freeware)
- VisualLast von Foundstone (GUI-Version, kommerziell vertrieben)
- Event Log Monitor (ELM) von TNT
- EventAdmin von Aelita Software

Netzebene

Dadurch, dass mit den bisher verfügbaren Industrial-Ethernet-Produkten kaum Sicherheitsmechanismen auf der Applikationsebene implementiert sind und die im letzten Abschnitt erwähnten Maßnahmen zur Absicherung der Systeme nur einen Teil der Angriffstypen abwehren können, müssen bei Einsatz von Industrial Ethernet geeignete Maßnahmen auf der Netzebene getroffen werden.

Diese Maßnahmen sind zum größten Teil als zusätzlicher Aufwand für die Implementierung und Betrieb von Industrial Ethernet zu verstehen, da sie nicht zum standardisierten Maßnahmenkatalog für die Absicherung der Netze gehören.

In den meisten Unternehmen muss die Vertraulichkeit der übertragenen Informationen durch deren Einstufung auf Applikations- oder Systemebene unterstützt werden, da die Differenzierung auf der Netzebene mit einem zu hohen Aufwand verbunden wäre. Gleiches gilt für die Authentizität des Kommunikationspartners. Weiterhin ist die Zugriffskontrolle und Rechteprofilverwaltung für Benutzer außerhalb der Zuständigkeit des Netzes.

Da somit die unternehmensinternen IP-Netze weitgehend als offene Netze gestaltet werden, müssen die zumindest bisher festzustellenden Sicherheitsdefizite auf der Ebene der Applikation durch Zusatzmaßnahmen auf der Netzebene geschlossen werden.

Auf die wichtigsten Sicherheitsmechanismen auf Netzebene, die auch für Industrial Ethernet relevant sind, wird im folgenden eingegangen.

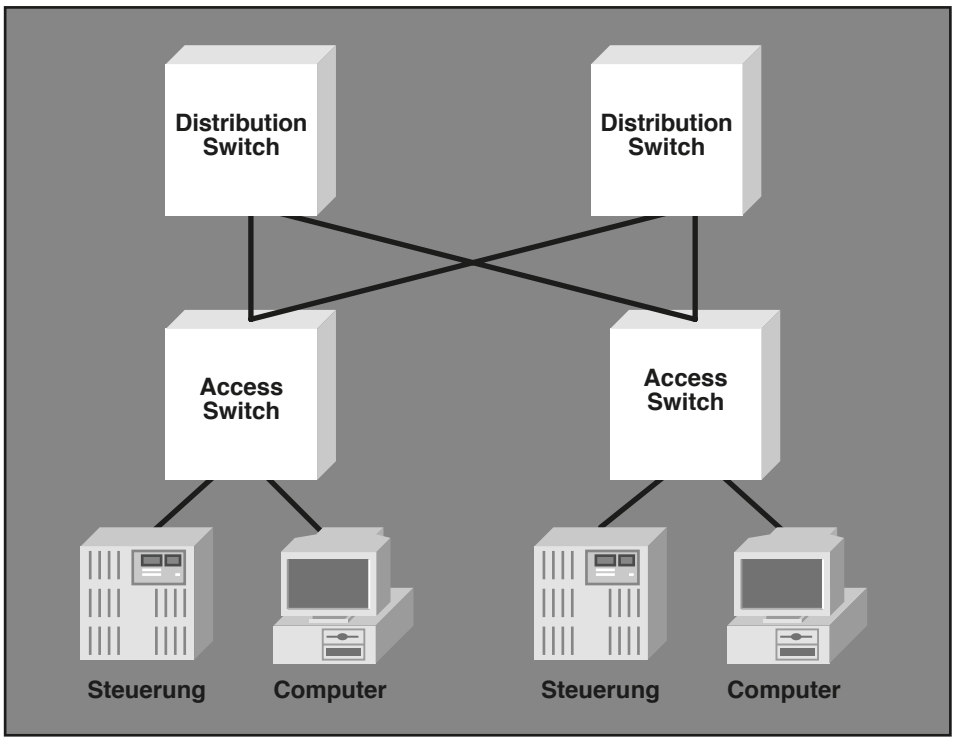
Netztrennung als Sicherheitsmechanismus

Alle Unternehmen, in denen potenziell oder bereits in der Praxis Industrial Ethernet zum Einsatz kommt, betreiben auch Netze für herkömmliche Büroapplikationen oder kaufmännische Applikationen. Eine Kopplung zwischen den beiden Bereichen „Industrie“ und „Büro“ ist in den meisten Fällen erforderlich, ja sogar einer der Gründe für die Einführung von Industrial Ethernet.

Der Aufbau von Industrial-Ethernet-Umgebungen ist nach den folgenden grundsätzlich denkbaren Varianten möglich:

Variante 1: Industrie- und Büronetz werden vollständig integriert. Zugriff von jedem System auf das andere ist im integrierten Netz möglich. Industrie- und Büroendgeräte werden an die selben Access-Komponenten angeschlossen. Bei dieser Variante können alle möglichen Störungen aus dem Büronetz (z. B. Broadcasts) das Industrienetz beeinträchtigen.

Bild 1: Industrienetz Variante 1



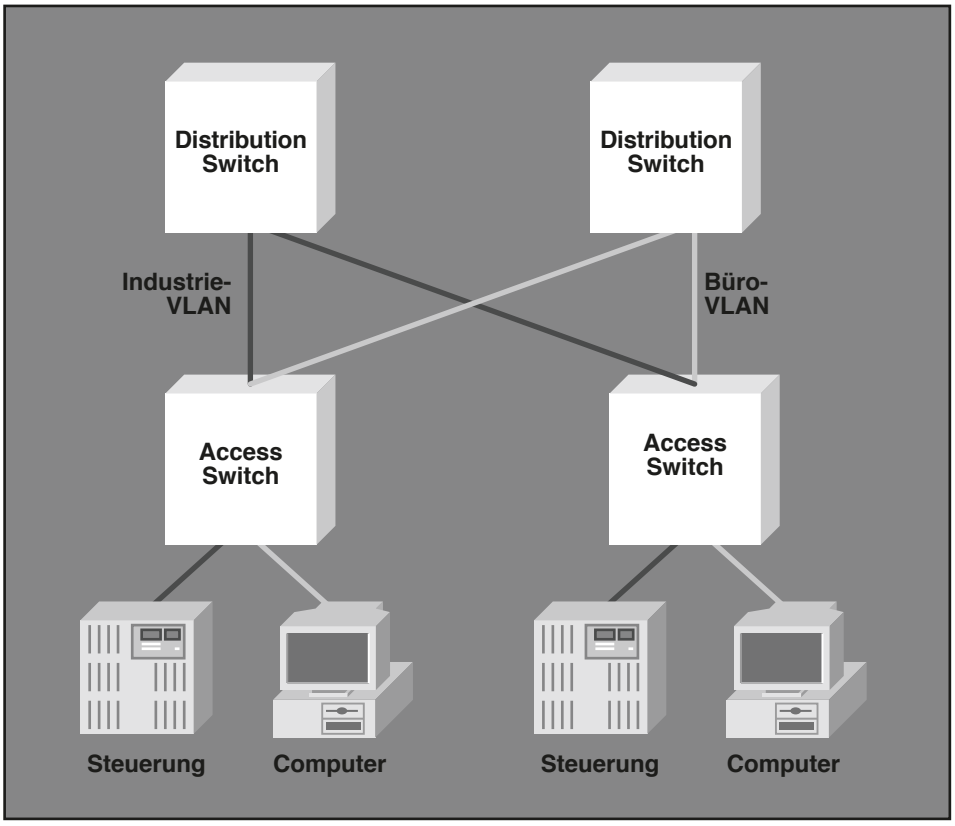
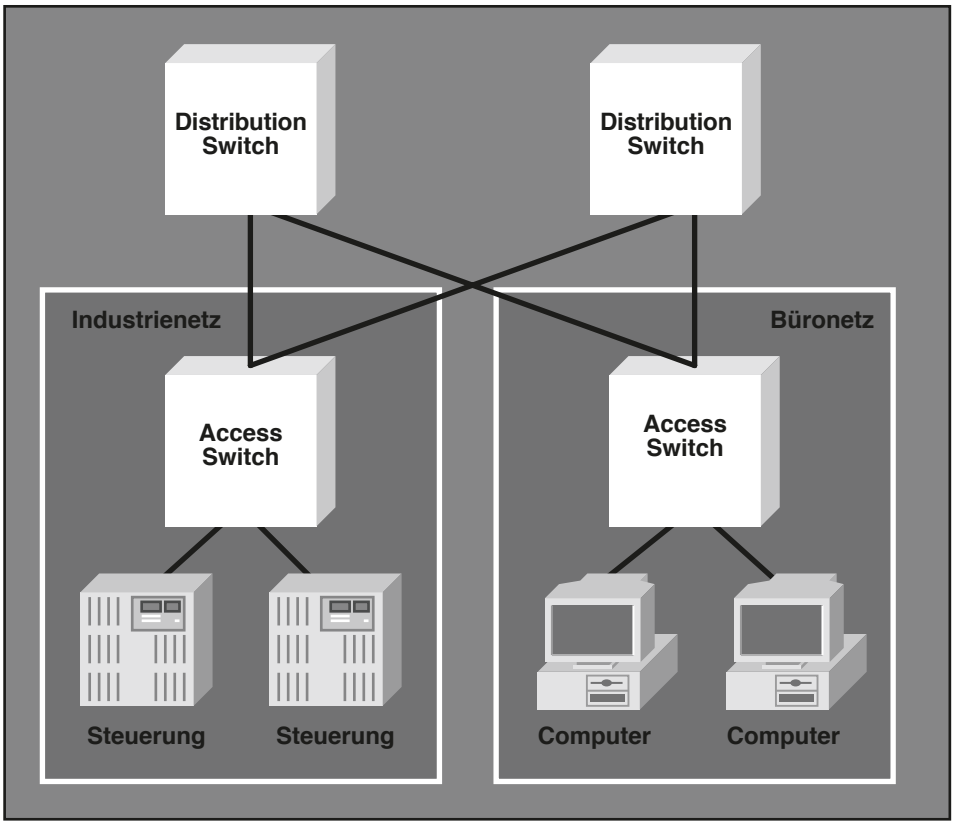


Bild 2 (oben): Industrienetz Variante 2

Bild 3 (unten): Industrienetz Variante 3



Variante 2: Industrie- und Büroendgeräte werden zwar an die selben Access-Komponenten, jedoch an unterschiedliche Broadcast-Domänen angeschlossen. Broadcasts aus dem Büronetz beeinträchtigen das Industrienetz nicht. Jedoch kann es vorkommen, dass Büroanwendungen temporär die gesamte Bandbreite in Teilen des Netzes in Anspruch nehmen und dadurch für die Industrieumgebung wichtige Anwendungen beeinträchtigen.

Variante 3: Industrie- und Büroendgeräte werden an unterschiedliche Access-Komponenten angeschlossen, die jedoch die gleiche passive Infrastruktur benutzen und an die gleichen übergeordneten Netzebenen angeschlossen sind. Es kann z. B. vorkommen, dass in einem LWL-Kabel ein Teil der Glasfasern für das Industrienetz und ein anderer Teil für das Büronetz verwendet wird. Auch ist beispielsweise denkbar, dass an ein und den selben Distribution-Switch ein Access-Switch der Industrie- und ein Access-Switch der Büroumgebung angeschlossen wird.

Variante 4: Das Industrie- und das Büronetz nutzen vollständig getrennte aktive und passive Infrastrukturen.

Bei getrennten Industrie- und Büronetzen ist in der Regel eine Kommunikation zwischen ihnen erforderlich. Die Kopplung zwischen den beiden Netzen ist auf folgenden Ebenen möglich:

Schicht-2-Kopplung (Bridging):
Eine Kopplung auf der Ebene der OSI-Schicht 2 ermöglicht die transparente Verbindung zwischen den beiden Netzen, ist jedoch mit dem Nachteil verbunden, dass Broadcasts aus dem Büronetz auf das Industrienetz übergreifen.

Schicht-3-Kopplung (Routing):
Eine Kopplung auf der Ebene der OSI-Schicht 3 ermöglicht die IP-Kommunikation zwischen allen Systemen der beiden Netze, ist jedoch mit dem Nachteil verbunden, dass von Büroendgeräten aus jedes IP-Paket an jedes Industrieendgerät gesendet werden kann (ping, TCP-Verbindungsaufbau, UDP-Datagramm). Unbeabsichtigte bzw. gezielte Manipulation ist somit möglich.

Schicht-3-Kopplung mit Access Lists:
Mithilfe von Access-Lists auf den Koppel-Routern zwischen den beiden Netzen kann bestimmt werden, welche IP-Adressen aus dem Büronetz mit welchen höheren Protokollen auf welche Systeme im Industrienetz zugreifen können.

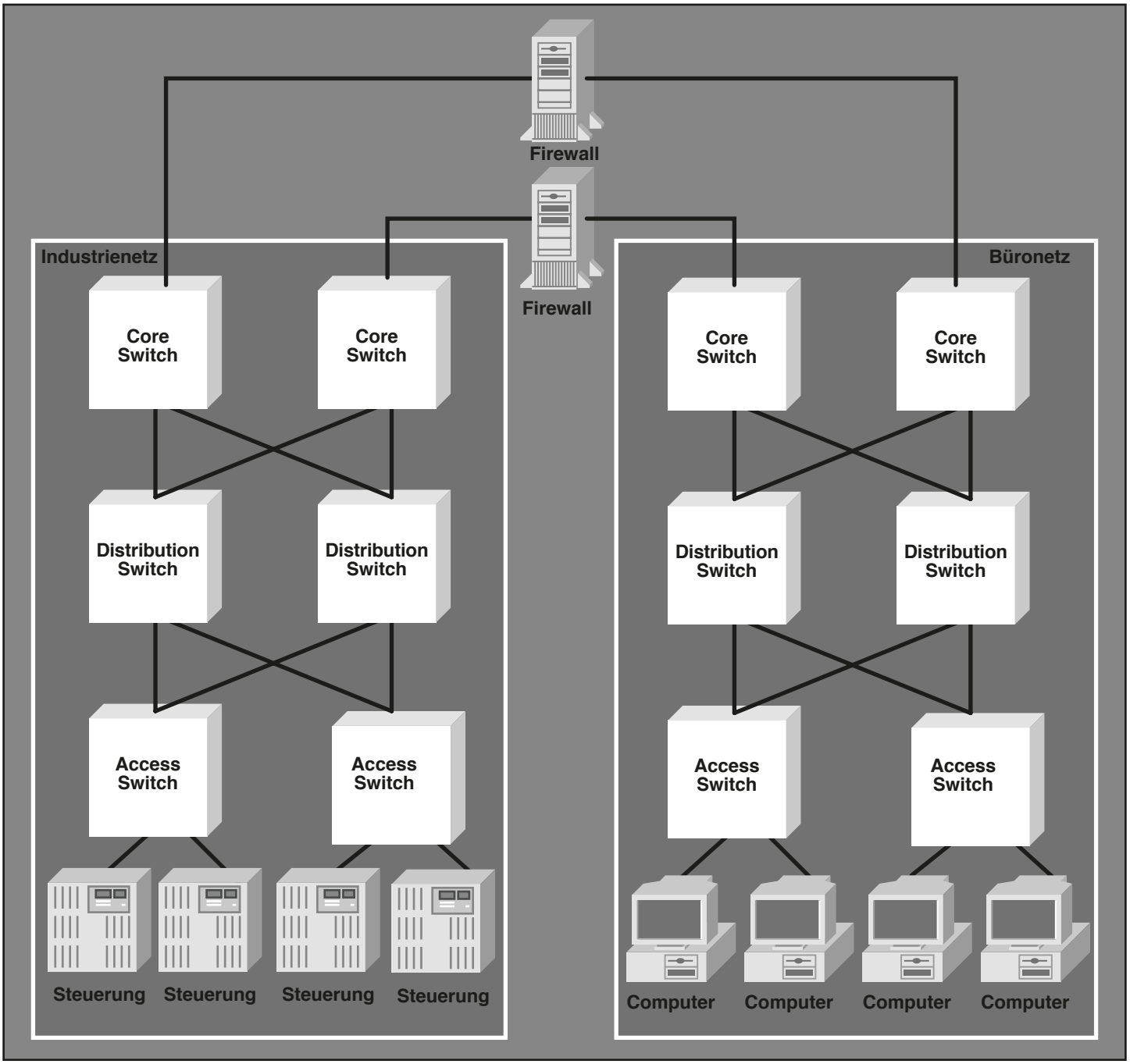


Bild 4: Industrienetz Variante 4

Damit wird zwar die Gefahr der Manipulation im Vergleich zur reinen Routing-Kopplung ohne Access Lists minimiert, aber die Zugriffsberechtigungen werden an veränderliche Parameter (IP-Adressen) geknüpft, und damit wird bei Änderungen von IP-Adressen ein hoher Administrationsaufwand verursacht. Zugleich kann ein berechtigter Benutzer nur von bestimmten Systemen aus die Verbindung nutzen, was die Flexibilität und die Mobilität der Benutzer einschränken kann.

Schicht-7-Kopplung (Application Level Gateway):
Mithilfe von Firewalls zwischen den beiden Netzen wird bestimmt, welcher Benutzer über welche Dienste (telnet, Web-Zugriff, FTP) auf das Industrienetz zugreifen kann. Proxy-Server auf dem Firewall-System gewähren auf der Basis von Passwörtern den Zugriff auf das Industrienetz. Zugleich unterstützen Firewalls auch Access-Lists auf der Basis von IP-Adressen für Datenströme, die von den Proxy-Servern nicht unterstützt werden.

Eine Kopplung auf der Ebene der Schicht 7 bietet den höchsten Schutz der Industrienetze vor Beeinträchtigungen aus dem Büronetz.

Die Entscheidung zu Gunsten eines dieser Modelle von den jeweiligen Rahmenbedingungen im Unternehmen, u. a. der Sicherheitspolitik für den Industrie- und Bürobereich, abhängig.

Deaktivierung der Default-Route

Die Rekonstruktion des Hergangs einiger Netzausfälle durch Wurm- und Virenangriffe zeigte, dass die Existenz einer Default-Route in LANs die Ausmaße des Ausfalls vergrößerte.

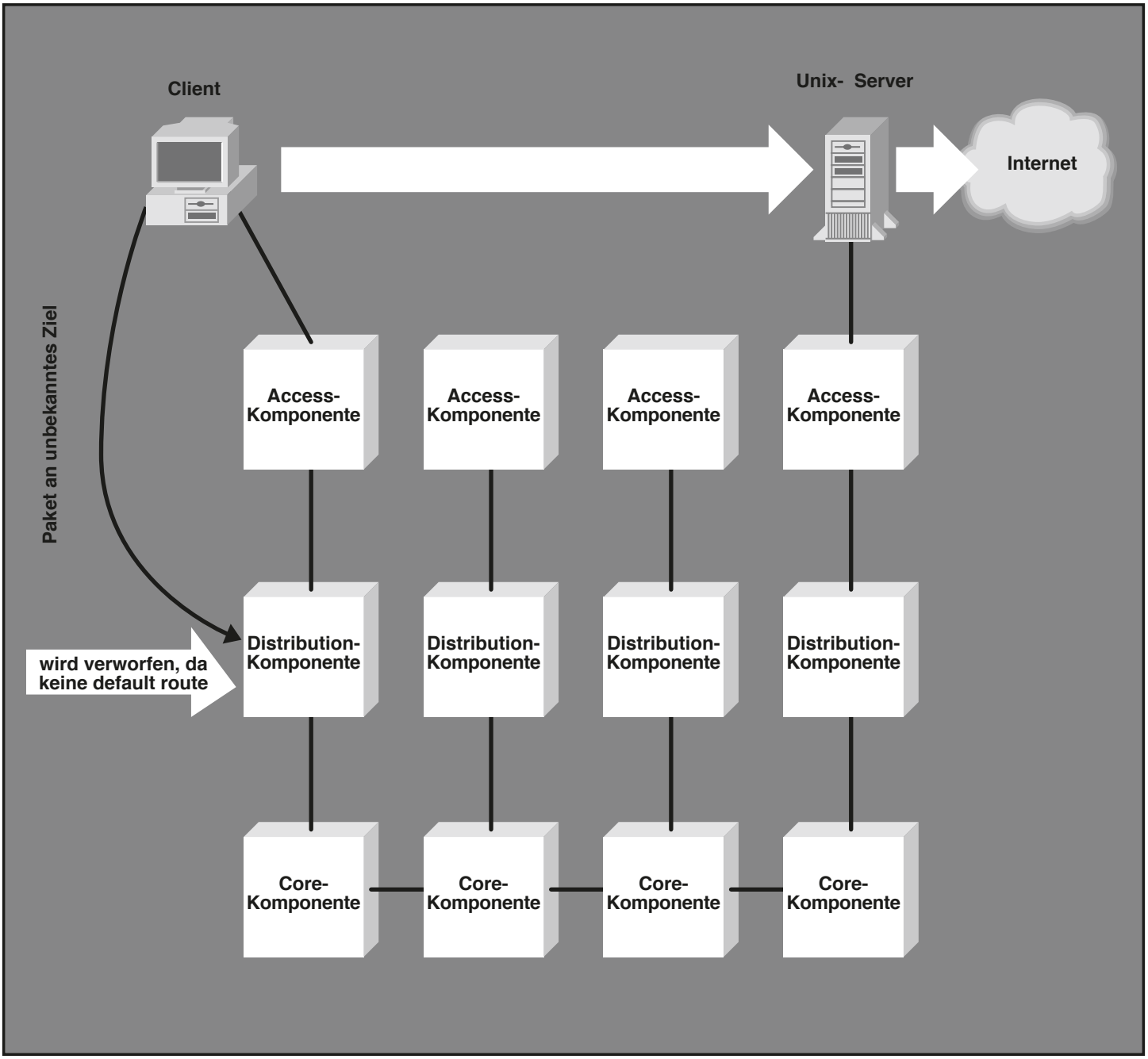
Die Default-Route wird bisher für solche Zugriffe von innen ins Internet benötigt, welche ohne Proxy-Funktion arbeiten, wie beispielsweise Einloggen auf Unix-Rechnern, File Transfer mit diesen von der Windows- oder Unix-Kommando-zeile aus etc.

Solche Anwendungen sind im Bereich von Industrial Ethernet in der Regel nicht notwendig. In den wenigen Ausnahmefällen kann beispielsweise ein interner Unix-Server mit einer Default-Route in Richtung Internet-Firewalls als Zwischenstation beim Zugriff auf beliebige Rechner im Internet dienen.

Analog ist bei den Web-Proxy-Servern sicherzustellen, dass deren Default-Route ebenfalls in Richtung Internet-Firewalls zeigt (s. Bild 5).

Bei Umsetzung dieser Maßnahmen ist eine Default-Route auf den Netzkomponenten nicht mehr erforderlich, und Pakete an unbekannte Ziele, die für schadensstiftende Software typisch sind, werden durch die erste Routing-Instanz, die solche Pakete erhält, verworfen.

Bild 5: Deaktivierung der Default-Route im Netz



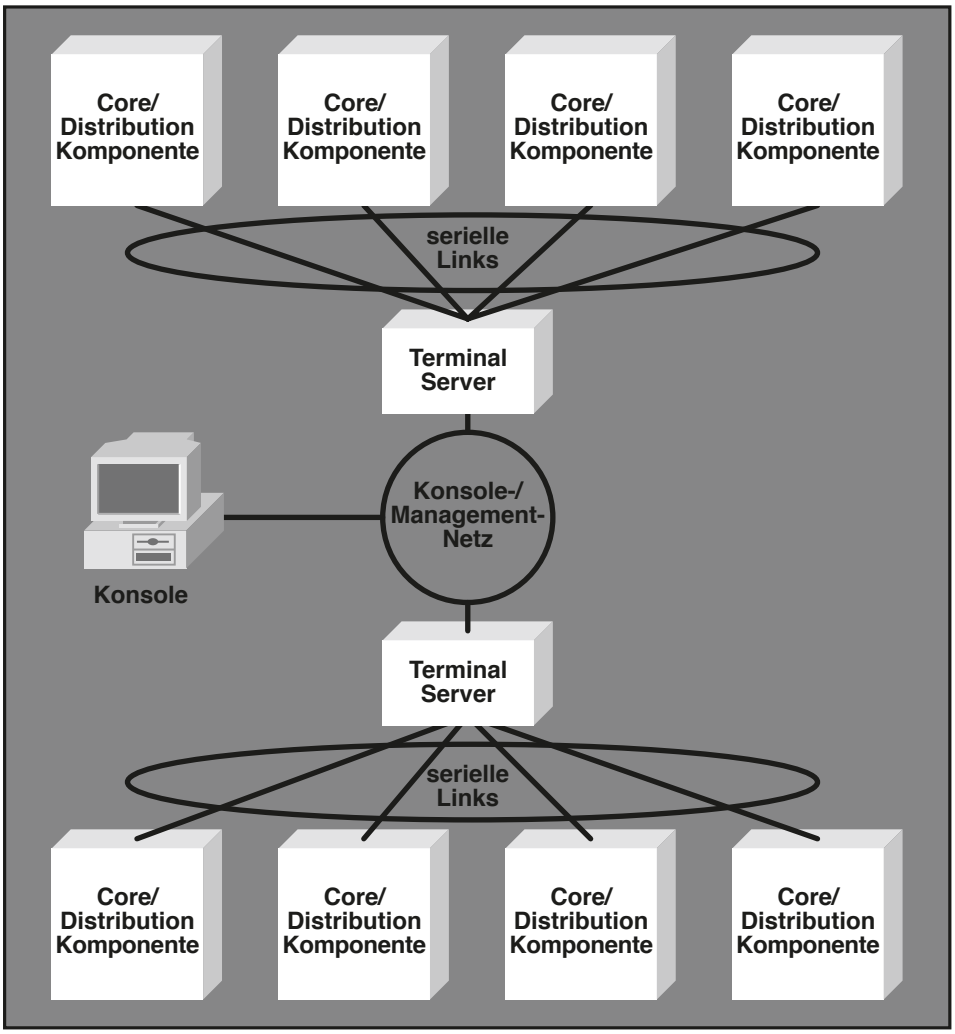


Bild 6 (oben): Konsolennetz

Outband-Management

Ein Outband-Management-Netz (Konsolennetz), das Zugriffe auf die Netzkomponenten unabhängig von der Verfügbarkeit des Hauptnetzes ermöglicht, ist auch für den Bereich Industrial Ethernet zu empfehlen und geht aus Bild 6 hervor.

Die Console-Ports aller Core- und Distribution-Komponenten werden über Terminalserver an ein vom Hauptnetz unabhängiges Netz angeschlossen.

Über dieses Netz und die Terminalserver kann man von der Konsole aus auf die Netzkomponenten zugreifen, auch wenn z. B. aufgrund eines Wurmangriffs das Hauptnetz gestört ist.

Dieser Zugriff kann die Fehlerbegrenzung beschleunigen.

Management-Netz

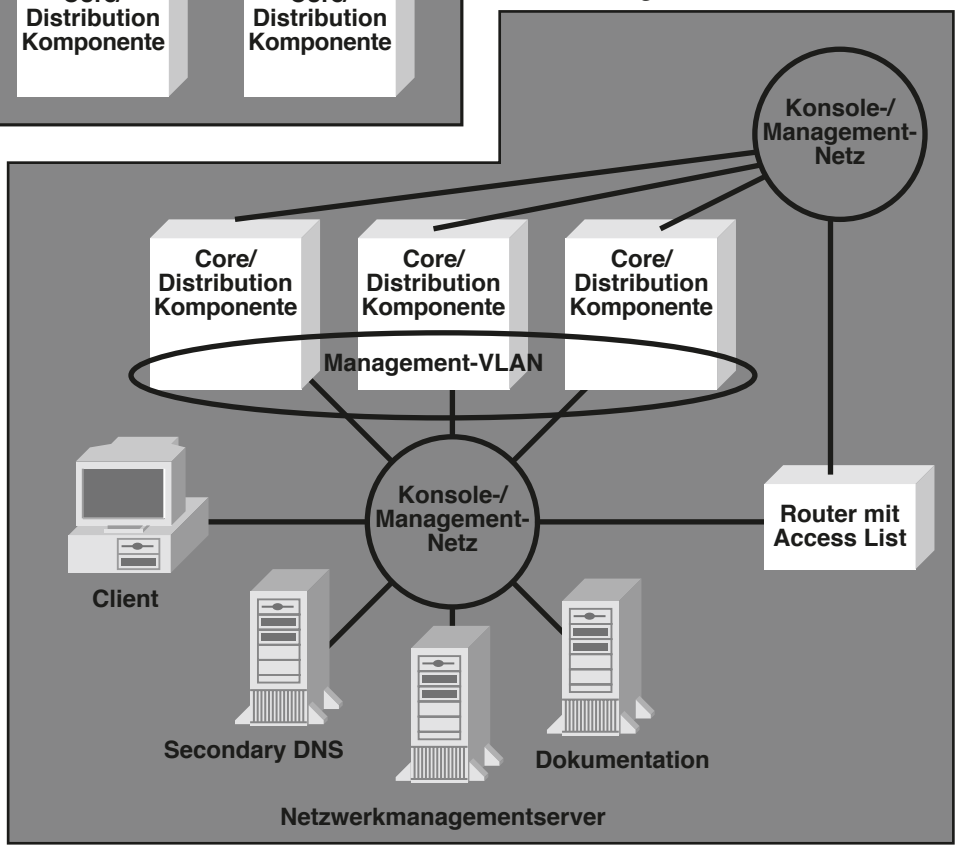
Das im letzten Abschnitt dargestellte Netz kann auch dem Anschluss von eigenen Management-Ports der Komponenten dienen, wie in Bild 7 dargestellt ist.

Dazu wird auf allen Core- und Distribution-Komponenten ein Management-VLAN definiert, und der Management-Port wird diesem VLAN zugeordnet. Sämtliche Überwachung der Systeme erfolgt über diesen Port und ist daher von Problemen im Hauptnetz (Wirknetz) nicht beeinträchtigt.

Das Management-VLAN wird als reines Layer-2-VLAN ohne IP-Interface auf den Core/Distribution-Komponenten eingerichtet. Das Dokumentationssystem, ein Secondary DNS Server und die Management-Server (Konsole, Element Manager) werden an das Management-Netz angeschlossen.

Daher braucht dieses Netz einen geschützten Übergang zum Hauptnetz. Über diesen Übergang werden nur die erforderlichen Kommunikationsströme per Access List auf dem Koppelelement (Routing-Instanz) zugelassen.

Bild 7: Management-Netz



Sicherheitsaspekte beim Einsatz von Industrial Ethernet

Fazit zur Sicherheit bei Einsatz von Industrial Ethernet

Die weltweite Verbreitung von Viren und sonstigem malicious code hat gezeigt, dass die Hosts im Allgemeinen gegen solche und andere Angriffe nicht ausreichend geschützt sind.

Die klassischen Kataloge von Schutzmechanismen in Netzen wie z. B. Router Access Lists, Firewalls, Intrusion Detection und Virenschutzmechanismen schützen nur bedingt vor solchen Angriffen.

Firewalls bieten z. B. Mechanismen, mit denen kontrollierte Kanäle geöffnet werden können. In der Regel besteht jedoch keine Möglichkeit, mithilfe von Firewalls die Prozeduren innerhalb dieser Kanäle zu überwachen bzw. zu steuern.

Insbesondere Denial-of-Service(DoS)-Angriffe sind in heutigen IP-Netzen kaum zu verhindern. Ethernet/IP-Netze sind hinsichtlich DoS mit einem wesentlich höheren Angriffspotenzial verbunden als konventionelle Feldbusse. Denial of Service bedeutet, dass der Angreifer die Beeinträchtigung der Funktionalität einer Anlage, Lösung oder Dienst zum Ziel hat.

Aufgrund der den Ethernet-Netzen innewohnenden Möglichkeit der Kommunikation „jeder mit jedem“ ist es sehr einfach, eine Ethernet-basierende Lösung lahmzulegen. Der Angreifer braucht lediglich einen Übertragungspfad (zum Beispiel IP-Pfad) zum Angriffsziel. Im Rahmen der einfachsten denkbare Variante von Denial of Service wird das Angriffsziel mit IP-Paketen „überflutet“. Über diesen sehr einfachen Angriff hinaus sind aber auch raffiniertere DoS-Angriffe denkbar, die kaum abzuwehren sind.

In den bisherigen Industrial-Ethernet-Produkten sind Sicherheitsmechanismen kaum standardmäßig implementiert. Somit kann eine mit den bisherigen konventionellen Feldbussystemen vergleichbare Sicherheit nach dem heutigen Stand nur durch die in diesem Kapitel zusammengefassten zusätzlichen Maßnahmen auf der System- und Netzebene erreicht werden.

Der Aufwand für diese Mechanismen muss beim Wirtschaftlichkeitsvergleich zwischen herkömmlichen Feldbussystemen und Industrial-Ethernet-Lösungen zusätzlich berücksichtigt und bewertet werden.

Dipl.-Inform. Dietlind Hübner ist seit mehr als 10 Jahren bei der ComConsult Beratung und Planung GmbH als Senior Consultant tätig. Neben ihren Spezialgebieten höhere Protokolle und Netzwerk-Anwendungen wirkt sie auf Basis ihres technischen Know How und Erfahrung regelmäßig in Projekten der Netzkonzeption in Büro- und Industrieumgebungen mit.

Dr. Behrooz Moayeri ist Mitglied der Geschäftsleitung der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrungen zurück. In den letzten Jahren hat er zahlreiche führende deutsche Unternehmen bei der Konzipierung und Planung von IT- und Kommunikations-Lösungen erfolgreich beraten.

Dipl.-Ing. Hartmut Kell kann bis heute auf eine mehr als 10-jährige Berufserfahrung in Datenkommunikation in lokalen Netzen verweisen. Als langjähriger Mitarbeiter der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt.

Dipl.-Ing. Thomas Simon, ComConsult Beratung und Planung GmbH, Vorsitzender des Arbeitskreises Industrie-Infrastrukturen der Benutzergruppe Netzwerke, einer der führenden deutschen Experten zum Thema Industriekommunikation.

Dieser Artikel ist eine verkürzte Version des entsprechenden Kapitels aus dem Report zum Industrial Ethernet. Der vollständige Report kann auf Anfrage an report@comconsult-research.com bezogen werden.

Neues Seminar

Smart Cards erfolgreich und effizient einsetzen

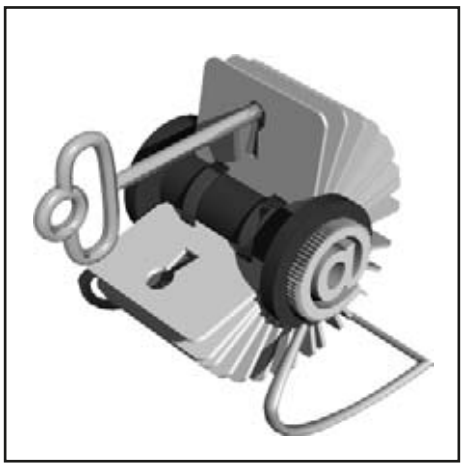
Vom 9. bis 10. März 2004 veranstaltet die ComConsult Akademie im Holiday Inn in Köln zum ersten Mal ihr neues Seminar "Smart Cards erfolgreich und effizient einsetzen".

Viele der heute verfügbaren Authentifizierungs- und Verschlüsselungsverfahren erhalten erst durch den Einsatz von Smart Cards ihr volles Leistungspotenzial. Smart Cards verkörpern in idealer Weise die Sicherheit von Kommunikation und Daten im Rahmen eines effizienten und wirtschaftlichen Betriebs. Der besondere Vorteil dieser Technologie liegt in der breiten, aber einheitlichen Nutzbarkeit. Vom sicheren User-Login, über die Netzwerksicherheit bis zur Mailverschlüsselung und zur Signatur kann eine weitgehende Sicherheit durch die Zwei-Faktor-Authentifizierung erreicht werden.

Sie lernen in diesem Seminar, welche vielfältigen und überzeugenden Einsatzmöglichkeiten es für Smart Cards in Ihrem Unternehmen gibt und wie sie diese betriebs-technisch umsetzen.

Die Referenten

Dipl.-Inform. Michael van Laak ist bei der ComConsult Beratung und Planung GmbH als Berater im Kompetenz Center Backoffice tätig. Zu seinen Spezialgebieten zählt das Design von Verzeichnisdiensten, die Migrationskonzipierung und Durchführung, sowie die Erstellung und Implementierung von (Fern-) Administrationskonzepten.



Dipl.-Ing. Hans Peter Mohn ist lizenzierter IT-Grundschutz-Auditor des BSI. Seine Aufgabenbereiche bei der ComConsult Beratung und Planung GmbH sind die Durchführung von Sicherheitsüberprüfungen, die Erstellung und Umsetzung von Sicherheitskonzepten sowie die Organisation des Betriebs von IT-Sicherheitsmaßnahmen.

Alexander Zarenko berät als Fachinformatiker/Systemintegration im Competence Center Backoffice in der Konzeption und Umsetzung von Migrationsprojekten auf Windows-Server. Schwerpunkte bilden hierbei die Themen Sicherheit, PKI, Policies & Profiles sowie Remote Access/VPN mit Windows 2000.

Im Einzelnen lernen Sie:

- welche Einsatzgebiete es für Smart Cards gibt
- welchen Grad an Sicherheit Sie damit auch gegenüber biometrischen Verfahren erreichen
- welche hohen betriebstechnischen Vorteile bestehen
- wie Smart Cards erfolgreich in Zertifizierungs-Infrastrukturen und eine PKI integriert werden
- welche besonderen Vorteile Smart Cards im Netzwerk bieten, wie ihre Nutzung technisch und organisatorisch umgesetzt wird
- welche Details dabei bei der Auswahl der PKI-Form und der Kombination mit anderen Verfahren wie 802.1x zu beachten sind
- wie optimale Integration in eine Windows 2000 und 2003-Server-Umgebung aussieht, warum dabei 2003 erhebliche Vorteile bietet
- wie erfolgreiche Lösungs-Szenarien innerhalb von Windows 2000 / 2003 aussehen
  – Authentifizierung im LAN/WAN
  – Einsatz im VPN
  – E-Mail Verschlüsselung und Signatur
  – Datei-Verschlüsselung
- Welche Wechselwirkungen und Einschränkungen zum Beispiel mit Citrix unbedingt zu beachten sind

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Smart Cards

Ich buche das Seminar
Smart Cards erfolgreich und effizient einsetzen
vom 09.03. - 10.03.04 in Köln

(Preis € 1.390,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

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

Studie des Monats

IP-Telefonie
Cisco versus Siemens

Aus dem neuen ComConsult Research Report "IP-Telefonie: Cisco versus Siemens"*

Die Siemens Produktwelt für Telefonie
Die HiPath-Produktlinien
HiPath 4000

Die HiPath 4000 stellt zurzeit das Flaggschiff der modularen IP-fähigen Anlagen dar und ist für mittlere bis große Unternehmen gedacht. Sie umfasst die bisherige Funktionalität der Hicom-300-E/H-Systeme. Da die HiPath 4000 intern immer noch als TDM-Anlage arbeitet, werden IP-Geräte und IP-Trunks durch eine Gatewayfunktion angeschaltet. Dies ist das 10/100-Mbit-Ethernet-Netzinterface mit integriertem Gateway (HG = HiPath Gateway). Es gibt drei Gateway-Baugruppen:

- HiPath HG 3530 für den vollfunktionalen Zugriff von IP-Clients (Telefonen),
- HiPath HG 3550 für IP-Trunkverbindungen zu anderen HiPath-4000-Systemen (CorNet-NQ) oder mit dem externen Gateway HG2500 zu Hicom-300H-Systemen,
- HiPath HG 3570 für die Anschaltung von Access Points über IP.

In der weiteren Beschreibung wird jeweils darauf verwiesen, wo welches Gateway eingesetzt wird.

Es gibt zwei HiPath-4000-Modelle: (siehe Bild 1)

- HiPath 4300 mit bis zu drei direkt angebundenen Shelfs (Access Points 3300) und bis zu 40 über das IP-Netzwerk angeschalteten Access Points sowie einer Leistungsklasse für bis zu 2.000 digitale Teilnehmer,
- HiPath 4500 mit bis zu 15 direkt angebundenen Access Points und bis zu 83 über das IP-Netzwerk angeschalteten Access Points sowie einer Leistungsklasse für bis zu 12.000 digitale Teilnehmer, optional redundant auslegbarem Controller Modul und redundanten PSUs. Die Maximalzahl von 98 Shelfs oder Access Points resultiert aus einer limitierten Adressierbarkeit.

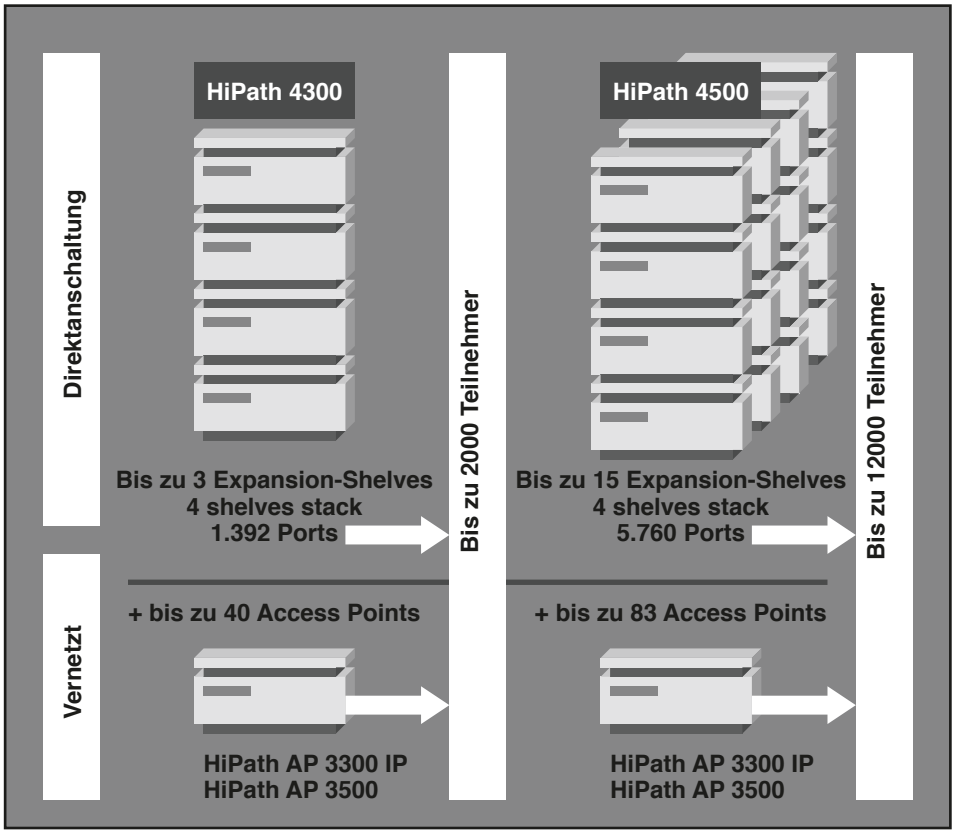


Bild 1: Modularer Aufbau der HiPath 4300 und 4500 (Quelle: Siemens)

Unterstützung von IP-Clients

Soll eine HiPath 4000 IP-Clients (in der Siemens Terminologie: IP-Workpoints) mit dem CorNet-Funktionsumfang integrieren, so muss das Gateway HiPath HG 3530 eingebaut werden, das für IP-Clients den HiPath-4000-Feature-Zugriff (HFA, HiPath 4000 Feature Access) ermöglicht. Eine HG-3530-Baugruppe unterstützt 30 parallele Kanäle d.h. 30 parallele Gespräche. Da die IP-Telefone nicht dynamisch zugeordnet werden können, sondern fix zugeordnet werden müssen, gilt in der Version 1.0 eine Beschränkung auf maximal 30 IP-Telefone je HG-3530-Baugruppe. Die feste Zuordnung bei Version 1.0 verhindert auch, dass bei Ausfall eines HG 3530 eine andere Baugruppe die Gespräche der hier konfigurierten Teilnehmer übernimmt. Insgesamt können bei der aktuellen Stromversorgung maximal 10 Baugruppen HG 3530 in ein HiPath-4000-Shelf eingebaut werden. Sollen zusätzlich HG-3570-Gateways eingebaut werden, reduziert sich die Zahl entsprechend (max. acht Baugruppen HG 3530 / HG 3550 / HG3570). Da die HG-3530-Baugruppe keine blockierungsfreie Durchschaltung auf das Koppelfeld (TDM-Matrix) benötigt, können zusätzlich zu acht Baugruppen HG 3530 auch noch klassische Baugruppen eingebaut werden, so dass die 128 Kanäle je Halb-Shelf überbucht genutzt werden können.

* IP-Telefonie: Cisco versus Siemens Report, ComConsult Research Technologie Report, zu beziehen über den Verlag ComConsult Technologie Information (weitere Informationen unter www.comconsult-research.com)

Im Maximalausbau können somit 15 Shelfs direkt und 83 Access Points 3300 über IP an eine HiPath 4500 angeschaltet werden. Direkt angeschaltet werden damit maximal 15 x 10 x 30 = 4500 IP-Clients (Hardphones, Softphones) unterstützt. Dies ist, besonders im Vergleich zu den ca. 12.000 über eine HiPath 4000 betreibbaren TDM-Geräten, eine deutlich limitierte Ausbaubarkeit der Anlage für IP-Telefonie. Offiziell sind bis zu 30 HiPath-4000-Systeme in einer Domäne vernetzbar. (Durch Bildung von bis zu 10 Sub-Domänen ließe sich die Anzahl der HiPath-4000-Systeme in einem Netz bis auf 300 erweitern. Hierfür dürfte es jedoch schwierig sein, Referenzinstallationen zu finden.) Somit ergibt sich eine maximale Anzahl von ca. 80.000 direkt konfigurierbaren IP-Telefonen, da sich ja über den Einbau der Trunking-Gateways die maximal einbaubare Anzahl von HG-3530-Workpoint-Gateways reduziert: Kalkuliert man zwei HG 3550 je Shelf und sechs HG 3530 je Shelf, so ergeben sich 15 x 6 x 30 = 2700 IP-Clients je HiPath 4000, bei 30 HiPath 4000 eine maximale Anzahl von 81.000 IP-Clients. In diesem Fall könnten jedoch keine Access Points mehr angebunden werden.

In Version 1.0 unterstützt eine HiPath 4500 maximal bis zu 4.500 IP-Telefone mit Direktzugriff. Im Anlagenverbund werden ca. 80.000 IP-Telefone mit Direktzugriff unterstützt. In Version 1.0 läuft jede IP-Session komplett über die HG-3530-Baugruppe in der HiPath 4000.

Ab Version 2.0 können IP-Telefone direkt miteinander kommunizieren, so dass nur die Signalisierung über die Anlage läuft, nicht aber der Datenanteil der Session. Diese Peer-to-Peer-"Direktverbindung" wird als Payload Switching bezeichnet.

Es wird erwartet, dass in 2004 mit Version 2.0 die Anzahl der je Gateway-Baugruppe unterstützten IP-Clients auf 240 verwaltbare und 120 parallel aktive IP-Verbindungen erhöht wird. Damit wäre immerhin die Unterstützung von 1350 aktiven und 2700 verwalteten IP-Clients je HiPath 4000 möglich.

Access Points: Verteilte Architektur für klassische TK-Geräte

Mit dem Konzept der Access Points wurde die HiPath-Anlage mit einer flexibleren dezentralen Architektur erweitert, da Access Points über ein IP-Netzwerk mit der HiPath 4000 verbunden werden können und nicht mehr sternförmig direkt angeschaltet sein müssen. Anstelle des früheren sternförmigen Konzepts mit Direktanschaltung sind nun Lösungen denkbar, bei denen an einen Ethernet-Switchport im Etagenverteiler ein Access Point angeschaltet wird, der seinerseits non-IP-TK-Geräte und unter strenger technischer Beachtung der Delay-Restriktionen (d.h. die Einhaltung der Delaygrenzen muss in der Regel projektspezifisch von Siemens oder einem zertifizierten Partner nachgeprüft werden) auch IP-Clients bedient.

Die Nutzung von Access Points macht nur dann richtig Sinn, wenn insbesondere non-IP-Geräte zu integrieren sind, die Anbindung über WAN erfolgt oder viele lokale Peer-to-Peer-Gespräche stattfinden. Ansonsten können die IP-Clients zukünftig besser über 3530-Baugruppen in die HiPath 4000 integriert werden.

IP-fähige Access Points sind der HiPath AP 3300 (entspricht einem HiPath 4000 Shelf) mit 16 Modulslots oder der HiPath AP 3500 mit 3+4 Modulslots (AP 3500 + AP 3505 Erweiterungseinheit). Beide Access Points haben als IP-Gateway ein HiPath HG 3575 eingebaut, das Gateway-Gegenstück in der HiPath 4000 ist das HiPath HG 3570. Hier gilt dieselbe Beschränkung wie für das HG 3530, es können bei der aktuellen Stromversorgung maximal acht HG 3570 in ein Shelf eingebaut werden. Sind schon HG 3530 oder HG 3550 eingebaut, reduziert sich die Zahl entsprechend (in Summe maximal acht Baugruppen HG 3530 / HG 3550 / HG 3570). Zusätzlich benötigen die HG 3570 und HG 3575 eine blockierungsfreie Durchschaltung auf die Koppelmatrix. Da je Halb-Shelf maximal 128 Kanäle blockierungsfrei auf der TDM-Matrix arbeiten können, müssen die acht Baugruppen dann zu jeweils maximal vier Baugruppen auf zwei Halb-Shelfs verteilt werden (linke und rechte Seite vom Steuermodul). Wird die maximale Zahl von Baugruppen ausgenutzt, können keine weiteren klassischen Baugruppen mehr genutzt werden, da dies die Restriktion von maximal 128 Kanälen pro Halb-Shelf überschreiten würde.

Alle HG 3570 Baugruppen in den HiPath 4000 Shelfs müssen eine Layer-2-Verbindung untereinander haben, d.h. im selben IP-Subnetz angebunden sein!

Sowohl HG 3575 als auch HG 3570 unterstützen maximal 30 parallele Kanäle, d.h. Endgeräte im IP-Netzwerk, die sowohl gleichzeitig als auch systemübergreifend kommunizieren. Hier ist die Zuordnung allerdings nicht statisch sondern dynamisch, d.h. alle HG 3570 in einer HiPath arbeiten als Pool. Es müssen daher nur so viele Baugruppen installiert werden, wie parallele Gespräche zu erwarten sind. Fällt eine Baugruppe aus, so übernehmen die anderen Baugruppen die hierüber vermittelten Gespräche. Eine Beispielrechnung für maximal unterstützte und aktive IP-Clients je HiPath 4000 ist in gezeigt. Wir weisen hier bewusst auf die maximale Anzahl konfigurierbarer Clients hin, sowie die maximale Anzahl von Clients, die gleichzeitig und systemübergreifend telefonieren können. Die Übersicht macht deutlich, dass der Unterschied zwischen diesen beiden Werten sehr erheblich ist. Die Berechnung in der rechten Spalte betrifft Gespräche von Access Points zur HiPath 4000; Gespräche zwischen den Access Points bzw. den über sie angekoppelten Geräten werden im IP-Netz vermittelt. Hier gilt jeweils die Beschränkung parallel möglicher Kanäle zwischen zwei Access Points (entsprechend der jeweils eingebauten HG-3575-Baugruppen).

Für Gespräche zwischen Endgeräten, die demselben Access Point zugeordnet sind (digital, analog und IP), hat das HG 3575 eine lokale TDM-Switchmatrix von 256 Kanälen, die intern blockierungsfrei bedient werden können.

Tabelle 1: Beispielrechnung für konfigurierte und aktive IP-Clients einer HiPath 4000 mit angeschalteten Access Points 3300

Komponente	IP Clients direkt an HiPath 4500	konfigurierbare IP Clients über AP 3300	parallel aktive IP Clients
Shelves / AP 3300	15	75	75
HG 3570 /3575 je Shelf / AP 3300	5	1	1
HG 3530 je Shelf / AP 3300	3	7	1
Kanäle je 3530	30	30	30
direkte IP Clients	1350		
IP Clients über AP 3300		15750	2250
Gesamt		17100	3600

Die Nutzung von Access Points 3300 / 3500 für IP-Telefone ist wegen enger Delay-Restriktionen des HG 3575 in den Access Points nicht allgemein freigegeben; sie unterliegt einer projektspezifischen Freigabe nach technischer Prüfung durch Siemens oder einen zertifizierten Partner.

Geht man von einem Konzept aus, das keine direkt angebundenen IP-Clients sondern ausschließlich Access Points einsetzt und darüber hinaus die drei noch verfügbaren Slots für IP-Trunking benutzt, so können wiederum hierüber 30 HiPath 4000 vernetzt werden. Die maximale Anzahl von IP-Clients im Anlagenverbund wäre dann 30 x 17.000 = 510.000 IP-Clients.

Technische Bewertung

Bewertungskriterien

Bei den technischen Bewertungen wurden die folgenden Bereiche berücksichtigt:

- Architektur als Kernstück der Voice-Lösung
- Leistungsmerkmale als herausragender und derzeit größter Funktionsbereich
- weiterführende Funktionsbereiche
  - Standardunterstützung
  - Konvergenz
  - Mobilität
  - Zusatzapplikationen
  - Benutzerschnittstelle, Bedienbarkeit
  - Betrieb und Management
  - Entwicklungsschnittstellen
- Migration vorhandener Anlagen und Telefone
- Zusatzapplikationen

Da die Gewichtung dieser Bereiche je nach Ausgangslage eines Unternehmens und Motivation für den Einsatz von IP-Telefonie zu unterschiedlich ist, wurde auf eine übergreifende Gesamtbewertung aller Bereiche verzichtet und stattdessen für jeden Bereich eine separate Bereichsbewertung erstellt. Eine individuelle Gesamtwertung kann sich jeder Leser mit Hilfe der beigefügten Tabellen erstellen. Jeder Bereich sollte hierzu den betrieblichen Bedingungen entsprechend gewichtet werden, die resultierende Gesamtbewertung ergibt sich dann aus den gewichteten Bereichsbewertungen. Die Tabellen mit vorgefertigten Berechnungsschemata befinden sich als Excel-Dateien auf der beiliegenden CD.

Architektur

Die Architektur ist absolut entscheidend für die Skalierbarkeit, Verfügbarkeit, Stabilität, Einheitlichkeit, Flexibilität, Funktionsbreite und Zukunftssicherheit einer Voice-over-IP-Lösung. Daher wurde die Architektur in einem eigenen Funktionsbereich bewertet. Diese Bewertung wurde in folgende Kriterien aufgeteilt:

- Skalierbarkeit
- Verfügbarkeit / Redundanz
- Stabilität
- Quality of Service (QoS)
- Flexibilität
- Einheitlichkeit
- Endgeräte-Abdeckung
- Stromversorgung

Skalierbarkeit

Cisco

Eine Lösung mit dem CallManager auf Basis Windows 2000 ist nach unten wenig skalierbar, d.h. bei Einsatz von nur 20 bis 50 Endgeräten entsteht ein relativ hoher Kostenanteil für den CallManager als zentralen Server, insbesondere wenn dieser aus Verfügbarkeitsgründen redundant ausgelegt werden muss. Für solche kleinen Lösungen können seit Q4/2003 auch Router mit der Software "CallManager Express" bestückt werden (Cisco ITS, 24 bis 120 Teilnehmeranschlüsse). Wegen der etwas reduzierten Funktionalität des CallManager Express wird die Skalierbarkeit nach unten "nur" als gut bewertet.

Ein einzelner CallManager kann theoretisch bis zu 7.500 Endgeräte bedienen, ein Cluster unterstützt maximal 30.000 Endgeräte. In diesem Fall sind jedoch keinerlei Backup-Definitionen mehr möglich und diese Werte beziehen sich auf die reinen Telefonie-Funktionen. Wenn weitere Funktionen und Applikationen zusätzlich eingesetzt werden (z.B. CTI, Konferenz, Music on Hold, XML etc.), reduziert sich die maximale Anzahl teilweise erheblich. Ein einzelner CallManager hat dann mit praktisch einsetzbaren 1.500 bis 2.000 Geräten eine gute Skalierbarkeit.

Ein CallManager Cluster kann mit praktisch 12.000 bis 16.000 Geräten ebenfalls als gut skalierbar bezeichnet werden.

Die genaue Berechnung, wie viele Endgeräte ein CallManager bzw. ein Cluster unterstützt, wird mit so genannten Device Weights berechnet. Das Konzept von Device Weights in zusätzlicher Kombination mit so genannten BHCA-Multiplikatoren führt zu so komplexen Berechnungen, dass nach unserer Einschätzung vom Anwender und Fachplaner nur noch ein automatisches Konfigurationstool eingesetzt werden kann. Für den CallManager v3.3.3 existiert ein solches Tool als Beta-Version. Es wird erwartet, dass dies für die nachfolgenden Versionen allgemein unterstützt werden wird und mittelfristig eine einfachere Kapazitätsberechnung implementiert.

Die maximale Skalierbarkeit über Intercluster Trunking funktioniert nur im Funktionsumfang von H.323 und kann daher nur als mittelmäßig bewertet werden.

Siemens

Mit den HiPath 3000 und 5000 ist die Skalierbarkeit nach unten gegeben, jedoch liegt dann nicht derselbe Funktionsumfang wie bei HiPath 4000 vor, da die beiden Systeme HiPath 3000 und HiPath 4000 laut Siemens für unterschiedliche Märkte gedacht sind. Die Skalierbarkeit nach unten wird daher insgesamt als gut bewertet.

Eine HiPath 4000 könnte mit bis zu 4.500 Geräten eine gute Skalierbarkeit erreichen. Allerdings stellt der Einbau vieler Gateway-Baugruppen hier einen erheblichen Kostenfaktor dar, und für die Anschaltung an das IP-Netzwerk werden viele bis sehr viele Switchports benötigt, die in die Kostenrechnung einzubeziehen sind (siehe hierzu das Kapitel "Kostenbewertung"). Die Zuordnung der Benutzer zu HG-3530-Baugruppen ist statisch und kann nicht im Pool erfolgen, was die Skalierbarkeit wiederum einschränkt. Daher wurde die Bewertung insgesamt als mittelmäßig eingestuft.

Eine HiPath 4000 im Verbund mit Access Points als Cluster-Äquivalent erreicht praktisch 17.000 Geräte. Die Access Points sind jedoch alle als Single-Point-of-Failure zu betrachten und beim Einbau von HG-3530-Baugruppen ist projektspezifisch die Einhaltung der geforderten Delaywerte zu prüfen. Ebenso ist eine komplizierte Berechnung der einzubauenden Gateway-Baugruppen für Trunking und direkten Clientzugriff erforderlich. Daher wird die Cluster-Skalierbarkeit nur als mittelmäßig bewertet.

Die maximale Skalierbarkeit über bis zu 30 HiPath 4000 mit IP-Trunking führt zu einer komplizierten Berechnung einzubauender Gateway-Baugruppen für Access Points und IP-Trunking.

HiPath 4000 und HiPath 3000 Anlagen sind nur mit eingeschränktem Funktionsumfang im Verbund zu betreiben. Daher wurde die maximale Skalierbarkeit insgesamt als mittelmäßig bewertet.

Mit der Version 2.0 soll für HiPath 4000 eine Erhöhung der Anzahl der IP-Clients auf 120 aktive und 240 angemeldete Workpoints erfolgen, was die Skalierbarkeit um den Faktor 4 bis 8 verbessern wird.

Mit der zukünftigen Version 5.0 der HiPath 3000 können HiPath-3000-Systeme ohne Einschränkung der Anzahl in einem HiPath-4000-Netz betrieben werden, so dass hier eine Verbesserung zu erwarten ist. Jedoch gilt auch hier ein eingeschränkter Funktionsumfang, erst im "September Release 2004" V5.x soll der volle Funktionsumfang der HiPath 3000 (nicht HiPath 4000) in der Vernetzung möglich werden.

Tabelle 2: Bewertungsübersicht der Architektur

Technische Bewertung: Architektur						
Funktionalität	**Max.**	**Gew.**	**Cisco**		**Siemens**	
			Wert	**Gew.**	**Wert**	**Gew.**
Skalierbarkeit nach unten	8	2	3	6	3	6
Skalierbarkeit Einzellösung	8	2	3	6	2	4
Skalierbarkeit Cluster / vernetzte Lösung	8	2	3	6	2	4
Skalierbarkeit maximaler Anlagenverbund	4	1	2	2	2	2
Verfügbarkeit / Redundanz TK-Server	12	3	4	12	2	6
Verfügbarkeit / Redundanz Gateways	12	3	4	12	4	12
Stabilität	12	3	3	9	4	12
Quality of Service (QoS)	4	1	3	3	2	2
Flexibilität	12	3	4	12	2	6
Einheitlichkeit	12	3	3	9	2	6
IP Endgeräte(-Abdeckung)	8	2	4	8	1	1
non-IP Endgeräte(-Abdeckung)*	4	1	1	1	3	3
Stromversorgung	8	2	2	4	2	4
Summe	112		39	90	31	68
Prozentzahl	100 %			80 %		61 %
0 = gar nicht, 1 = niedrig, 2 = mittel, 3 = gut, 4 = sehr gut						
*** wurde hier nur mit "1" gewichtet, da non-IP Geräte unter dem Punkt "Migrationsfähigkeit" mit hoher Gewichtung eingebracht wurden**						

Abkürzungen

AP	Access Point
BHCA	Busy Hour Call Attempts
CTI	Computer Telefonie Integration
HG	HiPath Gateway
IOS	Internetworking Operating System (Cisco)
IP	Internet Protocol
ITS	IOS Telephony Services (Cisco)
PSU	Power Supply Unit
QoS	Quality of Service
TDM	Time Division Multiplexing
TK	Telekommunikation
WAN	Wide Area Network
XML	Extensible Markup Language

Aktueller Report

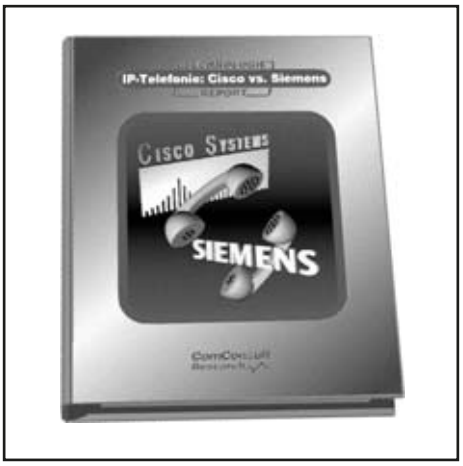
Studie des Monats: IP-Telefonie – Cisco versus Siemens

Ergebnisse einer Technologie Studie von Dipl.-Inform. Petra Borowka

Die neue Technologie Studie von ComConsult Research "IP-Telefonie – Cisco versus Siemens" analysiert die bestehenden und in der Zukunft zu erwartenden TK-Lösungen von Cisco und Siemens und stellt die spannende Frage, wer die bessere TK-Lösung hat. Auch die erkennbare Weiterentwicklung der nächsten Jahre wird dabei berücksichtigt. Der Report bewertet nicht nur rein technische Elemente sondern gibt auch Einschätzungen zur Zukunftssicherheit der Produkte ab.

Selten hat der Wettbewerb zwischen zwei Herstellern so viel Aufregung und Diskussionen erzeugt wie der Kampf zwischen Cisco und Siemens um den deutschen TK-Markt. Dabei könnten die beiden Kontrahenten kaum unterschiedlicher sein. Ergebnisse einer Technologie-Studie, wer hat die bessere TK-Lösung.

Auf der einen Seite der Repräsentant der Datenwelt Cisco und auf der anderen Seite das TK-Urgestein Siemens. Und tatsächlich sind die Produktansätze dieser beiden Firmen zur IP-Telefonie genauso unterschiedlich wie ihre Ausgangslage. Cisco konnte mit dem Call-Manager ohne Rücksicht auf „Altlasten“ eine moderne IP-Anlagen-Architektur entwickeln, die allerdings genau die Frage der Integration mit einer bestehenden TK-Welt technisch und wirtschaftlich nach sich zieht. Umgekehrt



Wer hat die bessere TK-Lösung?

hat der Siemens-Ansatz schon auf den ersten Blick den Vorteil der Integration der bisherigen Welt, aber genau mit dem Fragezeichen zur Tragfähigkeit der Architektur in einer IP-Zukunft. Entsprechend schwierig ist die Bewertung der Funktionalität aber auch der strategischen Bedeutung der einzelnen Siemens-Produktlinien.

Hier setzt der neueste und bisher kontroverseste Report von ComConsult-Research an. Auf über 280 Seiten und einem ausführlichen Anhang werden ausgehend von der Erklärung der technischen Rahmenbedingungen einer Lösung für IP-Telefonie sowie der Systemarchitekturen von Cisco und Siemens ein Kriterienkatalog entwickelt, auf dessen Basis die Produkte und Konzepte der beiden Hersteller miteinander verglichen werden.

Der Cisco-Siemens-Vergleich umfasst unter anderem die Bereiche:

- die Architektur der Lösung
- die Skalierbarkeit und Flexibilität
- die Verfügbarkeits-Gestaltung
- die Stabilität
- die Endgeräte-Technologie
- Leistungsmerkmale und Einzelfunktionen
- Benutzerschnittstelle und Bedienbarkeit
- Betrieb und Management
- Migration vorhandener Anlagen
- Zusatzapplikationen

Eine derartige Gegenüberstellung der IP-Telefonie-Produkte dieser beiden Hersteller hat es bisher nicht gegeben, sie ist einzigartig und kontrovers.

Diese neue Studie von ComConsult Research ist ein elementares Hilfsmittel für jede Evaluierung des IP-Telefonie-Marktes, sie darf auf keinem Schreibtisch in diesem Bereich fehlen.

Die Kriterien-Kataloge sind zudem so aufgebaut, dass sie auf andere Hersteller übertragen werden können.

Fax-Antwort an ComConsult 02408/955-399

Bestellung Cisco versus Siemens

☐ Ich bestelle den Research Report
IP-Telefonie: Cisco versus Siemens
(Preis € 398,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

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

Schwerpunktthema

Voice-over-IP Management

Fortsetzung von Seite 1

Dipl.-Inform. Petra Borowka hat langjährige Praxis-erfahrung mit mehr als 15 Jahren herstellerneutraler Netzwerkplanung in Projekten für verschiedenste Industrie- und Dienstleistungsunternehmen; bekannt durch viele Schulungen und Veröffentlichungen. Sie leitet das Planungsbüro Unternehmensberatung Netzwerke UBN in Aachen.

Zielsetzungen für Betrieb und Management von Voice-Lösungen in IP Netzwerken

Da Telefonie zu den unternehmenskritischen Anwendungen gehört, führt ihr Einsatz zu entsprechend hohen Verfügbarkeits-Anforderungen und zu entsprechenden Service Level Vereinbarungen mit den Netzbetreibern:

- 24 h x 365 Tage Zugriff auf TK-Server und TK-Anwendungsserver (CC, UM, CTI etc.)
- Einhaltung einer maximalen Antwortzeit, Schwankungsbreite und Verlustrate
- niedrige MTTR
- keine festen Wartungsintervalle mehr

Als eine der wichtigsten Konsequenzen aus diesen Anforderungen ergibt sich eine proaktive Informations- und Event- Strategie für den Betrieb. Zur Erfüllung ihrer Verantwortlichkeiten / SLA-Verpflichtungen müssen Netzbetreiber nicht mehr nur Auswertungen über den kompletten Ausfall von Netzkomponenten sondern weiterreichende Management-Aussagen verfügbar haben, mindestens über

- Erreichbarkeit und Verfügbarkeit des gesamten Kernnetzes (Gefahrenklasse I und II*)
- Erreichbarkeit und Verfügbarkeit der TK-Server
- Durchsatz-Werte für TK-Server, sowie für Einzelkomponenten und Gesamtwege zwischen Telefonen und TK-Servern
- Antwortzeiten von TK-Servern, -Anwendungen sowie einzelnen Telefonen
- Paketverlustraten
- Schwankung von Durchsatz, Delay und Verlustraten

Weiterreichende Aussagen für den Gesamtbetrieb sind

- Event-Korrelation
- Störfall-Analysen
- Reporterstellung
- SLA-Überwachung/Abgleich
- Langzeit-Überwachung/Historienverfolgung
- Accounting

Für Störfalldiagnose und –behebung kommen Aussagen über Protokoll-Aktionen und Telefonie-Prozesse hinzu

- Verbindungsauf– und –abbau
- Ablauf / Kompatibilität der Signalisierung zwischen zwei Komponenten (RTP mit ungerader Portnummer)
- Ablauf der Datensession zwischen zwei Komponenten (RTP mit gerader Portnummer)

Seminar zum Thema

IP-Telefonie: evaluieren, planen, betreiben

Seminar

01. - 03.03.04 Köln

24. - 26.05.04 Köln

Dieses Seminar evaluiert die Technologie und die verfügbaren Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise, analysiert typische Nutzungsformen und gibt eine Prognose für die Marktsituation und weitere Entwicklung.

Referent: Referentin: Dipl.-Inform. Petra Borowka
Preis: € 1.690,-- zzgl. MwSt.

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

Einordnung in eine Management-Architektur

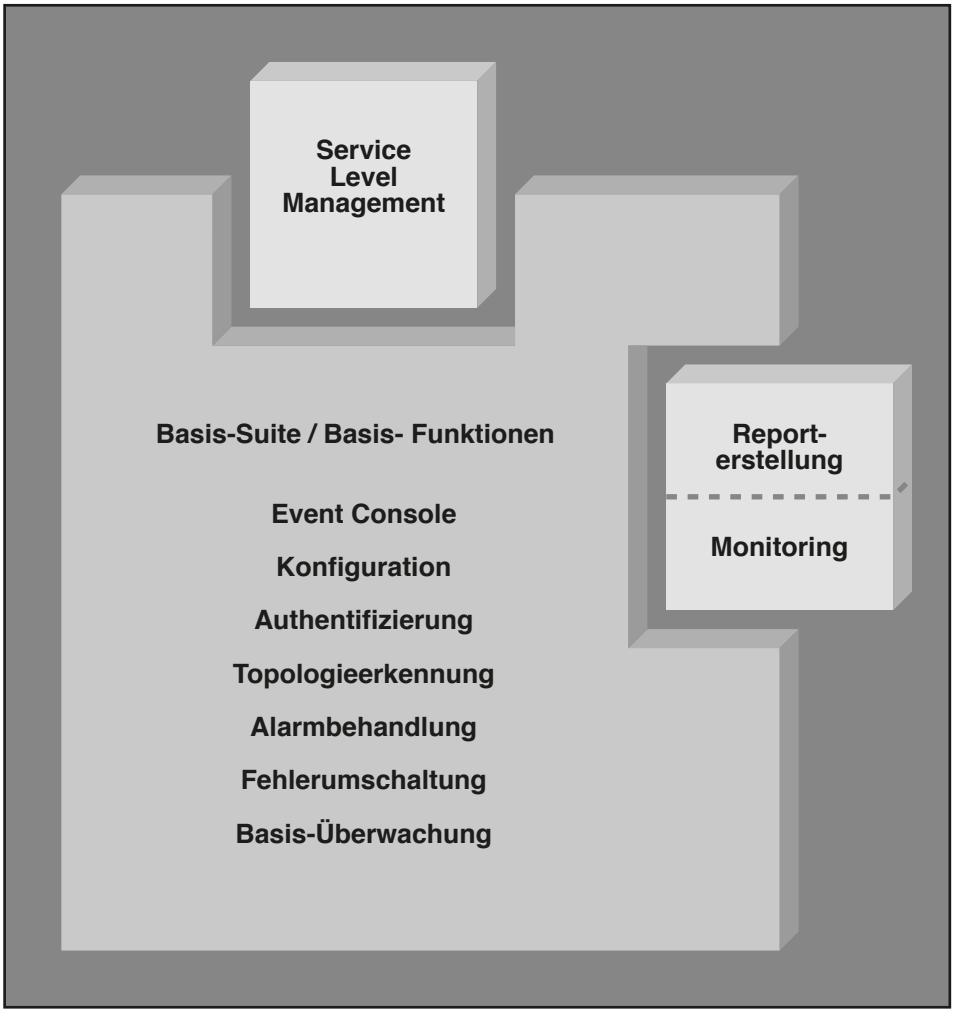
Die erforderlichen Managementfunktionen sind vielfach durch eine Kombination von drei Bausteinen realisierbar: ein Basis-Managementsystem, oft als Basis-Suite oder Element Manager eines Herstellers erhältlich, ein oder zwei Zusatztools für Monitoring und Reporterstellung sowie in ausgeprägten SLA-Umgebungen ein übergeordnetes Service Level Management Tool zur Zusammenführung der Einzelaktionen und Ergebnisse. Diese relativ simple 3-Baustein-Architektur ist in Bild 1 gezeigt.

Der Element Manager (Basis-Suite)

Für eine detailliertere Beschreibung der allgemeinen Element Manager Funktionen wird auf den Netzwerk Insider Artikel "Netzwerkmanagement-Lösungen 2003" vom April 2003 verwiesen, der Fokus liegt in diesem Beitrag auf den Element Manager Funktionen für Voice Komponenten.

Mit einem Element Manager kann die Konfiguration einzelner TK-Server (IP PBX'en) oder auch Mehrfach-Konfiguration (Bulk Action) gleicher Komponententypen wie z.B. IP Telefone über eine grafische oder Browser-Oberfläche durchgeführt und teilweise auf erfolgreiche Aktivierung überprüft werden. Das verwendete Protokoll ist meistens nicht SNMP sondern HTTP. Störfallanzeigen, z.B. über ausgefallene PSTN-Gateways, TK-Server, Telefone oder schlechte Verbindungsqualitäten werden im Event Log der Manager-Konsole angezeigt. Dienstgüteparameter einer Telefonieverbindung werden meistens nicht direkt vom Element Manager, sondern vom TK-Server überwacht. Statusmeldungen bei zu niedriger Qualität müssen in diesem Fall vom TK-Server an den Event Log des Element Managers weitergeleitet werden.

Bild 1: Architektur-Bausteine einer Management-Lösung



Report zum Thema

Voice over IP:

Anforderungs-katalog und Evaluierung

Dieser Report setzt sich kritisch mit dem Thema Voice over IP auseinander und stellt die Fragen nach Leistungsmerkmalen, Sicherheit, Verfügbarkeit und Skalierbarkeit der Produkte wichtiger Hersteller wie Avaya, Alcatel, CISCO, Nortel und Siemens und gibt Kriterien, wann ein Einsatz sinnvoll ist und wann man mit seiner Entscheidung noch warten sollte.

Voice over IP Report
Februar 2003
275 Seiten
Preis: € 398,-- zzgl MwSt.

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

Überwachte Betriebsparameter und Schwellwerte sind z.B.

- BHCA-Werte
- BHCC-Werte
- CPU-Auslastung und CPU-Überlastung von TK-Servern
- Speicher-Auslastung und Überlastung von TK-Servern
- Statuswerte einer Telefonie-Verbindung (d.h. die RTP Parameter Delay, Jitter, Verlustrate)
- Erfassung der Gesprächsdaten (CDR, Call Detail Recording)
- Protokollfehler beim Session-Aufbau oder dem Aushandeln von Leistungsmerkmalen

Die notwendige Entwicklung zu konvergenten Lösungen d.h. Management-Integration von Datennetz und TK-Lösung, soweit bei einem Hersteller eine eigene Lösungspalette in beiden Welten verfügbar ist (z.B. bei Alcatel, Avaya, Cisco, Foundry/Mitel, Nortel Networks), wird schrittweise verfügbar. Etablierte Element Manager Lösungen sind OmniVista von Alcatel, Visability von Avaya, CiscoWorks 2000 von Cisco, Optivity von Nortel Networks.

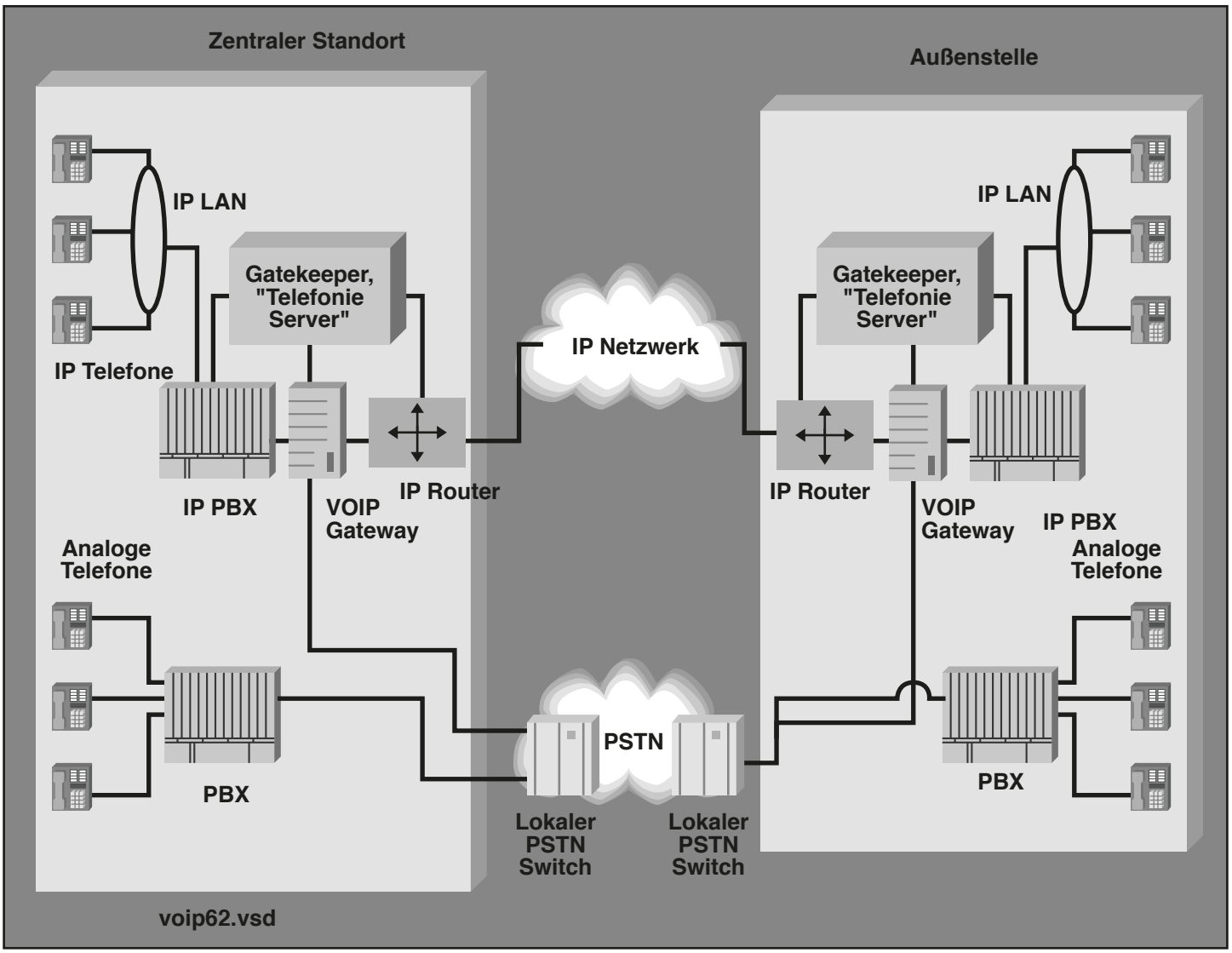
Authentifizierung des Management-Zugriffs, mindestens über CHAP oder RADIUS wird nicht von allen TK-Servern unterstützt. Verschlüsselung mit SSL / SSH oder anderen vernünftigen Verfahren sind noch seltener verfügbar. Als Betreiber sollten Sie entsprechend konsequent die Implementierung solcher Protokolle einfordern.

Voice Monitoring:
Überwachung von Voice Komponenten

Die verschiedenen Komponententypen, die überwacht werden müssen, reichen von der IP PBX bzw. vom Telefonserver über Signalisierung, Trunk oder Media Gateways bis zum Hardphone oder Softphone (wie in Bild 2 gezeigt).

Dazu werden Messverfahren für die physikalischen Verbindungen (dieselben Verfahren wie für die Datenkommunikation), für Datentransfer und Signalisierung bzw. die entsprechenden Kommunikations- und Signalisierungsprotokolle benötigt.

Bild 2: Komponenten für den Betrieb von Sprachanwendungen in IP Netzwerken



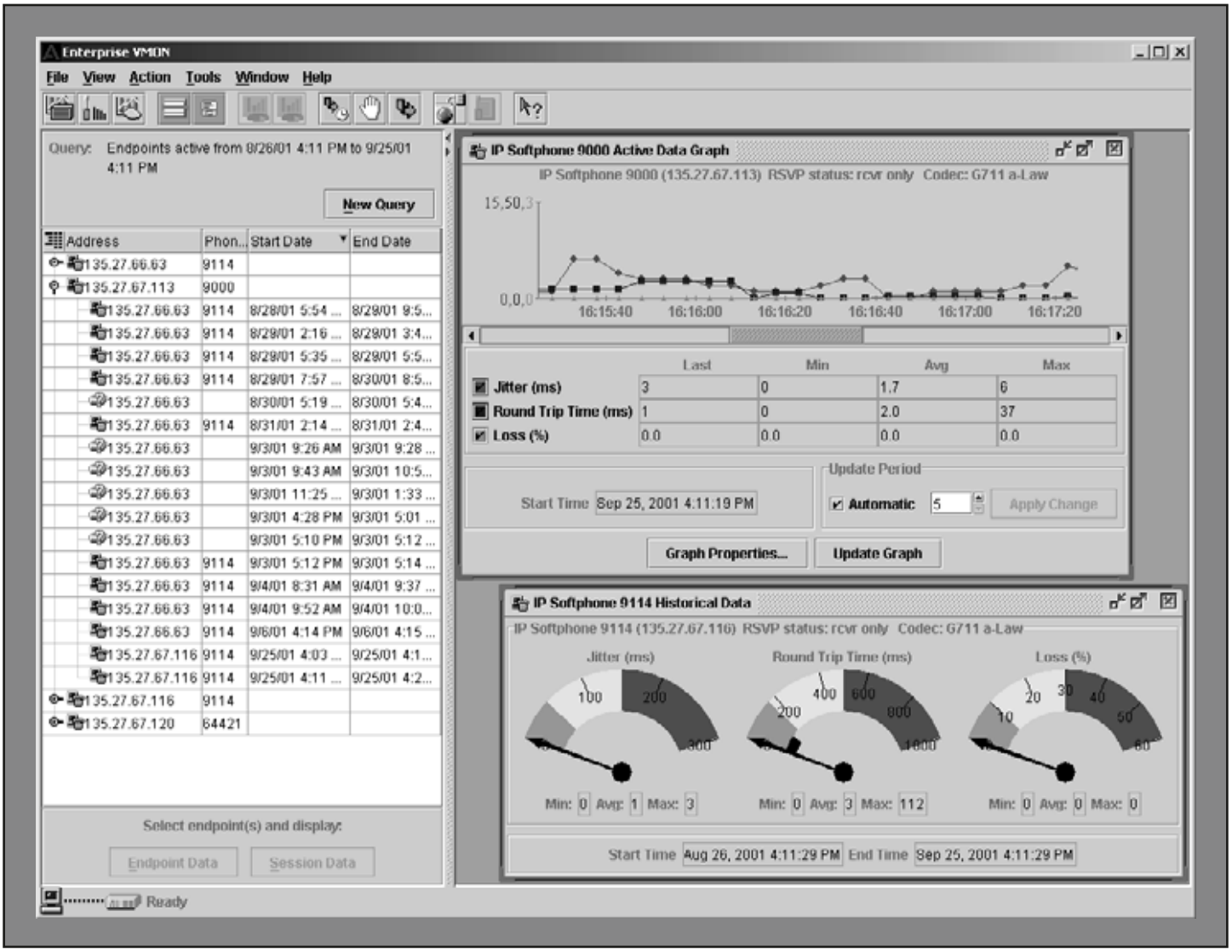


Bild 3: Überwachung eines IP Softphone im LAN mit dem Avaya VoIP Monitoring Manager

Bild 3 zeigt beispielhaft für ein im LAN betriebenes IP Softphone die historische Überwachung von Antwortzeit-Schwankung, Round Trip Delay und Verlustrate sowie die aktuelle Schwellwert-Überwachung dieser Parameter nach dem bekannten Ampel-Schema (grün, gelb, rot) mit dem Avaya VoIP Monitoring Manager. Für eine Beschreibung der verschiedenen Monitoring Konzepte (Client-/Server Monitor, passiver Monitor, aktiver Monitor, verteilte Probes, Kunstlasten etc.) wird auf den Netzwerk Insider Artikel "Netzwerkmanagement-Lösungen 2003" vom April 2003 verwiesen.

Die zum Einsatz kommenden Messtools müssen sowohl die private Betriebsseite als auch den Übergang zu öffentlichen Netzwerken abdecken. Eine Übersicht über die wichtigsten Protokolle, die auf beiden Seiten zum Einsatz kommen, sowie die Komponenten, zwischen denen sie ablaufen, ist in Bild 4 gezeigt.

Monitoring versus Fehlerumschaltung

Soweit Hardware-Störungen und (in begrenztem Umfang) Software-Störungen vorliegen, ist der Netzbetrieb nicht auf manuelle Störfall-Behebung mittels Konfiguration angewiesen, sondern bei Verfügbarkeit und Betrieb entsprechender Redundanzschaltungen kann eine automatische Fehlerumschaltung greifen. So können z.B. TK-Server und Gateways als hot standby oder N+1 Redundanz betrieben werden, Telefongespräche können bei Ausfällen im IP Netzwerks über das PSTN-Netz umgeleitet werden.

Monitoring ist jedoch insofern als komplementäre Maßnahme zu automatischer Fehlerumschaltung zu betrachten, als das Monitoring selbst bei eingehenden Meldungen oder schlechten Überwachungs-Werten eine Fehlerumschaltung initiieren kann, wie in Bild 5 gezeigt wird. Mittels Monitoring lassen sich Störfälle feststellen und überwachen, die nicht durch automatische Fehlerumschaltung behebbar sind, insbesondere Störfälle mit Leistungseinbrüchen, aber nicht Komplettausfällen. Bei zu schlechter Leistung des IP Netzwerks kann das Monitoring z.B. die Umleitung einer Telefon-Session über das PSTN-Netzwerk veranlassen, obwohl das IP Netzwerk grundsätzlich noch verfügbar ist.

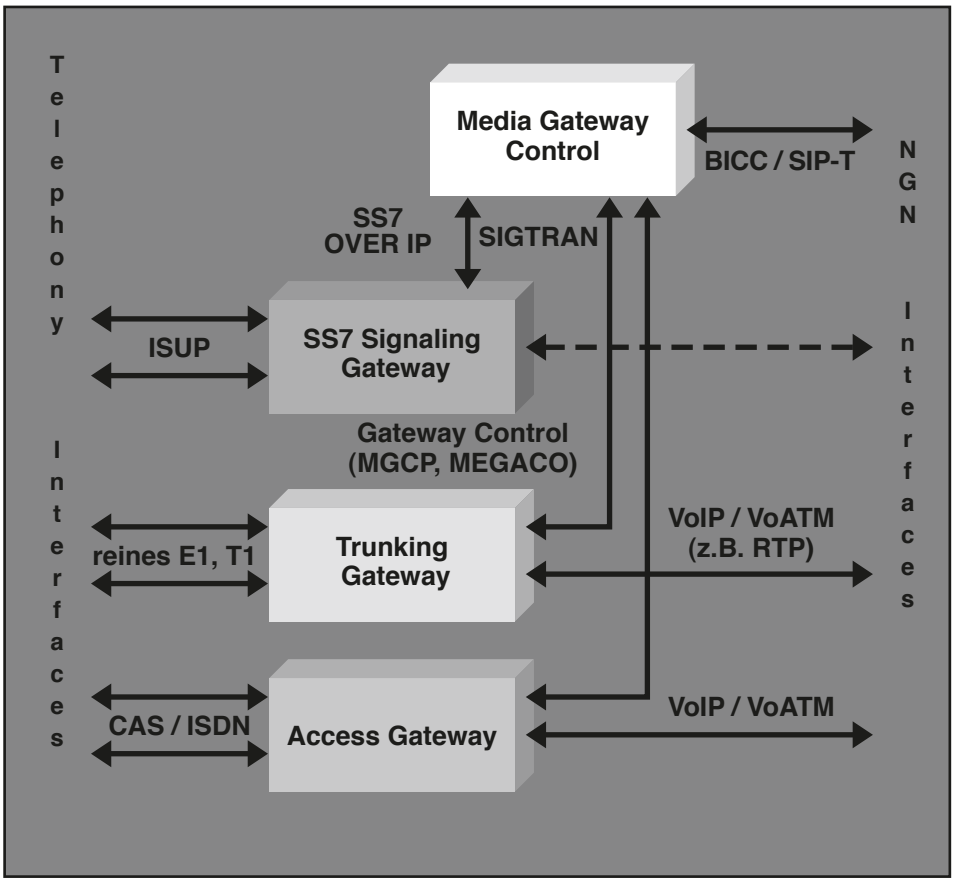
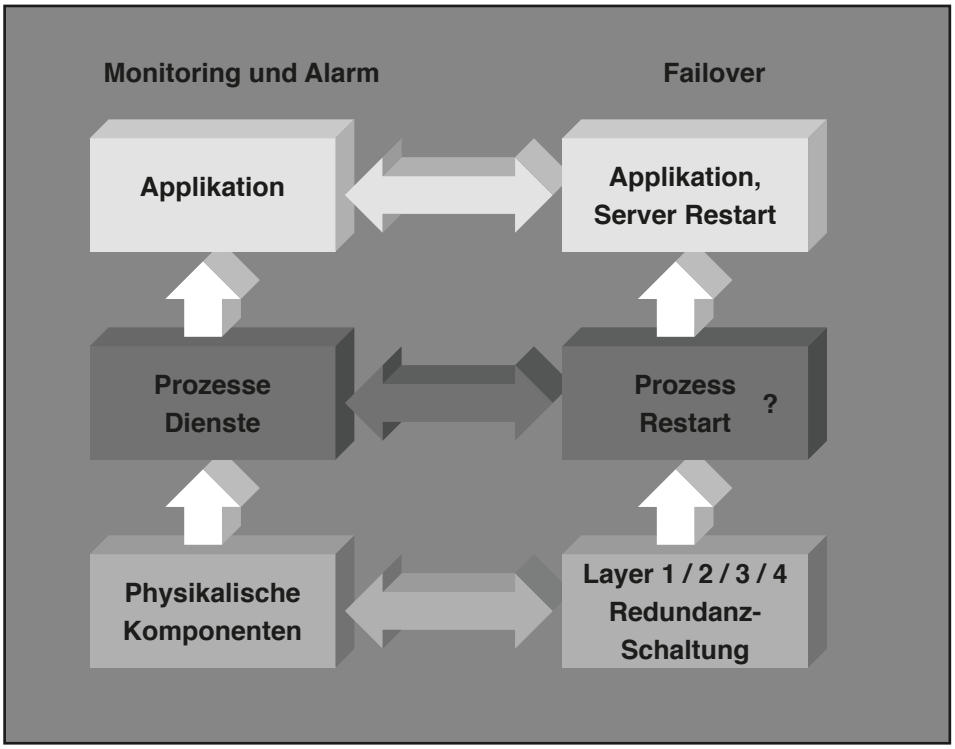


Bild 4: Protokolle und Schnittstellen von Sprachanwendungen

Bild 5: Komplementäres Zusammenspiel von Monitoring und Fehlerumschaltung



Messgrößen für Voice over IP

Ähnlich wie für Datenapplikationen werden im Voice-Umfeld Messwerte für die erreichte Sprachqualität, für Durchsatz, Delay und verstärkt auch Jitter sowohl bei Einzelkomponenten als auch Ende-zu-Ende Verbindungen, bei priorisierten und nicht-priorisierten Verbindungen, bei reinen LAN- und LAN-WAN-Verbindungen benötigt. Ergänzend lassen sich Funktionen für Simulation (Kunstlasten) einsetzen. Insbesondere die Messgrößen Durchsatz, Delay, Jitter und Verlustrate haben wechselseitige Abhängigkeiten, die für die Betriebsoptimierung von Bedeutung sind.

Nachfolgend betrachen wir die genannten Messgrößen und ihren Einfluss auf die Qualität einer Sprachverbindung.

Delay

Das Ende-zu-Ende Delay (Antwortzeit) zwischen Sender und Empfänger ist eine von zwei Hauptmessgrößen für die Überwachung einer Sprachverbindung.

Zu unterscheiden ist hier das One-Way Delay als Übertragungsdauer vom Sender zum Empfänger und das Round Trip Delay als Übertragungsdauer vom Sender über den Empfänger zurück zum Sender.

Das One-Way Delay liefert einen exakten Wert, ist jedoch aufgrund der Entfernung der Messpunkte voneinander sehr aufwändig (GPS in den Messgeräten).

Das Round Trip Delay ist einfacher zu messen, da nur an einem Punkt gemessen werden muss, was die Zeit-Synchronisierung von Senden und Empfangen der Rückantwort sehr einfach macht (z.B. Einsatz eines einzelnen Geräts). Der Nachteil ist, dass die Bestimmung der Ende-zu-Ende Antwortzeit aus dem Round Trip Delay (durch Halbieren des erhaltenen Wertes) im Regelfall ungenau ist, da das Delay meistens nicht in beiden Richtungen identisch ist. Der so erhaltene Antwortzeit-Wert ist ein Schätzwert mit umso höheren Ungenauigkeiten, je größer die Differenz zwischen Hin- und Rückweg der gemessenen Session ist.

Aufgrund der besseren Praktikabilität wird jedoch meistens mit Roud Trip Werten gearbeitet. Insbesondere sollte dann darauf geachtet werden, dass der Hin- und Rückweg tatsächlich derselbe ist und nicht aufgrund unsymmetrisch gesetzter Routingkosten in Sende- und Empfangsrichtung verschiedene Wege genommen werden!

Tests mit mehreren Benutzergruppen ergaben, dass bei einem Delay von maximal 100 ms bis 150 ms in einer Richtung die Verbindung als "Toll-Quality", d.h. gleichwertig zur PSTN-Telefontechnik empfunden wird. Die meisten Teilnehmer vermerken ein Round Trip Delay (auch RTT, Round Trip Time genannt) von mehr als 250 ms als Qualitäts-Einbuße, bei einem Delay von 500 ms (entspricht einem langsamen geostationären Satelliten) und mehr wird die Qualität als unakzeptabel empfunden. Die ITU-T legt in ihrer Empfehlung G.114 entsprechend eine Obergrenze von 150 ms für das One-Way Delay fest, die IEEE definiert in ihrem QoS Standard 802.1D/p 100 ms als erforderliches maximales One-Way Delay für Voice. In der Praxis muss auch beachtet werden, dass Gesprächsdaten und Signalisierung aufgrund der unterschiedlichen Protokolle zu unterschiedlichen Messwerten führen können. Dies gilt insbesondere für die Signalisierung beim Sessionaufbau. Es reicht daher nicht, bei einer Voice-Implementierung nur die Datenstreams zu messen.

Das Messbeispiel in Bild 6 zeigt das One-Way Delay eines 8 Minuten langen Gesprächsausschnitts mit Durchschnitts-Werten von 50 ms bis 60 ms und Peakwerten von 100 ms bis 120 ms. Die gemessene Sprachverbindung hat somit hinsichtlich Delay eine noch akzeptable Qualität.

Das Messbeispiel in Bild 7 zeigt das durchschnittliche Round Trip Delay verschiedener gemessener Gespräche. Dieses schwankt zwischen 40 ms bis 50 ms und 140 ms bis 150 ms, umgerechnet ein One-Way Delay von 20 ms bis 25 ms und 70 ms bis 75 ms. Die gemessenen Gespräche haben daher eine sehr gute Qualität.

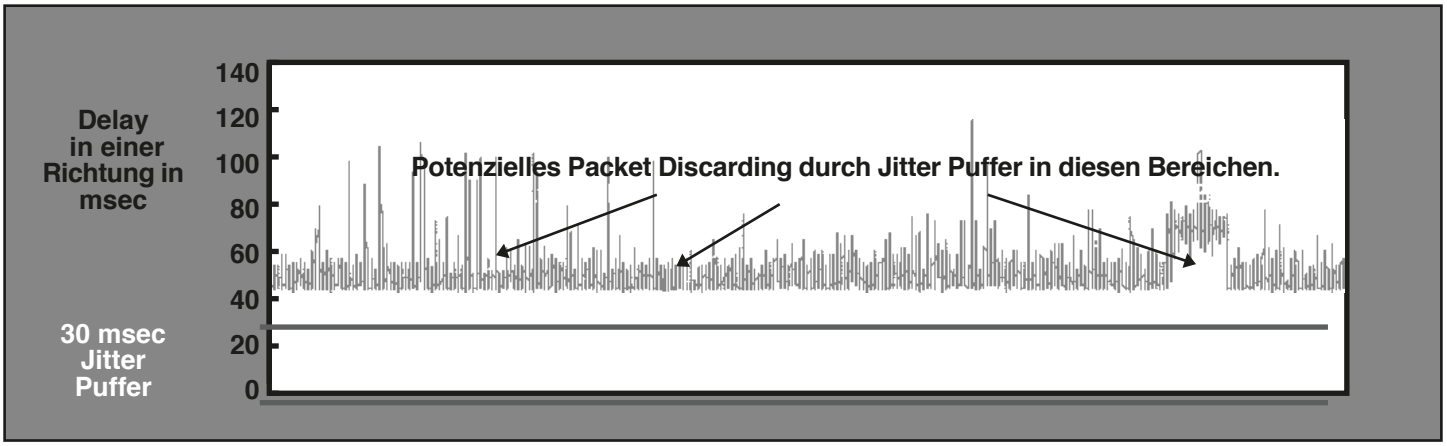
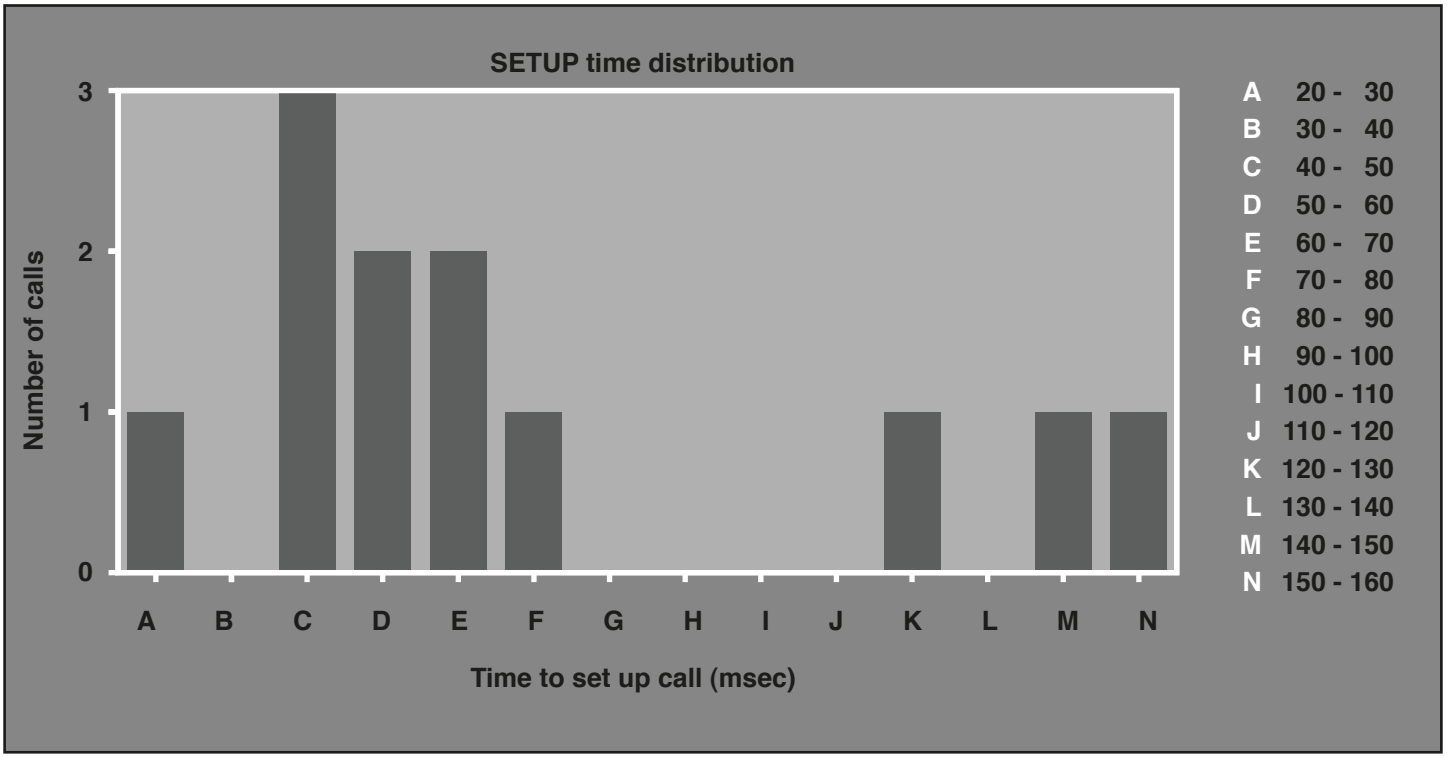


Bild 6: Messbeispiel von 8 Minuten Gesprächsdauer mit gemessenem One-Way Delay

Bild 7: Messbeispiel von 12 Gesprächen mit gemessenem Round-Trip Delay



Die tatsächlich erreichbare Antwortzeit während eines Telefongesprächs wird durch eine Reihe Faktoren geprägt: Schon beim Codec ist die Frage: Kompression oder nicht? Der Einsatz von Kompression kann z.B. zusätzliche 15 ms bei Sender und Empfänger bedeuten. Für einzelne verbreitete Codecs führen wir hier das spezifische Delay auf:

- G.711 vernachlässigbar (keine Kompression)
- G.723 benötigt 30 ms
- G.729 benötigt 15 - 25 ms

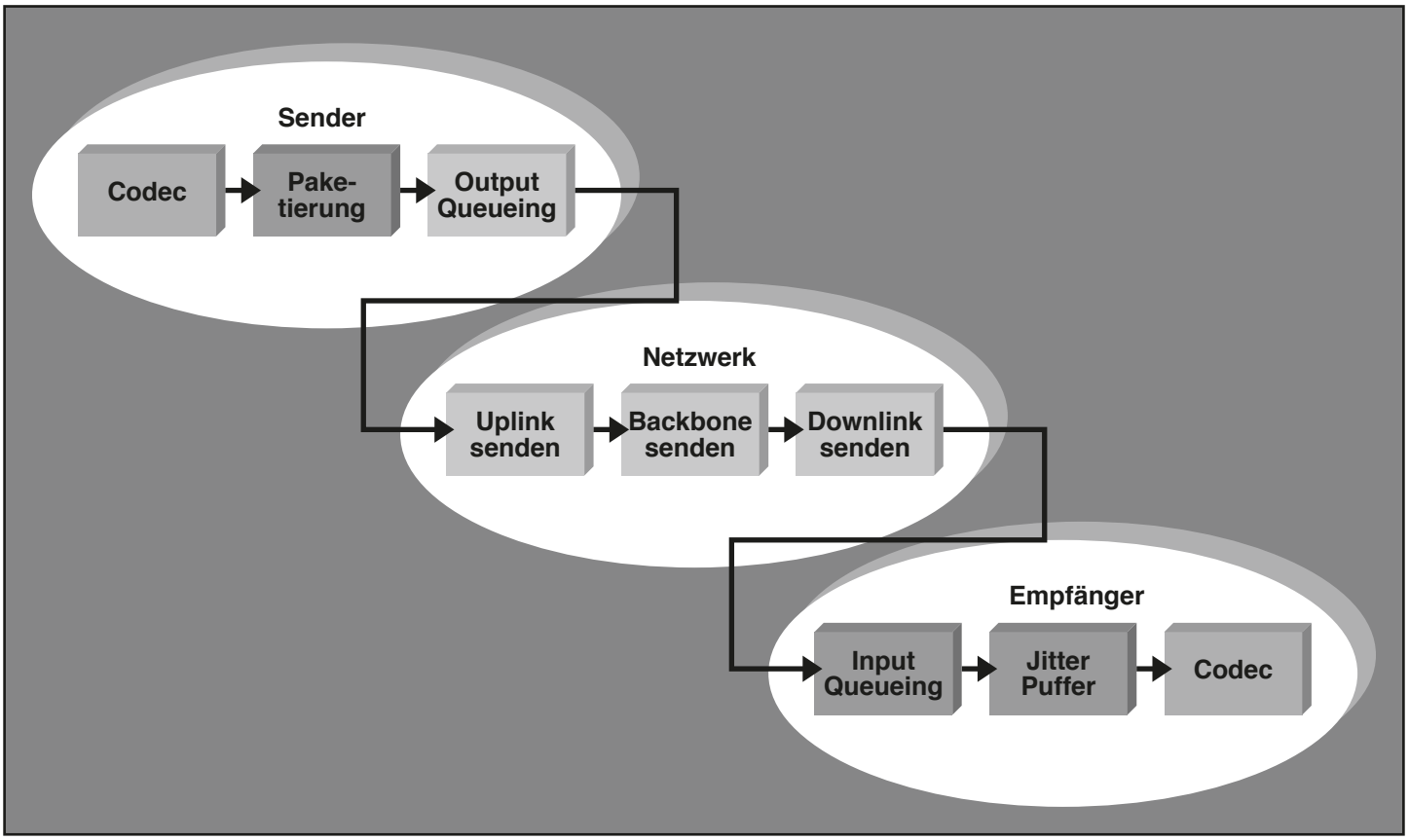
Die Paketierung der Voice-Anwendung beeinflusst das Delay durch die Anzahl Frames** pro IP Paket (1, 2, 4, ...). Je mehr Frames in ein Paket gepackt werden, desto höher wird die Nutzrate, desto höher wird aber auch das Delay. Die Empfehlung ist hier: im LAN nur 1 Frame pro Paket, im WAN nicht mehr als 2 Frames pro Paket; letzteres benötigt typischerweise maximal weitere 5 ms Delay. Falls zusätzlich Verschlüsselung aktiviert ist, kommen nochmals 10 bis 20 ms hinzu. Queueing- und Serialisierungs-Delays in allen Netzkomponenten wie Switches und Router liegen in Summe bei 20 bis 40 ms, aber auch mal bei bis zu 200 ms, zzgl. 5 bis 25 ms für die physikalische Entfernung. Last but not least muss jeweils ein Jitter Puffer beim Empfänger (15 bis 50 ms) und allen Zwischen-Gateways (25 bis 35 ms) durchlaufen werden. Eine grafische Darstellung der kaskadierten Delay-Faktoren in einer Sprachverbindung ist in Bild 8 dargestellt.

Jitter und Jitterpuffer

Jitter bedeutet die Schwankung, die bezogen auf die durchschnittlichen Leistungswerte real auftritt. Der am häufigsten betrachteten Jitterwert ist die Schwankung der Antwortzeit. Diese bedingt, dass die Pakete am Empfänger nicht mehr im Takt der Senderate, sondern verzögert oder "zu schnell" ankommen. Da jedoch die empfangenen Pakete mit einer festen Rate an den Decodierer weitergegeben werden müssen, wird ein so genannter Jitter Puffer benötigt, der die Schwankung der Antwortzeit ausgleicht, wie später erklärt wird. Die Messung der Antwortzeit-Schwankung wird one-way durchgeführt und benötigt keine Synchronisation, da nicht das Ende-zu-Ende Delay sondern die Zwischenankunftszeit zwischen den einzelnen Paketen gemessen wird. Auch für Jittermessungen gilt: Die Schwankung muss nicht in beiden Richtungen gleich sein. In mittelmäßig oder höher ausgelasteten Netzen ist eher das Gegenteil der Fall, da die Wege von den Servern zu den Clientsystemen höher ausgelastet sind als in umgekehrter Richtung. Wichtig für eine korrekte Berechnung sind:

- Kenntnis / Programmierung der tatsächlichen Sende-Intervalle
- Berücksichtigung von Reihenfolgevertauschungen
- Berücksichtigung von Paketverlusten durch Prüfen der Sequenznummern
- Berücksichtigung von Silence Suppression (bei G.729 z.B.oft bis zu 60% der übertragenen Pakete !): Zu Beginn der Silence Suppression wird das letzte gesendete Paket markiert, am Ende der Silence Suppression wird das erste gesendete Paket markiert. Das Intervall von vor dem ersten markierten Paket bis nach dem letzten markierten Paket muss bei der Jitterberechnung ignoriert werden.

Bild 8: Delayfaktoren einer Sprachverbindung



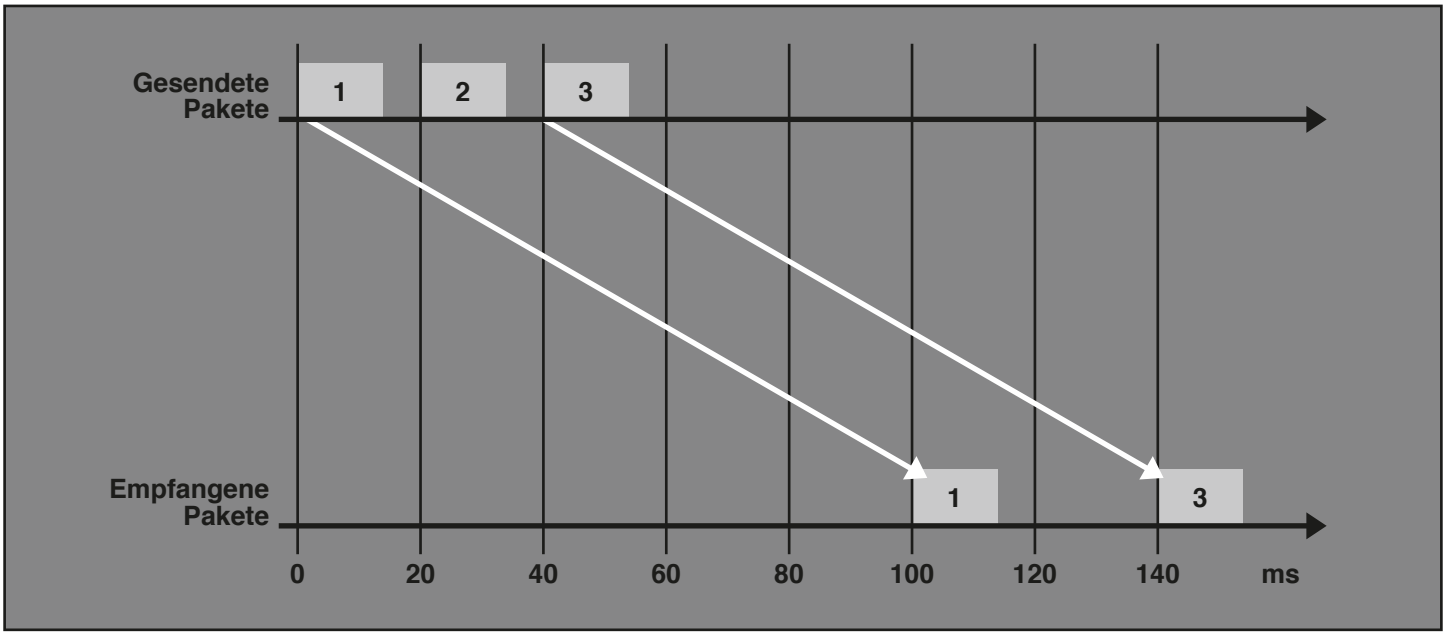


Bild 9: Messung der Zwischenankunftszeit zur Jitter-Bestimmung

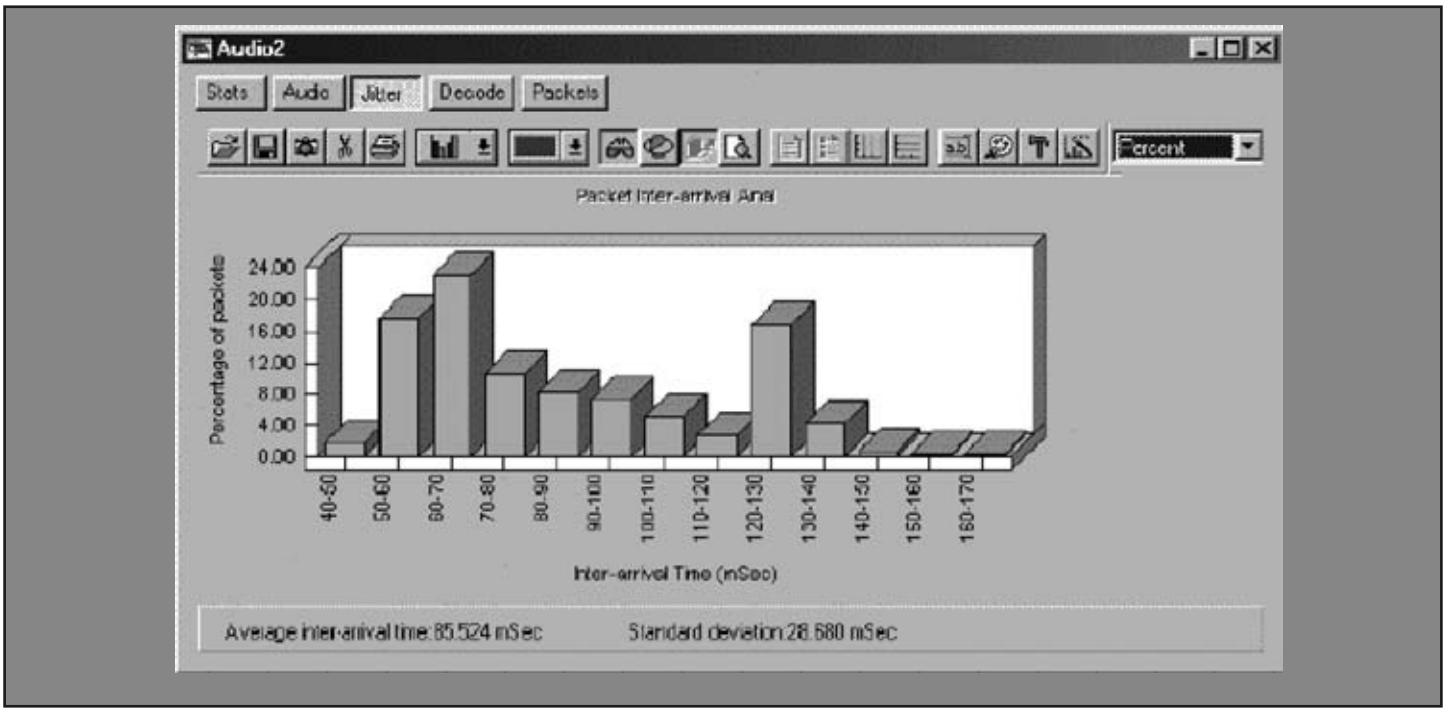
Das Beispiel in Bild 9 zeigt eine Zwischenankunftszeit von 40 ms bei einem Sendetakt von 20 ms. Gemessen wurde aber die Zeit zwischen Paket Nr. 1 und Nr. 3. Die tatsächliche Zwischenankunftszeit muss jedoch zwischen Paket Nr. 1 und Nr. 2 gemessen werden, welches sich entweder verzögert hat oder ganz verlorengegangen ist. Im ersten Fall ist der tatsächliche Jitter größer als 20 ms, im zweiten Fall kleiner als 20 ms!

Das Messbeispiel in Bild 10 zeigt ungünstige Werte: ca. 50 % der Pakete haben eine Zwischenankunftszeit von 50 ms bis 80 ms. Diese Schwankung würde durch einen Jitter-Puffer von 30 ms aufgefangen.

Sollen jedoch auch die ca. 16% Pakete mit einer Zwischenankunftszeit von 120 ms bis 130 ms noch "in time" empfangen werden, müsste der Jitterpuffer 80 ms lang sein! Dies ist jedoch unpraktikabel, da der Jitter Puffer alleine dann schon zwei Drittel eines Delay Budgets von 120 ms verbrauchen würde!

Hier müssen Netzdesign, Netzkonfiguration, Konfiguration der TK-Komponenten und TK-Anwendungen so geändert werden, dass die Häufung um den Wert 120 ms bis 130 ms entfällt.

Bild 10: Beispielmessung einer Verteilung der Zwischenankunftszeiten



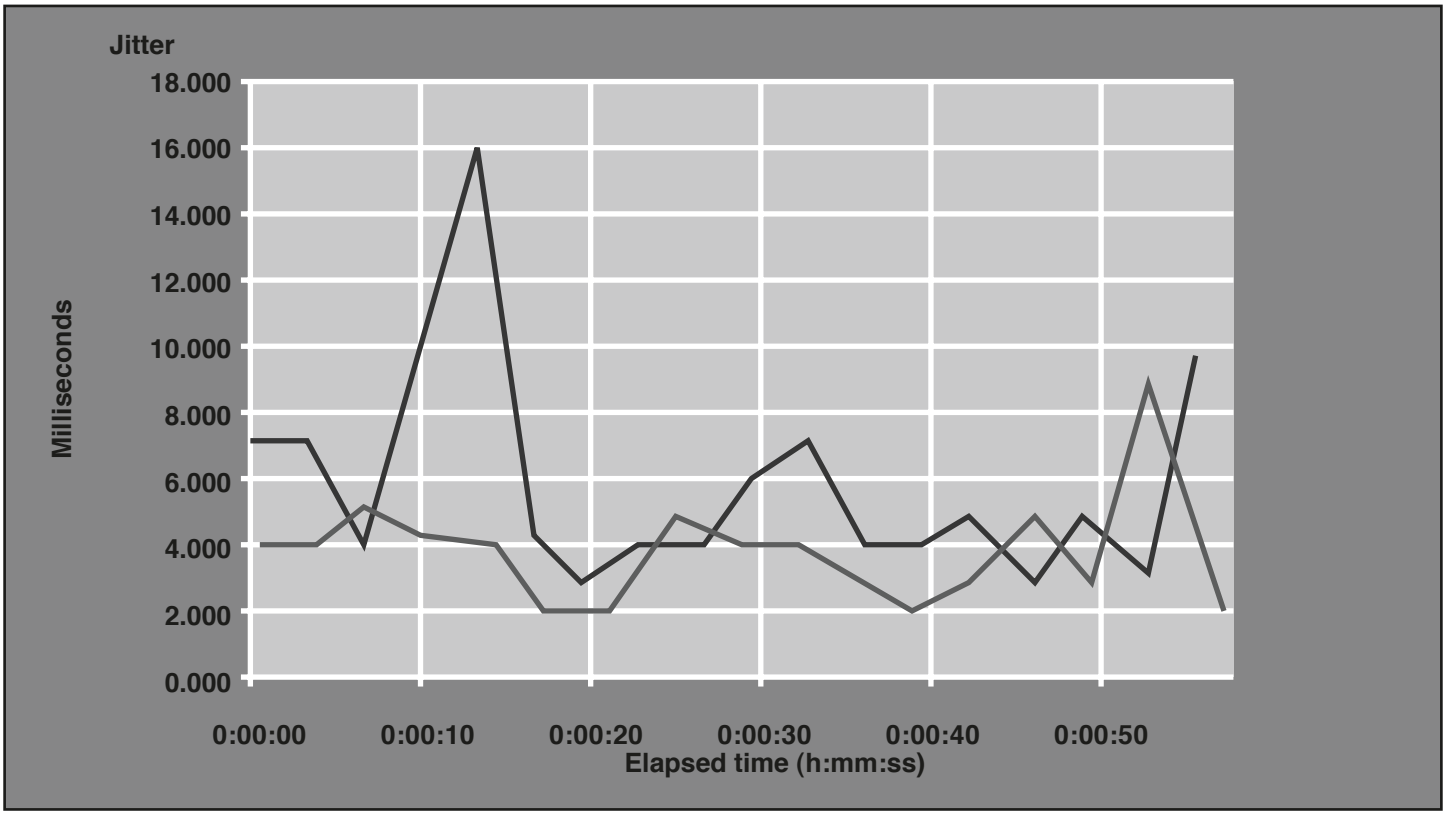


Bild 11: Gemessener Jitter für beide Richtungen einer RTP Session

Das Messbeispiel in Bild 11 zeigt dagegen sehr angenehme Werte, die für 100% der Pakete in einer Richtung einen maximalen Jitter von 16 ms ergeben, in der Gegenrichtung einen maximalen Jitter von 9 ms. Ein Jitterpuffer von 20 ms führt dazu, dass alle Pakete "in time" empfangen werden können.

Der Jitterpuffer wirkt nun folgendermaßen: Alle Pakete, die innerhalb einer Schwankung von der Größe des Jitterpuffers ankommen, können im Jitterpuffer zwischengespeichert und anhand ihrer Sequenznummer eingeordnet werden.

Alle Pakete mit einer größeren Schwankung werden als "out of time" verworfen, auch wenn sie korrekt empfangen werden. Die als "out of time" verworfenen Pakete gehen in die Verlustrate ein. Jedes "in time" empfangene Paket muss den Jitter Puffer vollständig durchlaufen, d.h. die Größe des Jitter Puffers geht als zusätzliches Delay in die Antwortzeit ein.

Bei der Konfiguration des Jitterpuffers oder der Programmierung einer automatischen Anpassung bestehen daher Trade Offs:

Je größer der Jitterpuffer, desto höher das Delay

Je kleiner der Jitterpuffer, desto höher die Verlustrate

Auf der Basis der Jitter-Messung lässt sich die Größe des benötigten Jitter Puffers bestimmen: Als Schritt 1 ergibt die kumulative Summe der Abweichung der Zwischenankunftszeiten den so genannten Bias. In Schritt 2 wird die Normalisierung des Bias um die 0-Abweichung herum berechnet. Als Schritt 3 wird der gewünschte Prozentwert empfangener Frames festgelegt, z.B. 98%. Schritt 4 ergibt als Formel für die Puffergröße

bei Verlustrate <= 2 %

Jitterpuffer := 98% des gemessenen Bias

Ein Beispiel: Wenn das mittlere Delay einer Sprachverbindung 70 ms beträgt (= 0-Abweichung) und mindestens 98% aller Pakete mit einer Zwischenankunftszeit von 25 ms bis 45 ms ankommen, führt eine Größe des Jitterpuffers von 20 ms zu maximal 2% Verlustrate. Wird der Jitterpuffer auf 20 ms konfiguriert, werden Pakete zwischen 25 ms und 45 ms Delay als "in time" akzeptiert. Dynamische Jitterpuffer passen sich selbständig der jeweils aktuellen Schwankung so an, dass eine maximale Verlustrate nicht überschritten wird.

Verlustrate

Die zweite wichtige Messgröße für die Qualität einer Sprachverbindung ist die Paketverlustrate. Versuchen Sie, spontan folgende Fragen zu beantworten:

> Welche Verbindung hat die bessere Qualität? Bei welcher Jitterpuffergröße?
>
> G.711 mit 3% Verlustrate, 150 ms Delay, 30 ms Jitter, Packet Loss Concealment eingeschaltet
>
> G.729a mit 2% Verlustrate, 160 ms Delay, 20 ms Jitter, Packet Loss Concealment ausgeschaltet

Als erstes gilt: Die reine Betrachtung der Durchschnittswerte ist nicht ausreichend. Der Verlust einzelner Pakete hat bis zu einer viel höheren Rate keinen oder wenig Einfluss auf die Sprachqualität als der Verlust mehrerer aufeinanderfolgender Pakete (Burst Loss). Letzteres führt zu Rauschen oder "Lücken" beim Empfänger. Zweitens kann die Verlustrate in beiden Richtungen einer Verbindung unterschiedlich sein. Es reicht also nicht, nur eine Richtung zu messen.

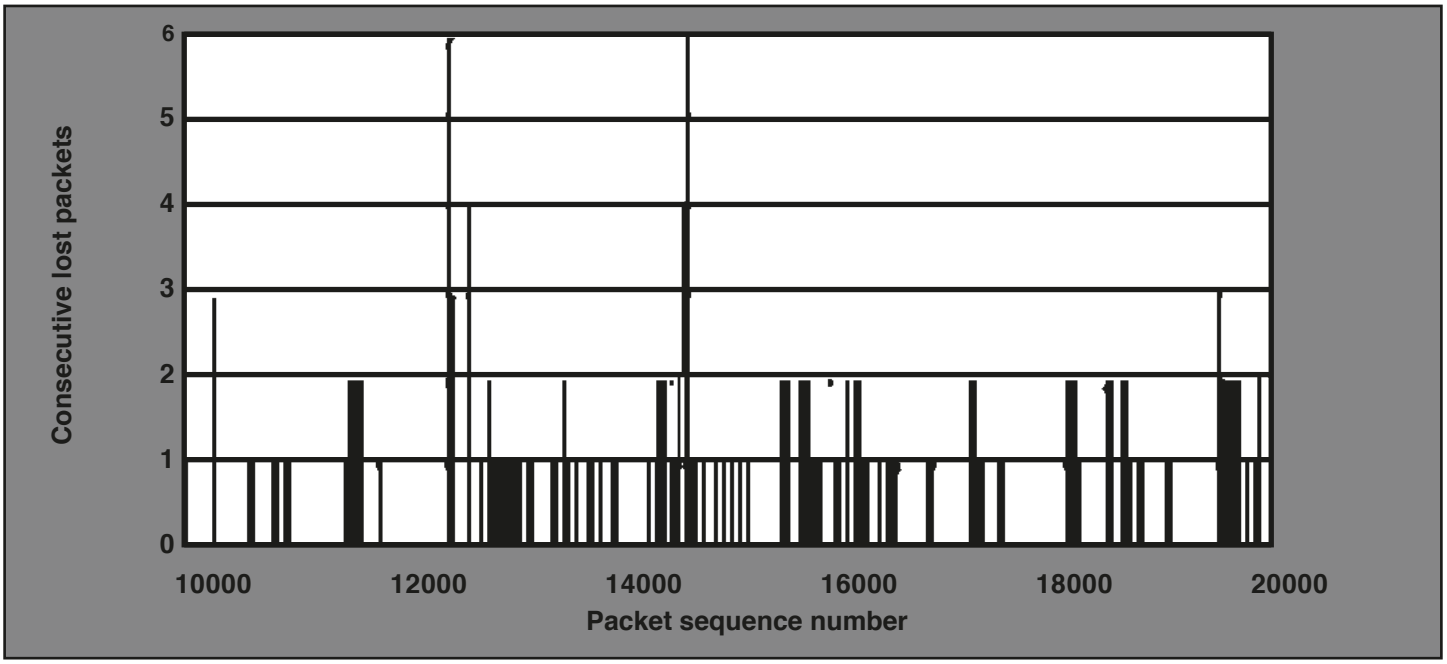


Bild 12: Messbeispiel mit Paketverlst und Burst-Verlust-Anzeige

Das Auftreten und die Verteilung von Bursts sind ein wichtiger Faktor:

5 % Verlustrate mit jeweils 1 verlorenem Frame ist vielfach unkritisch (bei G.711)

2 % Verlustrate mit jeweils 9 verlorenen Frames bei G.729 können kritisch sein

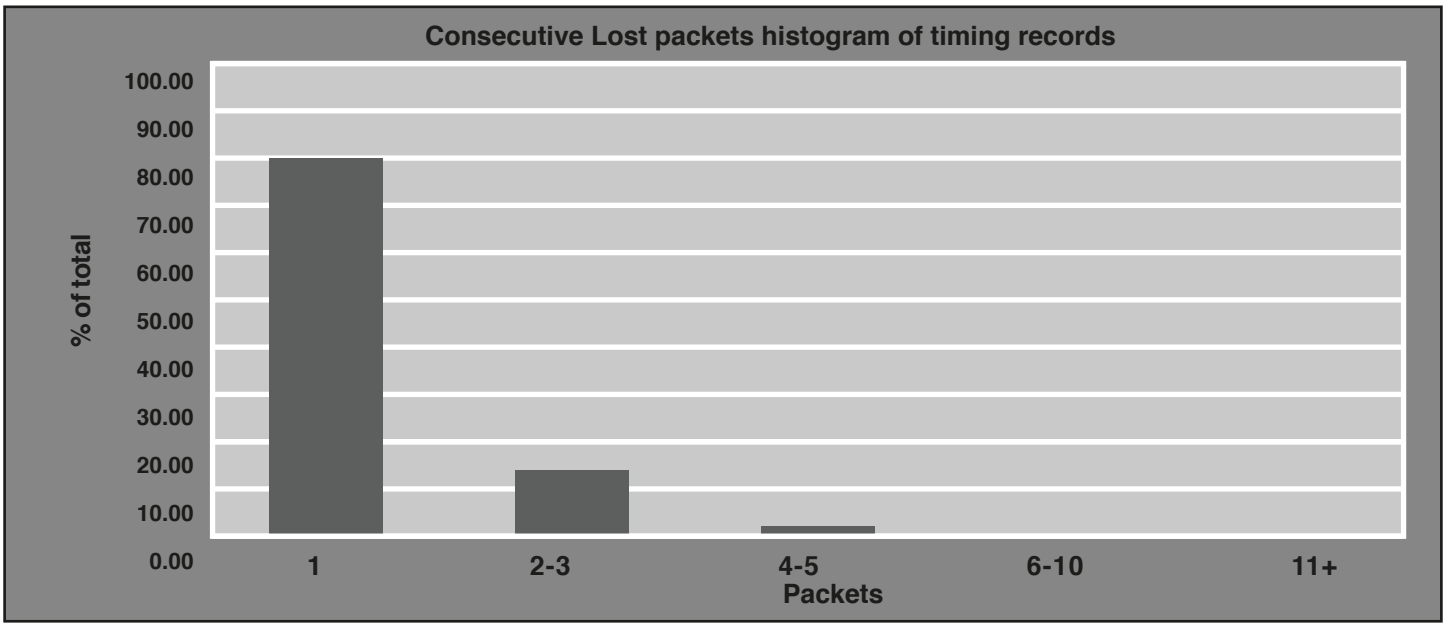
0,5 % Verlustrate in 3 Minuten bei real 2 Sekunden 50% Verlustrate sind unakzeptabel

Das Messbeispiel in Bild 12 zeigt eine Verlustverteilung mit überwiegend Einzelpaketen, teilweise zwei aufeinanderfolgenden Paketen und wiederkehrenden Bursts von 6 Paketen.

Das Messbeispiel in Bild 13 zeigt eine Verlustverteilung, bei der die meisten Verluste Einzelpakete sind und Bursts von 4 bis 5 Paketen nur zu etwa einem Prozent vorkommen.

Zusätzlich bestehen weitere Abhängigkeiten: Erstens füllt die Aktivierung von Packet Loss Concealment (Wiederholung des letzten empfangenen Frames** anstelle des fehlenden Frames) zwar die Lücken, bedeutet aber zusätzliches Delay. Zweitens sind Codecs mit starker Kompression erheblich verlustanfälliger als G.711 (arbeitet ohne Kompression), d.h. schon geringe Verluste sind aufgrund der Kompression nicht mehr korrigierbar und führen beim Empfänger zu Qualitätseinbußen.

Bild 13: Messbeispiel mit prozentualer Verlustverteilung



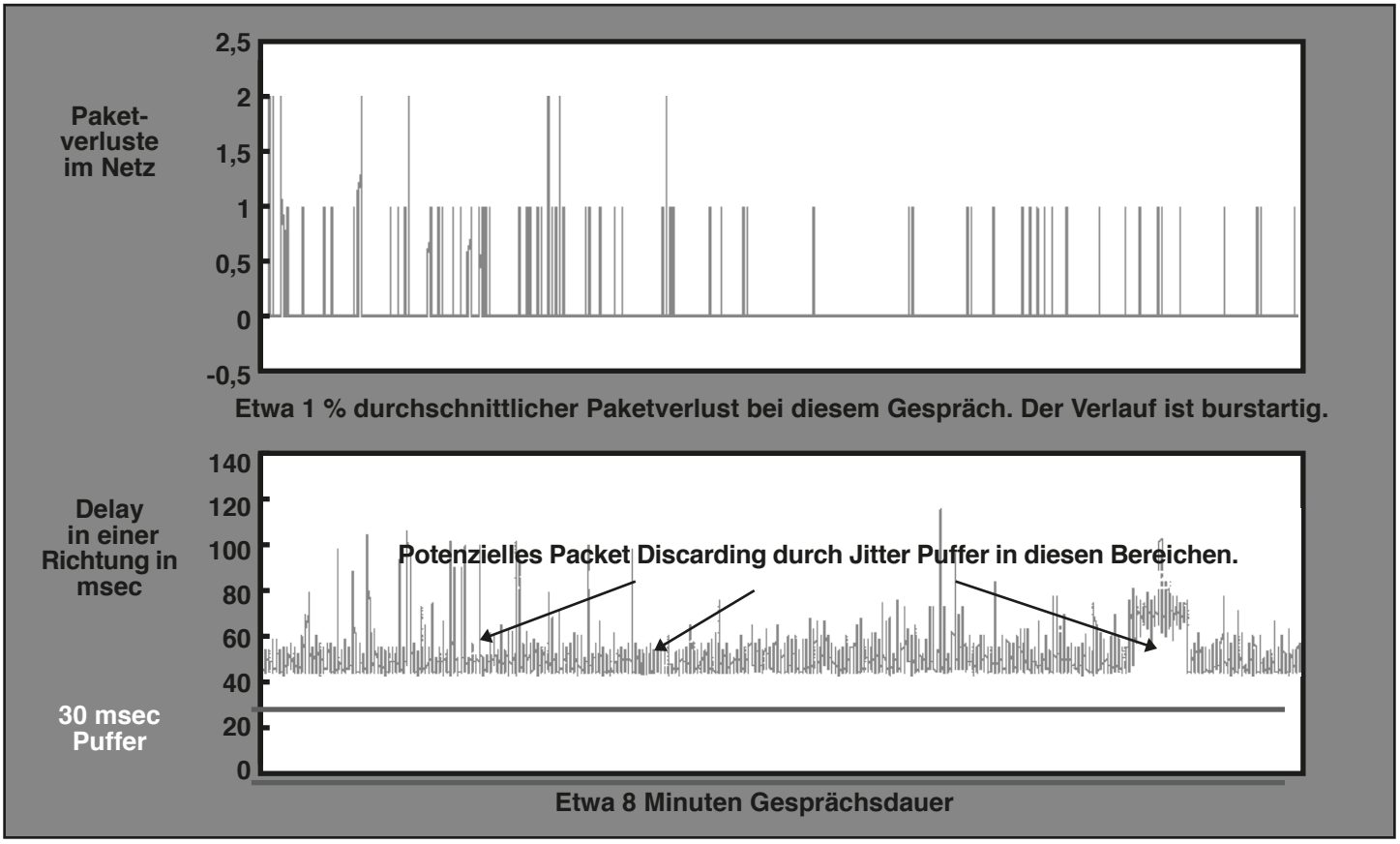


Bild 14: Delay und Verlustrate derselben Messung

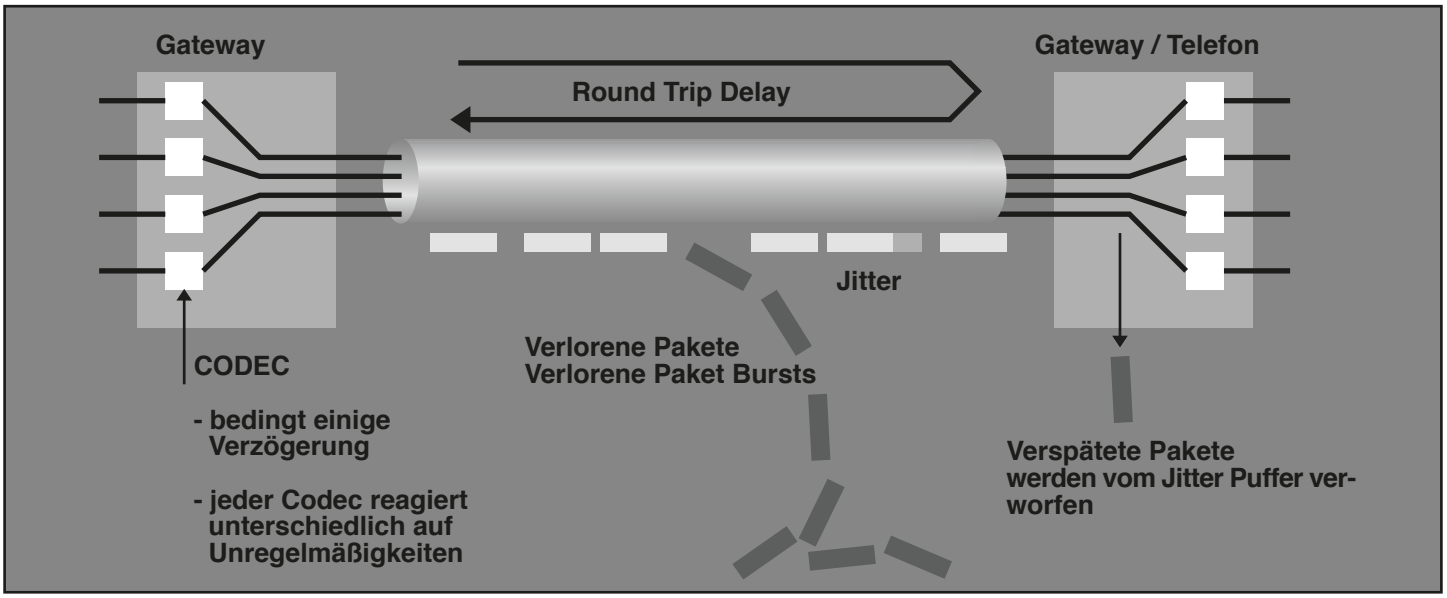
Die tatsächliche Sprachqualität hängt also mindestens ab von einer Kombination der Faktoren

- Delay
- Verlustrate
- Burst-Verluste
- Codec
- Packet Loss Concealment

Die wechselseitigen Abhängigkeiten führen zu Trade-Offs, d.h. es lassen sich nicht alle Werte gleichzeitig optimieren. Das Messbeispiel in Bild 14 zeigt den Zusammenhang von Delay und Verlustrate (inkl. "out of time" Paketen).

Das Zusammenspiel von Delay, Verlustrate und Jitterpuffer ist in Bild 15 gezeigt. Nachfolgend fassen wir die Abhängigkeiten zusammen:

Bild 15: Labiles Gleichgewicht: Delay, Verlustrate und Jitterpuffer



Codec und Delay:

- Je niedriger die Datenrate, desto höher die Codec-Komplexität / CPU-Last
- Je höher die Codec-Komplexität (aufgrund Kompression), desto höher das Delay
- Je höher das Delay, desto schlechter die Qualität

Verlustrate und Sprach-Qualität:

- Je niedriger die Datenrate (je stärker die Kompression), desto höher die Verlust-Anfälligkeit
- Je höher der Delay-Jitter, desto höher die Verlustrate
- Je höher die Verlustrate, desto schlechter die Qualität

Jitterpuffer, Delay und Verlustrate:

- Je größer der Jitter, desto größer der Jitterpuffer
- Je größer der Jitterpuffer, desto höher das Delay
- Je kleiner der Jitterpuffer, desto höher die Verlustrate

Auslastung:

- Je höher die Auslastung, desto höher das Delay und die Verlustrate
- Je mehr Frames pro Paket, desto niedriger die Datenrate, desto höher das Delay

Bewertung der Sprachqualität

Zur Kontrolle existierender Implementierungen oder auch Voruntersuchung von Produkten und Lösungen ist eine Bewertung der erreichten Sprachqualität wichtig. Die zuverlässigste Bewertung wird mit dem MOS-Verfahren (Mean Opinion Score) durchgeführt, das in der ITU-T Empfehlung P.800 beschrieben ist. Hierbei bewertet eine ausreichend große Gruppe von Testpersonen ein abgespieltes Sprachsample mit Werten von 1 bis 5 mit der Bedeutung 1 = unakzeptabel, 4 = PSTN-Qualität, 5 = höchste Bewertung (siehe auch Bild 16).

Untersuchungen wie im Messbeispiel Bild 17 ergaben, dass sich bei Verlustraten von 3 Prozent oder mehr Burst-Verluste erheblich stärker auf die Bewertung auswirken als statistische Verluste von Einzelpaketen. Es zählt auch der "menschliche Faktor" – und der Mensch ist vergesslich.

Bild 16 (oben):
Bewertung der Sprachqualität mit MOS

Daher wirkt sich der zeitliche Abstand eines Qualitätseinbruchs vom Gesprächsende auf den MOS Wert aus: Wurde bei einem Gespräch von 60 Sekunden zu einem definierten Zeitpunkt ein "Rauschen" erzeugt, so ist die Gesamtbewertung des Gesprächs umso schlechter, je näher der Zeitpunkt am Gesprächsende liegt. Dieses Phänomen wird Recency-Effekt genannt und ist in Bild 18 dargestellt.

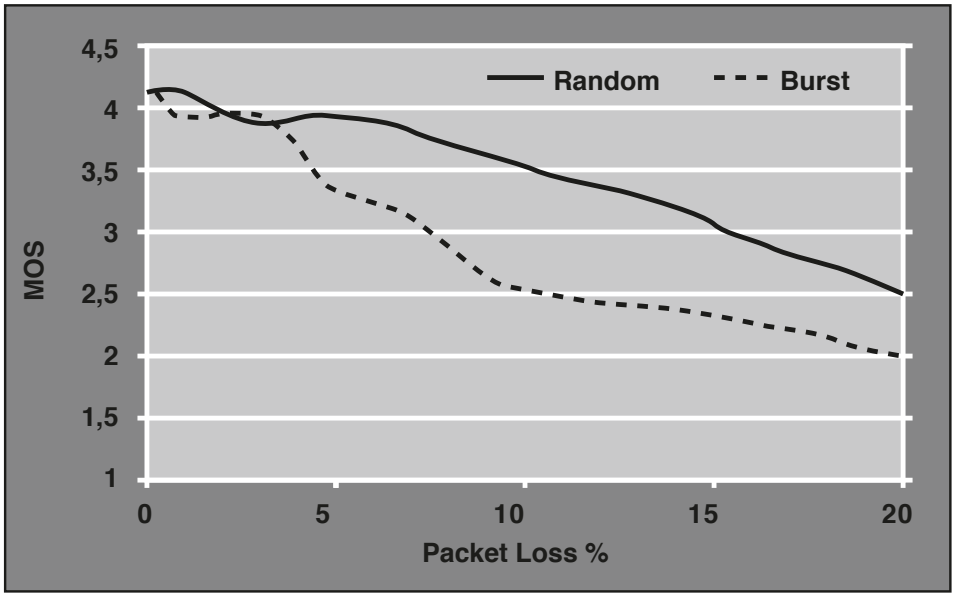
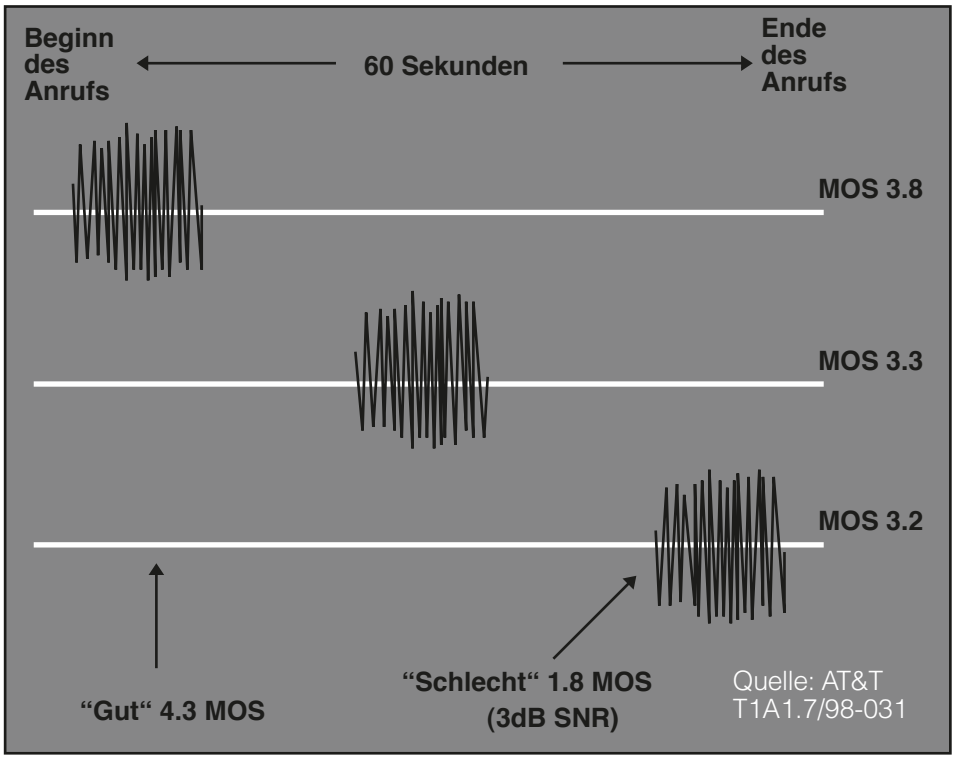


Bild 17 (Mitte): Random-Verluste, Burst-Verluste und resultierender MOS-Wert

Bild 18 (unten): Der Recency-Effekt



Da die Befragung von Testpersonen sehr aufwändig ist, wurden automatisierte Bewertungsverfahren für Sprachqualität entwickelt, die der Bewertung durch Testpersonen möglichst gut entsprechen.

Ein erstes Verfahren, das von der ITU-T als Empfehlung P.861 übernommen wurde, ist das Perceptual Speech Quality Measurement (PSQM, PSQM+) mit einer Bewertung von 0 bis 6,5, wobei 0 die beste Bewertung ist (0 = keine Qualitätseinbuße). Dieses Verfahren ist jedoch eher auf leitungsvermittelte Netze (PSTN) fokussiert, in denen keine Paketverluste (hier gibt es keine Pakete!) und kein Jitter auftreten. PSQM korreliert daher mit den MOS Werten für paketvermittelte Netze (d.h. praktisch IP Netze) nicht so gut.

Zur Verbesserung der Grenzen von PSQM entwickelte BT das Verfahren PAMS (Perceptual Analysis / Measurement System, welches Jitter- und Paketverlust-Phänomene besser berücksichtigt und daher mit MOS besser korreliert als PSQM (Versuche ergaben für PAMS Korrelationen bis zu = 0,9). PSQM und PAMS senden ein Referenzsignal durch das Telefonnetz (PSTN oder IP oder gemischt) und vergleichen das gesendete Signal mit dem empfangenen Signal mittels Digital Signaling Processing Algorithmen.

Aus den Stärken von PSQM und PAMS wurde PESQ entwickelt (Perceptual Evaluation of Speech Quality, ITU-T Empfehlung P.862), welches eine noch höhere Korrelation mit dem MOS Wert erzielt.

Management-Tools im Voice over IP Umfeld

Einige Simulatoren sind verfügbar, die erzeugten Kunstlasten benutzen jedoch im Regelfall Standard-Protokolle, also H.323 zur Signalisierung.

Beispiele sind (jeweils in alphabetischer Hersteller-Reihenfolge):
- VOIP Bulk Call Generator von Delta Information Systems
- OmterWATCH von GN Nettest
- Chariot Voice Modul von NetIQ
- Internet Simulator / VoIP Manager von Radcom
- NetAlly VoIP von Viola Networks

Beispiele für Messung der Sprachqualität sind:
- VQMon von Finisar (eigenes IP optimiertes Verfahren, kein ITU-Verfahren)
- VoIP Manager von RADcom

Monitoring Produkte sind in größerer Vielfalt auf dem Markt, z.B.
- Network Advisor von Agilent
- AppDancer / FA VOIP von AppDancer Networks
- VoIP Monitoring Manager von Avaya
- Sniffer von Network Associates
- VoIP Manager von RADcom

Ende-zu-Ende Monitoring Produkte sind dagegen nicht in großer Vielfalt vorhanden, z.B.
- Surveyor MultiQoS von Finisar
- VoIP Assessor von NetIQ
- NetAlly DART von Viola Networks

Die Tabelle zeigt eine Übersicht über verfügbare Hersteller / Produkte und ihren funktionalen Einsatzbereich.

Testszenarien

Um den Testaufwand in angemessenen Grenzen zu halten, ist es sinnvoll, Anzahl und Detaillierung der Tests im Vorfeld festzulegen und abzugrenzen. Hierzu gehört die Spezifizierung des benötigten Testequipments, auch unter der Zielsetzung, das Equipment und die ggf. dafür benötigte Mietzeit zu minimieren. Mit einer optimierten Reihenfolge verschiedener Tests lässt sich der Zeitaufwand minimieren.

Die Definition der Tests wird an den gewünschten Ergebnissen ausgerichtet werden. Zu testen sind z.B.:
- Dauer des Verbindungsauf- und -abbaus
- Anzahl paralleler Gespräche, die unterstüzt werden
- Sprachqualität während der Gespräche (d.h. ggf. Delay, Jitter, Verlustrate)
- Einfluss von Silence Suppression auf die Qualität
- Einfluss von Tageszeit und Wochentag auf die Qualität
- Einfluss anderer Anwendungen auf die Qualität
- Einfluss von Sprache auf andere Anwendungen
- Einfluss von Quality of Service Verfahren auf die Qualität
- Kompatibilität zu vorhandenen Herstellern / Produkten
- Erweiterbarkeit und Skalierbarkeit

Tabelle: Hersteller und Tools für Voice Monitoring

Hersteller	Produkt	SM	M	EEM	K
Agilent	Network Advisor		x		
Appdancer Networks	AppDancer		x		
	FA / VoIP		x		
Avaya	VoIP Monitoring Manager		x		
Delta Information Systems	VoIP Bulk Call Generator				x
Finisar	Surveyor MultiQoS	x		x	
GN	Nettest InterWATCH				x
NetAlly	VoIP				
NetIQ	Chariot Voice Modul				
Network Associates	Sniffer		x		
RADcom	VoIP Manager	x	x		x
Viola Networks	NetAlly DART				

SM = Speech Measurement, M = Monitoring, EEM = Ende-Ende Monitoring, K = Kunstlast

Voice-over-IP Management

Basis-Überwachung

Wichtige Parameter, die beim Betrieb von IP Telefonie überwacht werden sollten, sind z.B.

- Grundlast an Sprachverkehr
- Datenanteil des Sprachverkehrs: RTP Streams mit geraden Portnummern
- Kontrollanteil des Sprachverkehrs: RTCP Streams mit den ungeraden Portnummern, die neben den genutzten geraden Portnummern der Daten-Streams liegen
- Benötigte Zeit für den Verbindungsaufbau
- Maximale Verbindungsaufbau-Rate: Wie viele Verbindungsaufbauten pro Sekunde können Netzwerk und die TK-Komponenten erstens maximal, zweitens ohne Leistungseinbußen leisten?
- Verbindungsrate: Wie viele erfolgreiche Verbindungs-Aufbauten finden statt im Verhältnis zu den Verbindungsversuchen
- Grundlast an "normalem" Datenverkehr
- Grundlast an priorisiertem Datenverkehr, soweit Priorisierung eingesetzt wird
- Funktions- und Leistungstests, insbesondere bei erweitertem Dienstumfang (Leistungsmerkmalen)
  – Fax Gruppe 3: Pass Through oder native
  – Voice Mail
  – E-Mail
  – Unified Messaging
  – Computer Telefonie Integration

Bei allen Tests, bei denen Protokoll-Anlayse erforderlich ist, wird die Analyse vielfach maximal bis zur RTP bzw. RTCP Ebene gehen, da mit Ausnahme des Cisco-Protokolls SCCP die herstellereigenen Signalisierungsprotokolle nicht offengelegt sind und somit in den Analyse-Geräten auch nicht unterstützt werden.

Erfahrungswerte für Monitoring-Tests, insbesondere bei Störfall-Diagnose

Legen Sie den Fokus auf Ende-zu-Ende Ergebnisse: testen Sie zuerst stets gegen einen Client, d.h. Hardphone, Softphone oder gegen TK- / Anwendungsserver. Testen Sie im zweiten Schritt gegen Gateways, da hier aufgrund der Terminierung von Mediastreams oder Signalisierungsprozessen Engpässe auftreten können. Testen Sie erst im dritten Schritt gegen Router oder Switches, da diese nicht an den Endpunkten einer Netzverbindung liegen. Falls sich herausstellt, dass einzelne Netzkomponenten näher untersucht werden müssen, weil der Leistungsengpass nachweislich im Netzwerk liegt, testen Sie Netzkomponenten zuerst an den Punkten, wo das Netzdesign, die gemessene Auslastung oder die Systemauslegung der Komponenten Leistungsengpässe vermuten lässt. Hierbei gilt das Prinzip "der Schein trügt": Überprüfen Sie vermutete Bottlenecks jedenfalls nochmals durch einen kontrolliert gesteuerten Leistungstest. Isolieren Sie Leistungsengpässe, die nicht genau geklärt sind, mittels Eingrenzung nach dem "Hop by Hop" Prinzip.

Überprüfen Sie bei Leistungsengpässen grundsätzlich die nachfolgend genannten häufigen Fehlerursachen:

- Überlastung von CPU's und Hauptspeicher bei TK-Servern und TK-Anwendungs-Servern
- Überlastung von CPU's und Hauptspeicher; offene Prozesse von Gateways
- MTU Konflikte
- hdx / fdx Konflikte
- Seiteneffekte durch Parallelbetrieb vieler Anwendungen
- langsame NIC's
- langsame Router
- fehlerhafte Raten-Limitierung aufgrund von falsch konfigurierten QoS-Profilen
- WAN-Verbindungen mit hohem Delay

Für Beispiele zur Definition von Messpunkten wird auf den Netzwerk Insider Artikel "Netzwerkmanagement-Lösungen 2003" vom April 2003 verwiesen.

Fazit: Teillösungen sind vorhanden

Der Markt verfügbarer Produkte für Monitoring und Analysefunktionen im Telefonie-Umfeld ist in den letzten zwei Jahren deutlich breiter geworden.

Etablierte Analysator-Produkte und erweiterte Agenten-Konzepte bieten zunehmend Funktionen für Voice-Überwachung und Tests.

Es fehlen noch Analysemöglichkeiten für proprietäre Signalisierungen.

Die Element Manager für Voice leisten lediglich Konfiguration und in wenigen Fällen darüber hinaus Basis-Monitoring.

Weiterreichende Tools für Monitoring, Reporting, SLA-Überprüfung müssen entsprechend der spezifischen Bedarfe als ergänzende Bausteine einer Management-Architektur ausgewählt werden.

Anschaffung und Betrieb von einer erweiterten Event-Konsole und SLA Tools sind nicht für jede Management-Lösung erforderlich.

Literatur:

Berger, Stephen: An Overview of eHealth for System & Applications Management, Concord, 2002

NetQos: Monitoring Application Response Time, 2001

NetQos: Cisco NetFlow or RMON2: Considerations for Enterprises, 2002

Walker, John Q., Hicks, Jeff: Evaluating Data Networks for VoIP, NetIQ, 2001

Sidi, Moshe: Readying your Network for VoIP: Get it Right the First Time, Viola Networks, April 2002

Bean, Timothy E.: Finding and Fixing VoIP Problems, Finisar, Sept. 2002

Boger, Yuval: Fine-tuning Voice over Packet services, RADCOM Ltd.

* Unseren Design- und Management-Strategien liegt eine Einteilung von Netzwerken in drei Gefahrenklassen (I, II, III) zugrunde, wie sie auch im Report "Design-Varianten Lokaler Netzwerke im Vergleich" der Technologie-Information beschrieben wird.

** Für die Datentechniker unter den Lesern: Frame bedeutet bei der Übertragung von Sprache ein digitalisiertes Sprachsample und hat nichts mit Ethernet MAC-Frames zu tun: Ein oder mehrere Sprachframes werden als Datenteil in ein RTP/UDP/IP Paket gepackt, das dann im Falle einer LAN-Verbindung auch noch einen MAC-Header erhält und so ein "MAC-Frame" wird.

Abkürzungen:

BHCA	Busy Hour Call Attempts
BHCC	Busy Hour Call Completions
CC	Call Center
CDR	Call Detail Record(ing)
CHAP	Challenge Handshake Protocol
CLI	Command Line Interface
Codec	Codierer/Decodierer
CPU	Central Processing Unit
CTI	Computer Telefonie Integration
DNS	Domain Name Service
GPS	Global Positioning System
GW	Gateway
HTTP	Hyper Text Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ITU-T	International Telecommunication Union-Telecommunication Standards
LAN	Local Area Network
MAC	Media Access Control
MeGaCo	Media Gateway Control
MGCP	Media Gateway Control Protocol
ms	Millisekunde
MTBF	Mean Time Between Failure
MTTR	Max Time to Repair
NM	Netzwerkmanagement
PAMS	Perceptual Analysis / Measurement System
PBX	Private Branch eXchange
PESQ	Perceptual Evaluation of Speech Quality
PSQM	Perceptual Speech Quality Measurement
PSTN	Public Switched Telephony Network
RADIUS	Remote Authentication Dial In User Service
RAS	Registration, Admission, Status
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource ReSerVation Setup Protocol
RTCP	Real Time Control Protocol
RTP	Real-time Protocol
RTT	Round Trip Time
SAP	Session Announcement Protocol
SCCP	Skinny Client Control Protocol
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLM	Service Level Management
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TK	Telekommunikation
UDP	User Datagram Protocol
UM	Unified Messaging
VoIP	Voice over IP
WAN	Wide Area Network
µs	Mikrosekunde

Links:

www.acterna.com
www.altaworks.com
www.appdancer.com
www.avaya.com
www.chevin.com
www.cisco.com
www.ca.com
www.concord.com
www.dirig.com
www.edge-technologies.com
www.finisar.com
www.flukenetworks.com
www.hp.com
www.jaalam.com
www.lucent.com
www.micromuse.com
www.netiq.com
www.netqos.com
www.netscout.com
www.nettest.com
www.nai.com
www.net-reality.com
www.opticom.com
www.orchestream.com
www.packeteer.com
www.peregrine.com
www.precise.com
www.productivitynet.com
www.quallaby.com
www.radcom-inc.com / www.protocols.com
www.riversoft.com
www.sitaranetworks.com
www.smarts.com
www.tavve.com
www.tivoli.com
www.violanetworks.com

Seminar zum Thema

IP-Telefonie: Projektleitfaden

Seminar

15. - 17.03.04 Düsseldorf
03. - 05.05.04 Zürich
21. - 23.06.04 Berlin

Dieses Seminar erarbeitet einen Leitfaden zur Umsetzung von IP-Telefonie in der Praxis. Alternativen werden verglichen, bekannte Probleme aufgezeigt, erfolgreiche Konzepte vermittelt.

Referent: Dr. Behrooz Moayeri (ComConsult Beratung und Planung)
Preis: € 1.690,-- zzgl. MwSt.

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

CCNE

ComConsult Certified Network Engineer

Lokale Netze
- 19.04. - 23.04.04 Aachen
- 14.06. - 18.06.04 Aachen

TCP/IP und SNMP
- 03.05. - 07.05.04 Berlin
- 05.07. - 09.07.04 Bonn

Internetworking
- 19.04. - 23.04.04 Aachen
- 21.06. - 25.06.04 Aachen

Ethernet Technologien – neuester Stand
- 08.03. - 12.03.04 Aachen
- 28.06. - 02.07.04 Aachen

Paketpreis für alle vier Seminare: € 7.780 ,-- zzgl. MwSt.
(Einzelpreise: je € 2.290,--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
- 26.04. - 30.04.04 Aachen
- 05.07. - 09.07.04 Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
- 01.03. - 05.03.04 Aachen
- 10.05. - 14.05.04 Aachen

Trouble Shooting für TCP/IP-und Windows-Umgebungen
- 29.03. - 02.04.04 Aachen
- 21.06. - 25.06.04 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
- 01.03. - 05.03.04 Köln
- 24.05. - 28.05.04 Köln

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
- 22.03. - 24.03.04 Bonn
- 28.06. - 30.06.04 Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
- 19.04. - 23.04.04 Aachen
- 19.07. - 23.07.04 Aachen

Paketpreis: € 5.330,-- zzgl. MwSt.
(Einzelpreise: € 2.290,-- / € 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

Für unverlangt eingesandte Manuskripte
wird keine Haftung übernommen

Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages

© Dr. Suppan International Institute b.v.