ComConsult Research

Der Netzwerk Insider

September 2005

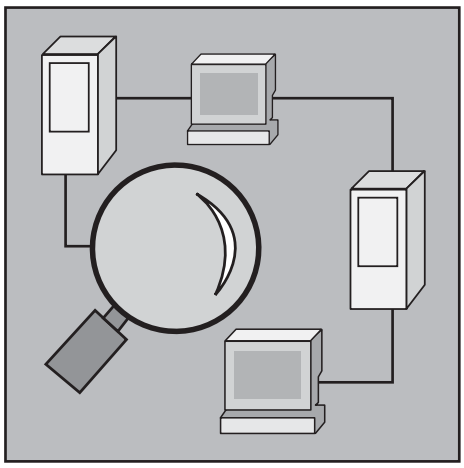
Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Neue Wege der Netzanalyse

von Dipl.-Inform. Dietlind Hübner, Dipl.-Ing. Hartmut Kell, Dr.-Ing. Joachim Wetzlar

Die „alten Hasen“ unter den Trouble-Shootern erinnern sich noch gerne an Zeiten zurück, als man einen Protokoll-Analysator irgendwo an ein Ethernet-Segment oder an einen Token-Ring anschloss, um fehlerhaft arbeitende Stationen identifizieren zu können. Dieses Universal-Messgerät war zwar teuer, half aber bei der Lösung fast beliebiger Netzprobleme. Die allgemeine Einführung der LAN-Switches und das damit verbundene Absterben der Shared-Media auf Basis von Sternkopplern, Repeatern und Ringleitungsverteilern veränderte die Welt der Messtechnik grundlegend. Der Protokoll-Analysator „erblindete“ in dem Maße, wie die Switches die Netze in mehr und mehr einzelne Segmente zertrennte. Die Hersteller haben



sich darauf eingestellt und entsprechende Messinstrumente entwickelt. Der LAN-Switch selber sammelt Daten über die an ihn angeschlossenen Segmente und meldet sie an die Messgeräte. Kleine „Handhelds“ zeigen in Sekundenschnelle die wichtigsten Parameter und geben erste Hinweise auf Fehler. Statistische Langzeitanalysen erlauben den lückenlosen Nachweis der Netzverfügbarkeit der vergangenen Monate. Die Protokollanalyse wurde verfeinert und in Richtung höherer OSI-Schichten verschoben. Der Protokoll-Analysator selbst ist zum Nulltarif im Internet „Down zu loaden“. Und die Anforderungen an den Netz-betreibenden Menschen steigen unaufhaltsam.

weiter auf Seite 21

Zweitthema

Das Internet Protocol (IP) erschließt sich neue Einsatzbereiche

von Dr.-Ing. Behrooz Moayeri

Gefahrenmanagement über IP

Die ComConsult Akademie veranstaltet im Herbst ein Forum mit dem Themenschwerpunkt Gefahrenmanagement. Die Unterstützung von Anwendungen in den Bereichen Videoüberwachung, Gebäudeleittechnik, Brandfrüherkennung und weitere Applikationen, die unter dem Oberbegriff „Gefahrenmanagement“ einzuordnen sind, rückt immer mehr in den Tätigkeitsschwerpunkt der Planer und Betreiber von Netzen auf der Basis des Internet Protocol (IP).

Gefahrenmanagement-Anwendungen sind keine klassische Domäne für IP. In mehreren Bereichen des Gefahrenmanagements haben die Nachrichten-, die Steuerungs- und die Regelungstechnik lange vor dem entscheidenden Siegeszug von IP-Netzen Lösungen realisieren müssen. Die Videoüberwachung beispielsweise arbeitete traditionell mit einer eigenen Verkabelung und eigenen Übertragungsverfahren für Videoinformation.

weiter auf Seite 11

Top Veranstaltung

Wireless LAN Forum 2005

auf Seite 4

Zum Geleit

Wireless-Switches und neue Protokolle beseitigen die Mängel der Wireless-Funktechnik

auf Seite 2

Neuerscheinung des Monats

VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

auf Seite 18

Zum Geleit

Wireless-Switches und neue Protokolle beseitigen die Mängel der Wireless-Funktechnik

Nahezu unbemerkt und erstaunlich undiskutiert vollzieht sich momentan ein Wandel der Wireless-Technik. Die massiven Mängel in der Funktechnik und im Medienzugangsverfahren werden durch Switching-Architekturen und neue Protokolle ausgeglichen. Diese Entwicklung ist vergleichbar mit dem Wechsel von Repeatern zu Switch-Systemen im traditionellen Ethernet. Für den Enterprise-Anwender steigt damit die Attraktivität der Wireless-Technik um Dimensionen. So überrascht es nicht, dass man trotz weiter fallender Preise mit einer Umsatz-Verdreifachung für die nächsten Jahre ausgeht.

Welche Mängel werden durch neue Protokolle, Architekturen und Produkte beseitigt? Im Folgenden ein kurzer Überblick über die Mängel:

- Völlig unabhängig von der verfügbaren Datenrate können Wireless-Zellen relativ leicht überlastet werden. Ein Teil des Probems ist die unklare Anzahl von Clients pro Funkzelle. Das in IEEE 802.11 festgelegte Medienzugangsverfahren stellt sich dabei als eine der größten Normungsfehlleistungen der LAN-Geschichte heraus. Es bricht unter Überlast schlicht zusammen. Selbst CSMA/CD, unser vielgescholtenes Ethernet-Medienzugangsverfahren, verhält sich unter Überlast um Lichtjahre besser

- Wireless-Netzwerke realisieren Layer-2-Netzwerke. In Kombination mit Roaming, also dem Wechsel zwischen Wireless-Funkzellen durch mobile Anwender, kann dies in einem ansonsten Layer-3-strukturierten LAN zu erheblichen Problemen führen

- Die funktechnische Beschränkung der Anzahl überschneidungsfreier Kanäle pro Zelle führt zu einem nicht zu unterschätzenden Planungsproblem. Im 2,4 GHz-Bereich mit nur 3 überschneidungsfreien Kanälen sind inzwischen die Berichte über Interferenz-Probleme aus den USA so intensiv, dass jede professionelle Planung dieses Frequenzband in Frage stellen muss. Da auch noch andere Anwendungen das 2,4 GHz-Band nutzen, kann durch diese auch ein Frequenzbereich komplett

weg fallen, so dass in der Praxis nicht drei sondern ggf. nur 2 überschneidungsfreie Bänder zur Verfügung stehen

- Eine statische Einmessung einer Wireless-Umgebung zum Zeitpunkt der Planung wird nie eine ausreichende Basis für einen dauerhaft stabilen Betrieb sein. Schon kleinste Änderungen in der Umgebung können die Funksituation drastisch verändern. Die Idee, dass eine einmal eingemessene und in ihrer Leistung optimal justierte Zelle für Jahre nicht mehr verändert werden muss, ist schlicht naiv

Betrachtet man diese Mängel, so verwundert, warum WLANs überhaupt funktionieren. Die Antwort ist trivial. Diese Mängel betreffen vorrangig Enterprise-Netze, die flächendeckend mit vielen Zellen und vielen Teilnehmern arbeiten. Für viele Kunden ist dies aber noch nicht die gegebene Situation. Allerdings geht der Trend genau in diese Richtung. Viele Kunden bereiten aktuell den flächendeckenden Einsatz von Wireless vor. Häufig geschieht dies im Zusammenhang mit strategisch wichtigen Anwendungen, zum Beispiel im Warenlogistik-Bereich.

Gerade im laufenden Trend der immer weiteren Ausdehnung des Installationsumfangs ist es deshalb wichtig und für den weiteren Erfolg von WLANs unverzichtbar, dass die bestehenden Mängel beseitigt werden. Für den Anwender ändert sich mit den neuen Entwicklungen Vieles, werden doch elementare Risiken für einen stabilen Betrieb beseitigt.

Welches sind die Wichtigsten der aktuell laufenden Entwicklungen:

- Ohne Frage ist der Übergang zu einem Wireless-Switch und der Weg weg von traditionell trivialen Access-Point-Installationen der Schritt, der den Übergang von der Konsumertechnik zur professionellen Enterprise-Technik am besten kennzeichnet. Wireless-Switches vereinen viele Vorteile:
  - Sie erleichtern die Administration und den Umgang mit einer größeren Zahl von Access-Points
  - Sie bringen adaptive Verfahren zur automatischen Abstimmung der gewählten Kanäle und Sendeleistungen unter den Access Points mit sich. Eine Wireless-Installation kann sich somit an veränderte Umgebungs- oder Bedarfssituationen leichter anpassen
  - Sie lösen das Layer-2-/Layer-3-Strukturproblem, indem sie Virtuelle Layer-2-Netze ontop auf Layer-3-Netzwerken realisieren
  - Damit schaffen sie auch zentrale Integrationspunkte und erleichtern die Umsetzung und den Betrieb von Sicherheitskonzepten erheblich

- Intelligentere Anmeldeverfahren der Clients an den Access Points können in Lastverteilungs-Algorithmen eingebunden werden. Stehen so einem Client mehrere Access-Points zur Wahl, kann die Anmeldung am lasttechnisch optimalen Access Point erfolgen

- Die Notwendigkeit eines Wechsels in den 5 GHz-Bereich ist unbestritten. Das große Problem dabei ist die Rückwärts-Kompatibilität zu 802.11b und 11g-Teilnehmern. Speziell die weiterhin hohe Zahl von 11b-Clients gerade auch bei Spezialgeräten wie Scannern erschwert jedes saubere Design. Auf den ersten Blick ist gerade dazu der 11g-Standard als Migrations- und Integrations-Stan-

dard geschaffen worden. Bei näherer Betrachtung ist das jedoch nicht haltbar, da ein 11b und 11g-Mischbetrieb die nutzbare Datenrate in der Funkzelle so weit senkt, dass von den 54 Mbit/s des g-Standards nichts übrig bleibt. Die einzig sinnvolle Lösung besteht in einer sauberen Trennung:

- 54 Mbit/s nach 11a/h im 5 GHz-Band als Standardfrequenz
- 11g/b mit den Nachteilen des Mischbetriebs für die Rückwärtskompatibilität

Problem ist, dass sich die Installation von 2 Access-Points dafür nicht rechnet. Die wichtige Neuentwicklung ist nun die Verfügbarkeit von Dual-Radio-Access-Points, die den gleichzeitigen Betrieb von 11g/b und 11a ermöglichen.

Dual-Radio-Access-Points sind der Weg in die Zukunft. In Kombination mit einem Wireless-Switch bilden sie die Basis für sichere Investitionen in Wireless-Technik

Ohne Frage hat sich Wireless-Technik mit den beschriebenen Entwicklungen massiv weiter entwickelt. Parallel konsolidieren sich die Hersteller. Die Übernahme von Chantry durch Siemens und von Airespace durch Cisco hat den Startschuss zur Marktbereinigung gegeben. Die Beteiligung von Nortel und Motorola an Trapeze und die enge Zusammenarbeit von Trapeze und D-Link gehen in die gleiche Richtung. Aruba und Alcatel begnügen sich - noch - mit einem OEM-Vertrag.

Bei allen Vorteilen und Perspektiven, die sich mit dieser Entwicklung bieten, darf die Komplexität dieser Entwicklung nicht unterschätzt werden. Eine aktuelle WLAN-Planung erfordert detailliertes Wissen über die neuen Verfahren und Produkte.

Hier setzen wir mit unserem Wireless-LAN-Forum 2005 an, unserer wichtigsten Netzwerk-Veranstaltung des zweitem Halbjahres. Das Wireless-LAN-Forum 2005 bietet Ihnen:

- Analysen der neuesten Entwicklungen
- Top-Vorträge durch Top-Experten
- Überblick über Markt und Produkte

Ihr
Dr. Jürgen Suppan
ComConsult-Research, Nelson

Top-Kongress

Wireless-LAN-Forum 2005
Jetzt noch Frühbucherphase

Wireless-LANs müssen sich in den nächsten Monaten gravierenden Neuerungen stellen:

- Mit IEEE 802.11n kommt Anfang 2006 ein neuer Wireless-Standard, mit den ersten Produkten ist zur CeBit zu rechnen. Er wird im Wesentlichen höhere Datenraten bieten und ggf. bei niedrigen Datenraten die Reichweiten erhöhen
- Mit IEEE 802.16 kommt eine völlig neue Wireless-Technologie, die über eine sehr hochwertige Funktechnik und vor allem eine Maschentopologie verfügen wird. Auf dieser Basis wird der Aufbau redundanter Wireless-Backbone-Strukturen möglich
- Mit dem Kauf von Airespace hat CISCO Systems eine neue Welle der Wireless-Technik ausgelöst. In den USA prägen Wireless-Switches mittlerweile den Kern der Wireless-Enterprise-Technologie. Wireless-Switches lösen signifikante Probleme der bisherigen Technologie, sie sind aber nur für bestimmte Anwendungsbereiche sinnvoll
- Nachdem die Interferenzen im 2,4 GHz-Band immer mehr zunehmen und auch bereits die ersten Konsumer-Produkte in das 5 GHz-Band wechseln, steht nun auch dem Enterprise-Markt dieser Wechsel bevor. Dominierte dieses Frequenzband hier bisher vor allem in Outdoor- bzw. Backbone-Anwendungsbereichen, so wird es zunehmend den Standard in WLAN-Enterprise-Netzwerken prägen
- Voice over Wireless wird Standard werden. Mit der Einführung von IP-Telefonie wird man einen Ersatz für die bisherigen DECT-Installationen suchen. Damit entstehen neue Herausforderungen, da ein wirklich mobiles Endgerät ins Spiel kommt
- WirelessLANs haben sich zur Mega-Technik im Logistik-Bereich entwickelt. Sei es als Infrastruktur für RFID-Anwendungen oder als Kommunikations-Infrastruktur für Transport-Steuerungen aller Art. Damit halten sie Einzug in den Produktionsbereich. In den letzten Monaten hat sich gerade hier eine sehr hohe Eigendynamik entwickelt
- IEEE 802.11i hat die bestehenden Sicherheits-Probleme gelöst und schafft die Voraussetzungen für eine hochwertige Sicherheits-Infrastruktur, die WLANs zu den sichersten Netzen überhaupt machen

Angesichts dieser doch erheblichen Veränderungen der Wireless-Technologie stellen sich mindestens folgende Fragen:

- Sind Investitionen in Wireless LANs gerade unter dem Blickwinkel der anstehenden Änderungen sicher? Lohnt es sich, auf 802.11n zu warten?
- Ist die IEEE 802.16-Client-Variante, mit der frühestens in 18 Monaten zu rechnen ist, mit der Einführung von 11n bereits vor ihrer Geburt gestorben? Lohnt sich das Warten auf 802.16-Backbone-Strukturen oder bietet 802.11a/h in Verbindung mit zusätzlichen Redundanzen hier bereits eine ausreichende Leistung?
- Wie stabil ist die Hersteller-Landschaft? Gerade die traditionellen Netzwerk-Hersteller haben sich im Bereich Wireless in den letzten 2 Jahren nicht gerade mit Ruhm bekleckert und diverse Investitionsruinen hinterlassen. Der Wechsel auf Wireless-Switches führt u.a. dazu, dass bei einzelnen Herstellern ganze Produktserien aussortiert werden. Auf welchen Hersteller sollte man setzen? Bieten spezialisierte Hersteller hier eine höhere Leistung, Stabilität und vor allem Investitionssicherheit?
- Wie lange wird 802.11n gültig sein, was kommt danach? Braucht man vor allem mehr als 11n leistet?
- Wie kann eine sinnvolle Langzeitmigrations-Strategie aussehen?
- Werden Wireless-Switches generell die traditionellen Access-Point-Strukturen ablösen? Wie sehen sinnvolle Migrationswege aus?
- Wie weit wird die Einführung von WLANs in den Produktionsbereich gehen? Sind sie wirklich tauglich für diesen Bereich? Welche Sonderfunktionen wird dies erfordern?
- Sind die Anwender wirklich bereit, die in 802.11i festgelegte Infrastruktur aufzubauen oder bleiben sie bei mehr oder weniger angreifbaren Einfach-Lösungen?

Auf diese Fragen geht das Wireless LAN Forum 2005 ein. Das detaillierte Programm finden Sie auf den folgenden Seiten.
Ein herausragendes Programm, hochaktuelle Themen, Top-Referenten und spannende Diskussionen erwarten Sie.

Zögern Sie nicht, sich rechtzeitig einen Platz auf dieser herausragenden Veranstaltung zu sichern! Die Frühbucherphase läuft nur noch bis zum 15. September.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Wireless-LAN-Forum 2005

☐ Ich buche den Kongress
Wireless-LAN-Forum 2005
vom 21.11. - 23.11.05 in Königswinter
zum Preis von € 1.430,- zzgl. MwSt.*
(*gültig bis 15.09.05)
regulärer Preis € 1.690,- zzgl. MwSt.

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Programmübersicht: Wireless LAN Forum 2005

Montag, den 21.11.2005

9:30 - 10:45 Uhr und 11:15 - 12:30 Uhr
Neue WLAN-Technologien in der Analyse: wohin wird die weitere Entwicklung gehen

- IEEE 802.11: aktuelle Entwicklungen und die Zukunft
  - Kampf um IEEE 802.1n: Konsumer kontra Enterprise, wer gewinnt?
  - IEEE 802.11n: der neue Standard in der Analyse
  - Wie arbeitet er
  - Können die bisherigen Schwachstellen beseitigt werden
  - Reichweite, Datenraten, Stabilität
  - Was kommt nach 11n: Ausblick auf zukünftige Wireless-Potenziale
- Was machen die Chip-Hersteller
  - Atheros und der Einfluss auf die Access-Point-Technologie
  - Airgo und die Bedeutung neuer Standards, oder: wer außer Airgo kann 802.11n rechtzeitig liefern
  - Broadcom: vom Wireless-Client zur Switch-Integration, in welchem Umfang wird Wireless-Switching in Zukunft eine Standard-Eigenschaft von Switch-Systemen sein
  - Intel: der Client bestimmt die WLAN-Technologie, welchen Einfluss kann Intel auf die zukünftige Wireless-Entwicklung durch seine starke Position im Notebook-Markt nehmen?
- IEEE 802.15 und IEEE 802.16: die Wireless-Revolution
  - Technische Hintergründe
  - Schlüsselfrage Client-Integration
  - Zusammenspiel mit 802.11: Aufbau einer Wireless-Hierarchie
  - Zeitachse und Ausblick
- Fazit: Empfehlungen für zukünftige Investitionen auf der Basis der beschriebenen Entwicklungen

Dr. F.-J. Kauffels, Unternehmensberater

14:00 - 15:30 Uhr
Netzwerk-Design 2005 und Integration von Wireless-LANs

- Bewertungskriterien für ein bestehendes Netzwerk-Design
- Neue Ansätze im Campus-Design
- Neue Verfahren im Tertiär-Bereich zur Optimierung von Konvergenz-Zeiten
- Integrations-Alternativen für WLAN-Netzwerke
  - Einzel-Zellen
  - Mehrzellen-Installationen
  - Sonderfall Wireless-Switches
- Die Rolle des Sicherheits-Konzepts
- Voice-ready und Quality-of-Service: was ändert sich durch WLANs?
- Integrierte Redundanz-Lösungen für Kabel-LAN und WLAN
- Benutzertrennung im Netzwerk: Konzepte und Nutzbarkeit
- Resultierende Design-Alternativen und ihre Nutzbarkeit
- Beispiele

Dipl.-Inform. Petra Borowka, UBN

16:00 - 17:30 Uhr
Switch-basierte WLAN-Architekturen kontra traditionelle Lösungen: wohin geht der Markt und wie verändert sich WLAN-Design?

- Konzepte der Hersteller (Cisco, Trapeze, Chantry, Aruba) im Vergleich
- Wie arbeiten die verschiedenen Lösungen, was leisten sie?
- Kommt der universelle Access-Point, der sich nur noch in der Software unterscheidet?
- Welches Control-und Provisioning-Protokoll für APs wird sich durchsetzen?
- Die IETF-CAPWAP-Norm: Architekturen und Protokolle
- Leightweight Access Point Protocol LWAPP vs. CAPWAP Tunneling Protocol
- Wo stehen andere Ansätze wie SLAPP, was wird Chantry machen?
- Wie offen werden diese Lösungen wirklich sein?
- Integration im Switch: wird Wireless-Switching in Zukunft ein Standard-Element jedes normalen Switches sein?
- Layer-3-Roaming, Trouble Shooting, Redundanzkonzepte
- Das virtuelle Distribution System als Standard-WLAN-Design
- Management von WLANs aus der Perspektive von Wireless-Switches
- Empfehlungen aus laufenden Projekten

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:45 - 11:15 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

Dienstag, den 22.11.2005 - vormittag

9:00 - 9:45 Uhr
Der Wechsel ins 5 GHz-Band: erfordern Interferenzen den Wechsel ins 5 GHz-Band für einen sicheren und stabilen Betrieb und wie werden 11b-Geräte integriert

- Gefahren im 2,4 GHz-Band
- Betriebs-Herausforderung: Erkennung von Interferenz-Problemen
- Merkmale einer 5 GHz-Lösung
- Ausleuchtung, Stabilität und Planung in der Analyse
- 11a kontra 11h: was 11h wirklich leistet, WiFi-Zertifizierung
- DFS und TPC und die Konsequenzen
- Sendeleistungen und Kanalwahl
- Reichweiten in Abhängigkeit von der Sendeleistung
- 5 GHz als Outdoor-Bridging: Nutzung der hohen Sendeleistungen
- Einbindung von 11b und 11g
- Multi-Radio-Acess-Points: ist dies der Trend? Sind Investitionen in Dual-Band/ Single Radio eine Fehlinvestition?
- Werden 5 GHz-Lösungen durch ihre hohe Kanalzahl zu Array-Lösungen tendieren? Sind Array-Lösungen eine echte Alternative?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

9:45 - 10:30 Uhr
Voice over WLAN: wie Sie ihre WLAN-Lösung Voice-tauglich machen

- Warum Sie von der Existenz von Voice over WLAN in Ihrem Netz ausgehen müssen
- Eignung von WLANs für Telefonie-Anwendungen
- IEEE 802.11e und WiFi-Multimedia: Technik und Produkte
- Sinn und Grenzen von Quality of Service, Integration mit dem Kabel-LAN
- Verschärfte Anforderungen an die Zellplanung: was ist anders als im Sprach-losen WLAN
- Was Endgeräte leisten müssen
- Wie offen kann eine Lösung sein?
- Integration in die Kabel-basierte VoIP-Landschaft
- Absicherung der Sprachübertragung: was heute schon möglich ist und worauf noch gewartet werden muss

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 - 11:45 Uhr
WLANs in der Fertigung
Wireles LANs in der Produktion

- WLAN-Eignung für das Produkstionsumfeld
- Anforderungen an Access Points
- Montage in rauen Umgebungen
- Mobile Anwendungen in der Fertigung: schneller Zellwechsel und Alternativen in der Umsetzung
- Echtzeit und WLAN: wie ist das zu bewerten, wo liegen die Grenzen
- Interferenzen: wo ist damit zu rechnen, was ist zu tun
- Funk-Ausleuchtung von Industrieumgebungen: was man wissen muss
- WLAN-Verfügbarkeit und seine Grenzen
- Neue Funktionen und Einsatzgebiete mit Siemens-Produkten
- Anwendungsbeispiel, Empfehlungen

Nicolas Heise, Siemens AG

11:45 - 12:30 Uhr
Ausbau der Wireless-Technologie, wohin geht Cisco, wie sieht die Migration aus?

- Airespace und Aironet: wohin geht der Weg?
- Wie sehen zukünftige Architekturen nach Anwendungsfeldern aufgeteilt aus:
  - Notebook-Integration an ausgewählten Flächen
  - Flächendeckend, nicht mobil (handover keine Forderung) - mobil
- Integration vorhandener Produkte: was wird aus Aironet?
- Wohin geht der Weg bei Neuprodukten?
- Welchen Stellenwert werden AccessPoints mit Multi-Radio haben?
- Wie viele Radios werden kommen? Wird Cisco auch Arrays einsetzen?
- Mit welcher Sendeleistung in welchen Frequenzen wird Cisco bei 11a/h in Zukunft arbeiten?
- Was wird aus WLSM und dem vorhandenen 6500 Blade
- LWAPP und was es leistet
- Wie offen ist LWAPP, wird die Cisco-Implementierung dem RFC entsprechen?
- Was macht Cisco, wenn die CAPWAP-Normung andere Protokolle unterstützt?
- Wired-Switching und Wireless-Switching: wachsen die Welten zusammen?
- Was heißt das konkret für Cisco: kommt ein neues Blade für den 6500?
- Wird eine Implementierung auch in andere Switch-Familien erfolgen?
- Wird das für vorhandene Switches nachrüstbar sein?
- Wireless-Switching und die Integration von APs anderer Hersteller
- Location Server
  - Was leistet der Location Server?
  - Wie funktioniert die Standort-Ermittlung?
  - Wie sehen sinnvolle Anwendungs-Szenarien in Europa aus?
  - Ist es geplant, Standort-Informationen in Lastverteilungs-Algorithmen zu integrieren?
- Voice over wireless
  - Wo steht Cisco?
  - Wie sieht die Unterstützung von Clients von Drittherstellern aus?

Martyn Cooper, Cisco Systems

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause

Programmübersicht: Wireless LAN Forum 2005

Dienstag, den 22.11.2005 - nachmittag

14:00 - 14:45 Uhr
Wireless Switching und Voice over WLAN: untrennbar verbunden?
- Architektur und technische Schwerpunkte
- Migrationswege von Fat-APs zu Wireless Switches
- Voice over WLAN: was leistet Chantry?
- Gibt es Besonderheiten für HiPath-Lösungen?
- CAPWAP: wo steht Chantry?
- Offenheit der Lösung
- Wie können Access-Points anderer Hersteller integriert werden?
- Integration von Voice-Anwendungen von Drittherstellern
- Was ist mit 11a/h und Multi-Radio-Lösungen
- Wie sieht die Zukunft aus: was ist mit 11n und WiMAX?

Dirk Abel, Chantry Networks / Siemens AG

14:45 - 15:30 Uhr
Wireless Switching und Layer-3-Roaming
- Architektur und technische Schwerpunkte
- Was leistet das Planungs-Tool?
- Roaming bei Trapeze
- CAPWAP: wo steht Trapeze?
- Offenheit der Lösung
- Integration der Access Points von Drittherstellern
- Was bedeutet die Zusammenarbeit mit Nortel und Enterasys für den Markt?
- Was ist mit 11a/h und Multi-Radio-Lösungen?
- Wie sieht die Zukunft aus: was ist mit 11n und WiMAX?

N.N., Trapeze Networks

16:00 - 16:40 Uhr
Neue Technologien bei Wireless-Switches
- Data Plane kontra Control Plane: Wo liegen die Unterschiede, wo liegen die Vorteile für den Anwender?
- Ist eine stufenweise Migration von Fat APs zu Wireless-Switching denkbar? Wie können Investionen in traditionelle Wireless-Technik abgesichert werden?
- Integration von Wireless-Lösungen in eine umfassende Sicherheits-Konzeption
- Wann kommt 11n? Wie wird es integriert?

Dipl.-Ing. Markus Nispel, Enterasys Networks

16:40 - 17:15 Uhr
Podiumsdiskussion
- Verdrängen Wireless-Switches traditionelle Ansätze im Enterprise-Markt?
- Lohnen sich große Investitionen noch vor der Verfügbarkeit von 11n?
- Wie offen werden diese Lösungen sein?
- Ist CAPWAP ein toter Standard oder wird sich wirklich jemand daran halten?
- Sind Prosumer-Produkte eine Alternative?
- Ist das 2,4 GHz-Frequenzband tot, liegt die Zukunft bei 5 GHz?
- Sind Access-Points mit nur einem Radio (Dual-Band, Single Radio) eine Fehlinvestition?
- Wird Voice over WLAN die Zukunft prägen?
- Ist WLAN-Sicherheit ohne Sicherheits-Infrastruktur erreichbar?

15:30 - 16:00 Uhr Kaffeepause

Mittwoch, den 23.11.2005

9:00 - 10:15 Uhr
WLAN-Planung und Betrieb 2005: Planungs- und Betriebsansätze für eine sichere, stabile und performante WLAN-Zukunft
- Was leisten Tools für Site-Survey und Netzplanung?
- Access-Punkt basiertes Site Survey
- Monitoring der Luftschnittstelle: Fehlersituationen, Performance-Indikatoren, Messtechnik und ihre Auswirkung auf Planung und Betrieb
- Automatische Kanalzuweisung
- Dynamische Einstellung der Sendeleistung
- Last-Verteilung zwischen den Access-Points
- Management von Mobilität, Roaming und Handover
- Erkennung und Bewertung von Interferenzen im laufenden Betrieb
- Einfluss der herstellerspezifischen Lösungsansätze
- Empfehlungen aus der Praxis

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:15 - 11:00 Uhr
Fast Roaming: Wireless-Infrastrukturen für mobile Teilnehmer
- Ausgangslage: Roaming-Problematik
- Konkrete Benennung messbarer Anforderungen
- Lösungsansätze im Standard
- Lösungsansätze der Hersteller
- Sicherheit und Mobilität
- Pre-Athentication nach 802.11i
- Zentrale Verwaltung der Schlüssel-Informationen
- Roaming-Vorteile der Wireless-Switch-Technik

Dr. - Ing. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:30 - 12:30 Uhr
Anwender-/Projektbericht: Der Siemens-Konzernstandard für Wireless-LANs
- Warum Wireless-Netzwerke einen Konzernstandard erfordern
- Ausgangslage im Siemens-Konzern
- Inhalt des Konzernstandards
- Besondere Anforderungen von Produktions-Standorten
- Besondere Anforderungen von Büro-Umgebungen
- Welche Teile waren kontrovers?
- Erfahrungen in ersten Pilotprojekten
- Empfehlungen und Erfahrungen aus dem bisherigen Projektverlauf

Dipl.-Ing. Bernhard Rößler, Siemens AG

14:00 - 15:00 Uhr
WLAN-Sicherheit praxisgerecht umsetzen
- WPA, WPA2 und IEEE 802.11i
- IEEE 802.11X: Gestaltungsalternativen im Vergleich
- Infrastruktur kontra Pre-Shared-Key: warum die Infrastruktur notwendig ist
- Geräte-oder Nutzer-Identifizierung?
- Was zum Aufbau der Infrastruktur zu machen ist
- Wo denkbare Probleme liegen
- Wie Teilnehmer und deren Geräte klassifiziert und in Benutzergruppen mit separaten Rechten eingeteilt werden können
- Integration von Gästen: Risikobetrachtung und Bewertung der verfügbaren Techniken
- Integration in eine Gesamtlösung für WLAN und Kabel-LAN

Markus Schaub, ComConsult Technologie Information GmbH

15:00 - 15:45 Uhr
Neue Wireless-Technologien und Elektrosmog
- Ausgangslage
- Physikalische und dosimetrische Quantifizierung
- Neue Empfehlungen des NRPB
- Beurteilung der EU-Kommission
- Die Ergebnisse des REFLEX-Projektes
- Konsequenzen für bestehende Grenzwerte, z.B. CE-Zertifizierung
- Gesenkte Grenzwerte und ihr Verhältnis zu aktuellen WLAN-Technologien
- Verantwortungsvolle vorsorgeorientierte Planung
- Erweiterte Möglichkeiten mit neuen Technologien

Dr. F.-J. Kauffels, Unternehmensberater

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
16:00 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor!

Aktueller Herbst-Kongress

Netzwerk-, System- und Service-Management Forum 2005

Die ComConsult Akademie veranstaltet vom 07. bis 10. November 2005 das Netzwerk-, System- und Service-Management Forum 2005 in Königswinter.

Auch in diesem Jahr ist dies unser Top-Kongress mit aktuellen Informationen, Analysen, Projekterfahrungen und einer Übersicht über Markt und Produkte.

Das diesjährige Forum teilt sich auf in

- Analyse der IT- und Management-Entwicklung 2006
  - was sind die herausragenden Entwicklungen und Technologie-Trends im Bereich Netzwerk-, Server-, System-Technik
  - welche Auswirkungen haben diese Entwicklungen auf bestehenden Architekturen und Lösungen
- Änderungen und Erweiterungen bestehender Management-Lösungen
  - Welche Erweiterungen sind nötig
  - Welche neuen Funktionsbereiche bringen wirklichen einen Nutzen
  - Welche bestehenden Funktionsbereiche haben ihren Zenith überschritten

- Vermeidung von Betriebsaufwänden und Reduzierung von Kosten durch präventive Lösungen
  - E-Mail und Spam
  - Browser-Management
- Projekterfahrungen: profitieren Sie direkt von den Erfahrungen aktueller Management-Projekte
  - BusinessProcess Management
  - CMDB
  - User Help Desk
  - Identity Management
- Vertiefungstag: steigen Sie tiefer ein in ausgewählte Technologiebereiche und Themen
  - Management von Wireless Netzwerken
  - Management von IPtel-Lösungen
  - Service-Management
  - Business Process Management
  - Trouble Shooting

Auch in diesem Jahr erwartet Sie ein Top-Programm aktuellster Themen. Details können Sie aus dem Programm entnehmen. (siehe nächste Seite)

Top-Informationen mit direkter Umsetzbarkeit in der Praxis haben in den letzten Jahren dazu geführt, dass sich diese Veranstaltung zu einem herausragenden und beliebten Treffpunkt der deutschen IT- und Management-Szene entwickelt hat. Viele treue Stammkunden speziell dieser Veranstaltung belegen die hohe Qualität, Aktualität und den Bezug zur Praxis.

Zögern Sie nicht, sich rechtzeitig einen Platz zu sichern. Diese Veranstaltung war in den letzten Jahren häufig ausgebucht!

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Netzwerk-, System- und Service-Management Forum 2005

☐ Ich buche den Kongress
Netzwerk-, System- und Service-Management Forum 2005
vom 07.11. - 10.11.05 in Königswinter
zum Preis von € 1.990,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____05

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

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Programmübersicht: Netzwerk-, System- und Service-Management Forum 2005

Montag, den 7.11.2005

9:30 Uhr - 12:30 Uhr

IT- und Management-Trends 2006: IT-Technologien und Management-Architekturen im Wandel (Exklusiv-Analyse des internationalen Labors von ComConsult-Research)

- Dominante Trends auf dem Weltmarkt
- Neue Technologien 2006: welche sind relevant?
- Globalisierung und die Auswirkung auf IT-Architekturen
- Standortübergreifende Prozesse und ihre Umsetzung
- Kollaborations-Lösungen: Einfluss auf Architekturen und Betrieb
- IP-Telefonie, Multimedia-Kommunikation und der Einfluss auf IT-Architekturen
- Netzwerk-Technologien 2006
  - Sind Netzwerk-Technologien am Ende ihrer Entwicklung?
  - Konvergente Netze definieren harte Trennungs- und Schutzanforderungen
  - Neue Prozesse erfordern veränderte Netzwerk-Architekturen
  - Design-Änderungen im Core-Design
  - Wireless-Technologien und ihre Auswirkung
  - Anforderungen an Betrieb und Management
- Sicherheits-Technologien 2006:
  - Traditionelle Lösungen wie die Firewall sind zunehmend unwirksamer
  - Neue Angriffsmuster erfordern neue Konzepte
  - Das Netzwerk im Kern aller Lösungsansätze
  - Wohin geht der Weg?
- Analyse Netzwerk- und System-Management: welche Funktions-Bereiche gewinnen an Bedeutung?
  - Element-Manager in der Kritik: aufwendig und wirkungslos?
  - Stellenwert der Alarmkonsole
  - Unterstützung der aktiven Service-Prozesse im Fokus
  - Vom Betrieb zur Dienstleistung, von der Aktion zum Prozess, vom Tool zur Lösung
- Ausblick

Dr. Jürgen Suppan, ComConsult Research

14:00 Uhr - 15:30 Uhr

Analyse: die Zukunft der Netzwerk-Technologien

- 10 Gigabit auf Basis Twisted Pair
  - Arbeitsweise
  - Bedarf
  - Bewertung der Eignung bestehender Kabel-Infrastrukturen
  - Müssen aktuelle Infrastruktur-Projekte diesen Standard berücksichtigen?
- Die Wireless-Revolution
  - Die neuen Standards IEEE 802.11n, 802.15, 802.16 und 802.20
  - Was sie leisten
  - Wie daraus eine sinnvolle Architektur im Sinne einer Wireless-Hierarchie aufgebaut werden kann
  - Analyse: sind Wireless-Netzwerke gesundheitsschädlich?
- Evolution der Netzwerk-Technologien
  - Wie Netzwerke in 5 Jahren aussehen können
- Handlungs-Empfehlungen

Dr. F.-J. Kauffels, Unternehmensberater

16:00 Uhr - 17:30 Uhr

Netzwerk-Design 2006

- Bewertungskriterien für ein bestehendes Netzwerk-Design
- Aktuelle Trends im Netzwerk-Design und ihre Bewertung
  - Neue Ansätze im Campus-Design
  - Neue Verfahren zur Optimierung von Konvergenz-Zeiten im Tertiärbereich im Kurzüberblick
  - Autodiscovery von Endgeräten: IEEE 802.1AB / LLDP, LLDP-MED
- Wireless-Switching und CAPWAP: die neue Dimension von Wireless-Technologien
  - Was sind CAPWAP-Funktionen
  - Welche wesentlichen WLAN-Switching-Architekturen gibt es
  - Warum eine Grundsatzentscheidung jetzt erforderlich ist
- Integration von Wireless und Wireline
- Alternativen zur schrittweisen Integration von WLAN-Netzwerken
- Integrierte Redundanz-Lösungen für Wireline und Wireless
- Benutzertrennung im Netzwerk: Konzepte und Nutzbarkeit
- Integration von Voice: Voice-ready, was bedeutet das in der Praxis?
- Beispiele und Empfehlungen

Dipl.-Inform. Petra Borowka, UBN

11:00 - 11:30 Uhr Kaffeepause | **12:30 - 14:00 Uhr Mittagspause** | **15:30 - 16:00 Uhr Kaffeepause** | **ab 18:00 Uhr Happy Hour**

Dienstag, den 8.11.2005

9:00 Uhr - 10:00 Uhr

Business-Process-Management in der Analyse

- Was ist BSM, was leistet es, was nicht
- Für welche Projekte ist es sinnvoll
- Welche Voraussetzungen müssen erfüllt sein
- Einbindung in bestehende Lösungen
- Mit welchen Kosten ist zu rechnen
- Projekterfahrungen und Empfehlungen

Dipl.-Kfm. Martin Woyke, ComConsult Kommunikationstechnik GmbH

10:00 Uhr - 11:00 Uhr

User-Help-Desk 2006: aktuelle Trends und wichtige Erweiterungen

- Wo steht der UHD heute
- Von der technischen Betreuung zur Prozess-Einbindung
- Innovative Funktionen
- Effiziente Arbeitsoberflächen
- Integration von Service-Management, BSM
- Beispiele
- Empfehlungen

Dipl.-Ing. Stefan Rolf, ComConsult Kommunikationstechnik GmbH

11:30 Uhr - 12:30 Uhr

Configuration Management Data Base CMDB: erfolgreiche Umsetzung und Projekterfahrungen

- CMDB im Mittelpunkt aller modernen Management-Architekturen
- ITIL und CMDB: vom Leitfaden zur Lösung
- Praktische Anforderungen
- Alternativen zur Umsetzung
- Einbindung in bestehende Management-Lösungen
- Notwendigkeiten und Nutzenpotenziale
- Automatisierung als logische Folge:
  - Spezialthema Automatisierung: Generierung aus einer CMDB
  - Spezialthema Sicherheit: Zugangspflege der Netzwerk-Plattform automatisiert mit Hilfe der CMDB
  - Spezialthema Management: Konfigurationspflege der Management-Plattform auf Basis der CMDB
- Kosten und Betrieb
- Bewertung und Ausblick

Dipl.-Ing. Christian Roszak, ComConsult Kommunikationstechnik GmbH

14:00 Uhr - 15:00 Uhr

Self Defending Networks: vom passiven zum aktiven Sicherheits-Management

- Traditionelles Sicherheits-Management ist nur begrenzt erfolgreich
- Modernste Sicherheits-Technologien im Überblick
- Sicherheit im Netzwerk: der Schlüssel zum Erfolg
- Self defending network: was bedeutet das?
- Beispiele und Empfehlungen

Holger Unterbrink, Cisco-Systems

15:00 - 15:45 Uhr

Vom Service Level Management zum Business Service Management

- Herausforderungen
- Lösungs-Positionierung
- Definition BSM • BSM-Lösungen
- Vorgehensweise • Nutzen • Projektbeispiel

Arnold Schmidt, Hewlett Packard GmbH

16:15 - 17:00 Uhr

Verursachergerecht IT-Leistungsabrechnung auf der Basis von Service-Management

- Ausrichtung der IT an den Unternehmenszielen
- Modellansätze
- Activity based costing
- Sinnvolle Kennzahlen • Tool-Architektur
- Die Rolle der CMDB • Beispiel
- Fazit und Empfehlungen

Aria Naderi, BMC Deutschland GmbH

11:00 - 11:30 Uhr Kaffeepause | **12:30 - 14:00 Uhr Mittagspause** | **15:45 - 16:15 Uhr Kaffeepause**

Mittwoch, den 9.11.2005: Vertiefungs-Tag

Die Durchführung des Vertiefungs-Tages wird am Teilnehmerinteresse ausgerichtet.
Bitte wählen Sie aus den angebotenen Vertiefungsthemen drei aus.
Die Zeiten sind von 9:00 - 11:45 Uhr, von 13:00 - 15:45 Uhr und von 16:00 - 18:45 Uhr

(Detaillierte Inhalte finden siehe auf S.2)

1. **Vertiefungsthema 1: Management von Wireless-Netzwerken**
2. **Vertiefungsthema 2: Service-Management**
3. **Vertiefungsthema 3: Management von IP-Telefonie-Lösungen**
4. **Vertiefungsthema 4: Integrierte BSM-Lösung in der Live-Präsentation**
5. **Vertiefungsthema 5: Fehlersuche in konvergenten Netzwerken**
6. **Vertiefungsthema 6: Benutzer-Schulung im Umgang mit Browsern**
7. **Vertiefungsthema 7: Trennung von Benutzer-Gruppen in Netzwerken**

Donnerstag, den 10.11.2005

9:00 Uhr - 9:45 Uhr

Rechtliche Aspekte der E-Mail-Sicherheit

- Virenhaftung / Spamhaftung
- Aufbewahrungspflichten und Überwachung
- Beweisrecht • Signaturen und Verschlüsselung

Ulrich Emmert, esb Rechtsanwälte

9:45 Uhr - 10:30 Uhr

Auf dem Weg zu internationalen Standards zur Vermeidung von SPAM

- Ausgangslage: SPAM-Filter und ihre Grenzen
- Auf dem Weg zum internationalen Standard: Yahoo kontra Cisco kontra Microsoft
- Was die Lösungen leisten
- Wie hoch der Aufwand ist
- Wer sich durchsetzen wird
- Empfehlungen zur Einführung

Markus Schaub, ComConsult Technologie Information GmbH

11:00 Uhr - 11:45 Uhr

Biometrie: Stand der Technik, Nutzbarkeit oder Illusion?

- Vorstellung der heute relevanten Verfahren
- Sicherheitsgewinn durch Biometrie?
- Bewertung der eingesetzten Techniken
- Absehbare Entwicklungen im öffentlichen und industriellen Bereich

Henning Daum, Fraunhofer IGD

11:45 Uhr - 12:30 Uhr

Identity und Access-Management bei der Thyssen-Krupp AG

- Vorgeschichte
- Bedarfssituation eines verteilten Konzerns
- Identity kontra Access-Management
- Anforderungen an ein konzernweites Identity-Management
- Vorgehensweise
- Vorgehensmodell
- Status und Ergebnisse
- Projekterfahrungen und Empfehlungen

Antje Hüllinghorst, Thyssen-Krupp AG

14:00 - 14:45 Uhr

Konfiguration und Management von Browsern im Netzwerk

- Browser-Eigenschaften und Architektur: was ist „modern“?
- Aktuelle Browser im Vergleich - gibt es den besten Enterprise-Browser?
- Der Browser aus Betriebssicht: warum im Enterprise-Einsatz Browser-Management Pflicht ist (Beispiele zu modernen Browsern)
- Schlüsselfaktor Browser-Management
- Was muss konfiguriert werden
- Achtung Betriebsaufwand: zentralisiertes Management bei Browsern?!
- Moderne Browser und Patch-Management
- Der Programmierer hat gepatzt: rollback bei Browsern?
- Ausblick und Empfehlungen

Dipl.-Inform. Oliver Flüs, ComConsult Beratung und Planung GmbH

14:45 - 15:30 Uhr

Netzwerk Management 2006: VoIP-Ready

- Neue Anforderungen an Netzwerk- und System-Management durch den Einsatz von VoIP
- Welche Parameter können/müssen überwacht werden?
- Praxisgerechte Analysefunktionen für den Fehlerfall
- Leistungsbezogene Abrechnung durch Einsatz von Netflow/Sflow

Georg Kieferl, Realtech AG

Der Veranstalter behält sich Änderungen im Programm vor!

10:30 - 11:00 Uhr Kaffeepause | **12:30 - 14:00 Uhr Mittagspause** | **15:45 Ende der Veranstaltung**

Sonderveranstaltung
IP-Telefonie: Markt und Produkte in der Analyse

Vom 14. - 16. November 2005 veranstaltet die ComConsult Akademie erstmalig ihre Sonderveranstaltung „IP-Telefonie: Markt und Produkte in der Analyse“ in Aachen.

Die Auswahl eines geeigneten Produkts für IP-Telefonie ist für jedes Unternehmen nicht leicht:
- Hersteller haben ihre Strategien, Produkte und Ankündigungen mehrfach geändert
- Produkt-Architekturen sind komplex, insbesondere in redundanten Standort-übergreifenden Situationen
- Die gleiche Komplexität betrifft die Umsetzung von Sicherheits-Konzepten, die gerade bei IP-Telefonie elementar sind
- Neue Standards wie SIP verändern Produkte und ArchitekturenSDo
- Neue Funktionsbereiche wie Multipunkt-Audio und Video-Konferenzen, Kollaboration oder Präsenzbasierte Team-Funktionen erfordern die Kenntnis der zukünftigen Weiterentwicklung der Produkte

An dieser Stelle setzt diese hochaktuelle Sonderveranstaltung an, die Sie umfassend in Markt und Produkte einführt.

Erfahren Sie:
- Was IP-Telefonie-Produkte leisten
- Worauf Sie bei der Auswahl achten müssen

- Wo typische Schwachstellen und Probleme liegen
- Welche Strategien ausgewählte Hersteller verfolgen
- Welche Erfahrungen ausgewählte Anwender gemacht haben

Die Veranstaltung besteht aus folgenden Teilen:
- Einführung in das Thema
- Anlagen-Architekturen, Funktionsmerkmale, Leistungsprofile
- Ergebnisse unserer großen Marktstudie
  - o Alcatel
  - o CISCO
  - o Siemens

In der Analyse und Bewertung, wer hat die beste Lösung für IP-Telefonie
- Vorstellung unseres Request for Information
- Stellungnahme und Präsentation der Hersteller
- Ausgewählte Anwender stellen ihre Erfahrungen mit IP-Telefonie-Installationen vor
  - o Wie erfolgte die Auswahl
  - o Wie hoch war der Konfigurationsaufwand
  - o Wie aufwendig ist der Betrieb
  - o Sind Erwartungen an Kostensenkung erfüllt worden
  - o Wie zufrieden sind die Anwender
- Ergänzt wird das Programm durch Detailanalysen:
  - o Die Zukunft der Siemens-Telefonie: was leistet die HiPath 8000
  - o IP-Telefonie und Sicherheit: Lösungsansätze und Alternativen

Wie Sie sehen, eine herausragende Veranstaltung, die Sie auf keinen Fall versäumen sollten, wenn Sie sich für IP-Telefonie interessieren. Die Veranstaltung steht unter der Leitung von Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke, unter deren Leitung auch die großen Marktanalysen über Alcatel, CISCO und Siemens entstanden sind. Als Teilnehmer an der Veranstaltung können Sie diese Markt-Analysen zu einem sehr attraktiven Sonderpreis erwerben.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
IP-Telefonie:
Markt und Produkte in der Analyse

☐ Ich melde mich verbindlich an zur Sonderveranstaltung **“IP-Telefonie: Markt und Produkte in der Analyse“**
vom 14.11. - 16.11.05 in Aachen
(Preis € 1.990.-- zzgl. MwSt.)

☐ Bitte reservieren Sie für mich ein Hotelzimmer vom_____ bis_____05

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

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Programmübersicht: IP-Telefonie: Markt und Produkte in der Analyse

Montag, den 14.11.2005

10:00 bis 11:00 Uhr
Einführung: IP-Telefonie und ihre Varianten: wie funktioniert sie, welche Alternativen hat der Kunde zur Auswahl
- Die verfügbaren Standards
- Grundprinzipien und Protokolle
- Komponenten einer Lösung: VoIP Endgeräte, VoIP-Server, VoIP Gateways und ihre Netzanbindung

Dipl.-Inform. Petra Borowka, UBN

11:15 bis 12:30 Uhr
Architekturen, Einsatz-Konzepte
- Klassische TK
- Zentrale Hybrid-Anlage
- Dezentrale Hybridlösung
- Reine Soft-PBX
- Beispiel-Szenarien: Single-PBX, Filial-Situation, Teleworker; Mehrstandort-Konzepte

Dipl.-Inform. Petra Borowka, UBN

13:30 bis 14:00 Uhr
Evaluierung von VoIP Lösungen, Kriterien
- Projekterfahrungen
- Funktionale Bewertung
- Strategische Bewertung
- Total Cost Ansatz
- Evaluierungs-Bereiche: Architektur, Endgerät, TK-Server, Leistungsmerkmale, weiterführende Funktionen, Zusatzanwendungen

Dipl.-Inform. Petra Borowka, UBN

14:00 bis 15:00 Uhr
Anwendervortrag: Rollout- und Bestriebserfahrungen mit IP-Telefonie von Cisco
- Komponenten der Lösung in der Finanzverwaltung NRW
- Voraussetzungen im LAN und WAN
- Einige wesentliche Funktionen / Highlights für die Anwender
- Installations-, Konfigurations- und Rolloutprozess
- Stand des Rollouts
- Wo liegen die Probleme
- Was verursachte den meisten Aufwand
- Wie aufwändig ist der Betrieb
- Sind Erwartungen an Kostensenkung erfüllt worden

Karl-Heinz Hommen-Menz, RZF

15:15 bis 16:15 Uhr
Produkte, Strategie, Marktposition
- Alcatel
- Cisco
- Siemens

Dipl.-Inform. Petra Borowka, UBN

16:30 bis 17:30 Uhr
Report-Ergebnisse: Alcatel vs. Cisco vs. Siemens Teil 1
- Bewertungs-Kriterien
- Technische Bewertung:
  - Architektur
  - Leistungsmerkmale
  - Weiterführende Funktionen

Dipl.-Inform. Petra Borowka, UBN

11:00 - 11:15 Uhr Kaffeepause **12:30 - 13:30 Uhr Mittagspause** **15:00 - 15:15 Uhr Kaffeepause** **ab 18:00 Uhr Happy Hour**

Dienstag, den 15.11.2005

9:00 bis 10:00 Uhr
Report-Ergebnisse: Alcatel vs. Cisco vs. Siemens Teil 2
- Kostenbewertung:
  - Zwei RFI-Projekte
  - Lösungen
  - Kostenvergleich

Dipl.-Inform. Petra Borowka, UBN

10:00 bis 11:00 Uhr
Anwendervortrag: Praxiserfahrungen mit IP-Telefonie von Siemens
- Wie hoch war der Konfigurationsaufwand
- Wie aufwendig ist der Betrieb
- Sind Erwartungen an Kostensenkung erfüllt worden
- Wie zufrieden sind die Anwender

Heinz Lebeck, LTU

11:15 bis 12:30 Uhr
Produkte, Strategie, Marktposition
- Avaya
- Mitel
- Nortel

Dipl.-Inform. Petra Borowka, UBN

13:30 bis 14:45 Uhr
Zusatzanwendungen und ihre Bedeutung
- Unified Messaging / Unified Communication
- Call Center
- Kollaboration
- Einsatz-Szenarien
- Worauf ist beim Einsatz zu achten?

Dipl.-Inform. Petra Borowka, UBN

15:00 bis 15:30 Uhr
Projekt-Vorstellung des RFI
- Projektumgebung
- Anforderungen
- Mengengerüst

Dipl.-Inform. Petra Borowka, UBN

Hersteller präsentieren ihre Lösungen an einem vorgegebenen Projektbeispiel
Eingeladen sind: Alcatel, Avaya, Cisco, Mitel, Nortel, Siemens

15:45 bis 16:45 Uhr
RFI Präsentation der Alcatel-Lösung *Dr. Jörg Fischer, Alcatel*

16:45 bis 17:45 Uhr
Präsentation der Avaya-Lösung *Stefan Neumann, Avaya / Tenovis*

11:00 - 11:15 Uhr Kaffeepause **12:30 - 13:30 Uhr Mittagspause** **14:45 - 15:00 Uhr Kaffeepause**

Mittwoch, den 16.11.2005

9:00 bis 10:00 Uhr
RFI Präsentation der Cisco-Lösung *Joachim Baumann, Cisco*

10:00 bis 11:00 Uhr
RFI Präsentation der Mitel-Lösung *Eric Vocke, Mitel*

11:15 bis 12:15 Uhr
RFI Präsentation der Nortel-Lösung *Heinz Behrens, Nortel Networks*

12:15 bis 13:15 Uhr
RFI Präsentation der Siemens-Lösung *Dr. Ralf Tyras, Siemens*

14:15 bis 15:15 Uhr
SIP: Der Telefonie-Standard der Zukunft in der kritischen Analyse
- Arbeitsweise und Anlagen-Architektur
- SIP-Clients
- Softclients
  - Hardclients • Multimedia-Clients
- Funktionserweiterungen Instant Messaging und Presence
- Einsatz-Beispiele: Alcatel OTUC, Nortel MCS 5100, Siemens OpenScape
- Erfahrungen aus dem German SIP Center

Dipl.-Inform. Petra Borowka, UBN

Zusatzunterlagen
Implementierungs-Aspekte für Voice-ready Netzwerke
- Anforderungen (Delay, Verlust, Jitter)
- Netzwerk-Voraussetzungen
- Pover over Ethernet
- Voice-VLAN's ja oder nein?
- Quality of Service: Priorisierung
- Sicherheits-Überlegungen

Dipl.-Inform. Petra Borowka, UBN

11:00 - 11:15 Uhr Kaffeepause **13:15 - 14:15 Uhr Mittagspause** **15:15 Uhr Ende der Veranstaltung**

Der Veranstalter behält sich Änderungen im Programm vor!

Zweitthema

Das Internet Protocol (IP) erschließt sich neue Einsatzbereiche

Fortsetzung von Seite 1

Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

In der Gebäudeleittechnik (GLT) dominierten jahrelang speziell auf die Bedürfnisse der GLT zugeschnittene Verfahren und Protokolle. Gleiches gilt für Meldesysteme und solche für Steuerung und Regelung, deren Anforderungen an die Echtzeitfähigkeit von Netzen lange Zeit nicht von IP erfüllbar zu sein schienen und die daher mit eigenen Bussystemen und Netzen arbeiteten.

Diese Situation ändert sich. Einerseits werden die IP-Netze immer leistungsfähiger, zuverlässiger und auch preiswerter, und zum anderen müssen immer mehr Unternehmen, die bisher keine Gebäudeleittechnik, keine Videoüberwachung, kein zentrales Gefahrenmanagementsystem etc. eingesetzt haben, solche Lösungen realisieren. Da liegt sicherlich nahe, die vorhandenen Netzstrukturen und das vorhandene Know-how für diese Lösungen zu nutzen. Und der Stand der Technik für Netze besteht nun einmal aus Ethernet und IP.

Damit erschließen sich Ethernet und IP neue Einsatzbereiche. Von trivialen Lösungen wie beispielsweise Videoüberwachung mittels Webkameras mit Ethernet-Anschluss oder Ansteuerung von Türöffnern von XML-fähigen IP-Telefonen aus bis hin zu komplexen integrierten Systemen verbreiten sich immer mehr.

Auch im Bereich Gefahrenmanagement sind - ungefähr vergleichbar mit dem Bereich der Telekommunikation - viele Ideen, die jetzt mit IP-basierenden Lösungen assoziiert werden, nicht so neu. Ein zentrales und integriertes Gebäude- und Gefahrenmanagement ist schon lange die Vision von Verantwortlichen für die Planung moderner Gebäude. Was neu ist, ist die Nutzbarkeit einer universellen Netzinfrastruktur, welche die Schnittstellenproblematik zwischen verschiedenen Bereichen des Objekt- und Gefahrenmanagements ein Stück weit löst und die Integration verschiedener Gewerke erleichtert. Ansonsten werden alte Ideen neu aufgegriffen. Zum Beispiel sind dem Autor Firmen bekannt, die über ihr eigenes TK-Anlagennetz bereits seit Jahren die zentrale Überwachung der Zugänge zu Gebäuden durchführen, in denen sich kein eigener Empfangsbereich oder kein ständig besetzter Empfangsbereich befindet. Dass eine solche Überwachung in vielen Fällen auch mit einer Übermittlung des Türklingelsignals zum zentralen Überwachungsplatz und der ferngesteuerten Türöffnung gekoppelt sein muss, ist eine Selbstverständlichkeit. TK-Anlagen und an diese angeschlossene Server werden schon seit Jahren dafür genutzt. Diese Lösungen müssen nun auch in einer Umgebung funktionieren, die statt der klassischen Leistungsvermittlung das Medium IP-Netz verwendet.

Die Visionen gehen aber über solche etablierte Lösungen hinaus. Man stelle sich vor, dass die Fernüberwachung und Fernsteuerung des Gebäudezugangs mit der Aufzugssteuerung gekoppelt ist. Das heißt, man sieht vom Überwachungsplatz aus nicht nur die Person, die in das Gebäude eintreten möchte und öffnet ihr die Tür, sondern ermöglicht ihr genau den einzig möglichen Weg durch das Gebäude mit dem Aufzug bis zu einer bestimmten Etage. Dazu ist am besten ein integriertes System geeignet. Das integrierte Managementsystem muss nicht nur die Informationen der Videokameras aufnehmen und anzeigen, das Klingelsignal empfangen und bemerkbar machen sowie die Türöffnung bedienen, sondern auch den Aufzug steuern können.

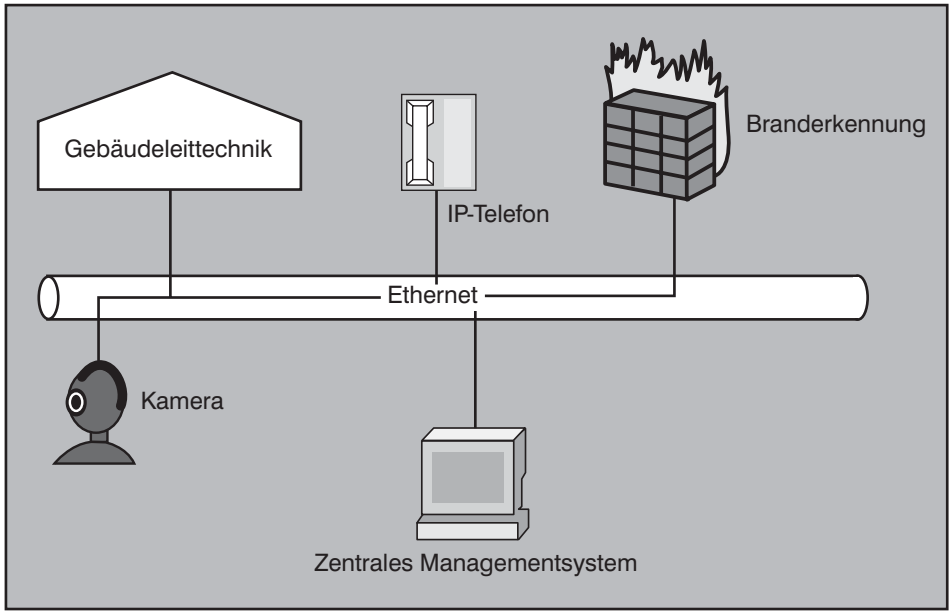


Abbildung 1: Kopplung verschiedener Systeme über Ethernet/IP

Das Internet Protocol (IP) erschließt sich neue Einsatzbereiche

Weiterhin denkbar sind integrierte Anwendungen des Gebäudemanagements in Gefahrsituationen. Üblich sind bislang Kombinationen von Maßnahmen unter Zugriff auf verschiedene Systeme. Kommt es beispielsweise zum Brand, veranlasst man einerseits durch Ansagen eine Evakuierung des Gebäudes, steuert andererseits manuell oder automatisch Brandschutztüren und Fluchttüren, nimmt Einfluss auf die Steuerung der Aufzüge, die Stromversorgung der Aufzüge etc. Denkbar sind aber auch integrierte Gefahrenmanagementsysteme, welche zum Beispiel bei einem Brand in der fünften Etage die Evakuierungsansagen zeitversetzt und der Reihe nach für die Etagen vier, drei etc. veranlassen, in Abhängigkeit von der Lage des Brandherds die Steuerung der Türen bestimmen, die Aufzüge entsprechend beeinflussen etc.

Welche Maßnahmen und in welcher Reihenfolge ein Alarm eines Bewegungsmelders in einem Bereich auslöst, könnte ebenfalls mittels eines integrierten Gefahrenmanagementsystems programmiert werden. Ist sofort die Wach- und Schließgesellschaft vor Ort zu schicken, sind zunächst andere Informationen wie die von Videokameras einzubeziehen oder sind beide Maßnahmen gleichzeitig einzuleiten - das könnten typische Einstellungen eines Gefahrenmanagements bei Verdacht auf Einbruch sein.

Planer von Rechenzentren kennen das ganze Ausmaß der Komplexität, die mit Branderkennung, Brandmeldewesen und Brandlöschung in Rechenzentren zusammenhängt. Hinzu kommen Fragen der Stromabschaltung ob und wann und mit welcher Reihenfolge und natürlich auch der Evakuierung des Rechnerraums.

Für solche Szenarien ist es erforderlich, dass alle genannten Anlagen und Gewerke miteinander kommunizieren können. Die Voraussetzung dafür schafft am besten das bereits allgegenwärtige IP-Netz.

Freilich ist eine solche omnipräsentes Kommunikationsinfrastruktur nicht die einzige Voraussetzung, die erfüllt werden muss, damit Ideen wie das dargestellte Szenario realisiert werden können. Die wichtigste Komponente ist nämlich das zentrale integrierte Managementsystem, die in Software realisiert werden muss. Eine solche Software ist hinsichtlich der Komplexität nicht zu unterschätzen. Allein wenn man bedenkt, wie komplex die modernen Aufzugssteuerungen geworden sind, wird die zusätzliche Komplexität durch Kopplung mit anderen Systemen deutlich. Für den Autor war es in diesem Jahr ein prägendes Erlebnis zu erfahren, dass in einem neuen Gebäude nicht die klassischen IT-Anwendungen und Netze und sogar nicht das neue IP-basierende Telefonsystem waren, welche die meisten Anfangsschwierigkeiten hatten, sondern die Aufzüge, und das sicherlich nicht wegen der Mechanik. In allen technischen Systemen ist mittlerweile mehr oder weniger (eher mehr) komplexe Software enthalten. Während diese IT-Lösungen (denn um nichts anderes handelt es sich dabei) bisher als entkoppelte Inseln funktioniert haben (oder manchmal auch nicht), werden sie jetzt dank Ethernet und IP gekoppelt und integriert. Dabei kommen Lösungen und Gewerke zusammen und müssen interagieren, die bislang nichts miteinander zu tun hatten.

Können sich diese Systeme und Gewerke auf das IP-Netz verlassen? Ist es nicht fahrlässig, Menschenleben Systemen anzuvertrauen, die über IP miteinander kommunizieren? Diese und ähnliche provokative Fragen müssen gestellt werden. Nur eine solche kritische Haltung stellt sicher, dass die mit IP möglichen innovativen Lösungen tatsächlich vorankommen und nicht an den - meist behebbaren - Defiziten und Problemen scheitern. Dabei sind vor allem die nachfolgend dargestellten Themenkomplexe Verfügbarkeit und Sicherheit im Zusammenhang mit IP-Netzen zu diskutieren.

Verfügbarkeit

Eine Anlage, von der die Sicherheit von Menschen, aber auch von Objekten abhängig ist, muss mindestens so zuverlässig und ausfallsicher arbeiten können wie zum Beispiel das Bremssystem eines Automobils. Sicherlich haben IP-Netze in den letzten Jahren wesentliche Fortschritte in dieser Hinsicht gemacht. Aber immer noch hört und liest man zu viele Berichte über den Ausfall von Netzen, als dass man sorgenfrei die herkömmlichen Netzstrukturen 1:1 auf Bereiche übertragen könnte, in denen ein Netzausfall nicht nur die Verfügbarkeit von herkömmlichen IT-Anwendungen beeinträchtigen könnte, sondern Gefahren wie Brandausbreitung, unbefugtes Eindringen in Gebäude und nicht aufgehende Fluchttüren entstehen lassen könnte.

Was ist zu machen, damit die erforderliche Verfügbarkeit von IP-Netzen erreicht wird? Bei der Beantwortung dieser Frage muss vor allem berücksichtigt werden, was heute die IP-Netze außer Gefecht setzt. Da ist vor allem menschliches Versagen zu nennen. Eine fatale Konfigurationsänderung, die man vornimmt, ein falsches Kabel, das man zieht, ein nicht kompatibles System, das man anschließt - wer kennt nicht solche Szenarien, die ein Netz zum Erliegen bringen?

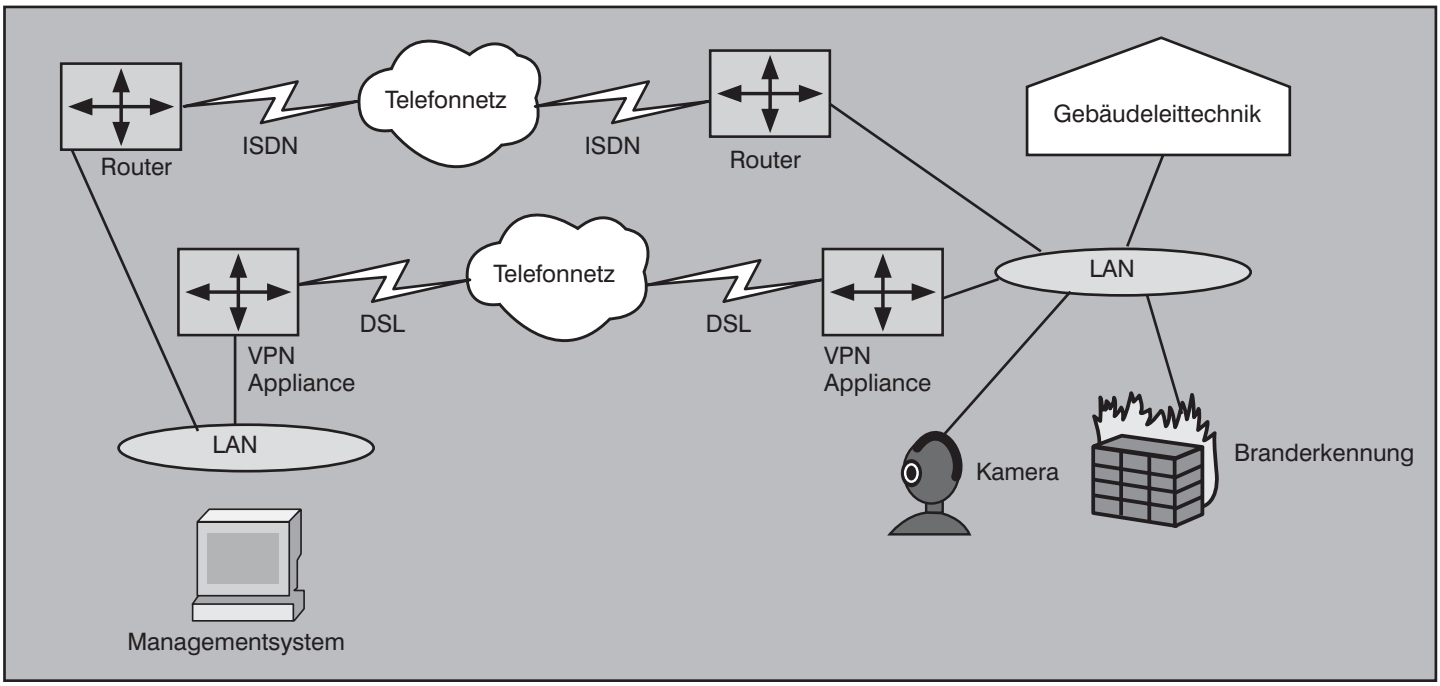


Abbildung 2: Fernsteuerung eines Gebäudes

Wie schützt man die IP-Netze vor solchen Szenarien? Nur eine Kombination von Mechanismen kann helfen. Zunächst einmal ist unnötige Funktionalität und damit Komplexität zu vermeiden. Je komplexer ein System, desto anfälliger wird es und desto größer ist die Wahrscheinlichkeit, dass bei der Bedienung Fehler passieren. Eine weitere wichtige Regel ist ein geregeltes Änderungsmanagement. Keine Änderungen durch jeden und jederzeit, sondern nur abgestimmt und qualitätsgesichert. Und dann sollte man erwägen, dass man Netzbereiche mit hohen Verfügbarkeitsanforderungen, die in der Regel keinen häufigen Änderungen unterliegen, möglichst sicher von solchen trennt, in denen ständige Änderungen unvermeidbar sind.

Solche Maßnahmen helfen auch gegen Software-Bugs, die ein Netz außer Gefecht setzen könnten. Je weniger Funktionalität aktiviert ist, desto geringer ist die Wahrscheinlichkeit von Problemen aufgrund von Softwarefehlern. Und je weniger Änderungen, umso unwahrscheinlicher solche, die einen bisher unwirksamen Softwarebug aktivieren könnten.

Nicht zu vergessen ist die Regel, nur ausreichend erprobte Systeme einzusetzen. Leider ist dies nur möglich, wenn man nach der Markteinführung von neuen Komponenten nicht gleich zu den ersten Kunden gehört, denn diese werden von den Herstellern bekanntlich als Testkunden missbraucht.

Erprobtes einsetzen, das hilft sowohl gegen Software- als auch gegen Hardware-Fehler. Letzteren kann auch dadurch entgegengewirkt werden, dass Netze redundant und ohne Single Points of Failure aufgebaut werden. Mechanismen für die automatische Umgehung nicht funktionierender Hardware binnen von Sekunden oder Sekundenbruchteilen gibt es in Netzen mittlerweile zu genüge.

Sicherheit

Die mit IP-Netzen verbundenen Risiken sind nicht nur auf die Beeinträchtigung der Verfügbarkeit aufgrund von Fehlfunktion und menschlichen Fehlern beschränkt, sondern zum Teil auch Gefahren durch bewussten Missbrauch von Netzen. So könnte ein Einbrecher oder Terrorist gezielt das IP-Netz nutzen, um das Gefahrenmanagement außer Funktion zu setzen. IP-Netze, die vom Gefahrenmanagement genutzt werden, müssen daher mindestens das Sicherheitsniveau von Kommunikationsinfrastrukturen erreichen, die bisher für solche Anwendungen genutzt werden. Starke Verschlüsselung, sichere Authentifizierung, Einschränkung der Berechtigungen auf das absolut erforderliche Minimum, Prüfung der Integrität von Nachrichten - all das sind Mechanismen, die bereits heute von IP-basierenden Systemen angeboten werden und genutzt werden können. Bereits vor zwei Jahren hat die amerikanische National Security Agency, die nicht gerade für einen sehr laschen Umgang mit Informationssicherheit bekannt ist, verkündet, dass die für Netzverschlüsselung verfügbaren Standards für den Schutz von Staatsdaten höchsten Schutzbedarfs ausreichend sind. Starke Verschlüsselung nach dem Stand der Technik ist tatsächlich stark und sicher. Was allerdings nicht bedeutet, dass es keine Sicherheitslücken in Bereichen wie Schlüsselmanagement, Fehlkonfiguration und menschliches Fehlverhalten gibt.

Aber IT-Sicherheit ist machbar. Wenn sie mit anderen Zielen wie Bequemlichkeit in Konflikt gerät, dann hilft am besten die Differenzierung zwischen verschiedenen Bereichen mit unterschiedlichen Schwerpunkten auf den genannten Zielen – womit wir wieder beim Thema Netztrennung sind. Dass Gefahrenmanagement IP-Netze nutzt, muss nicht bedeuten, dass es ein- und dasselbe IP-Netz ist, welches für Videoüberwachung und Brandmeldesysteme einerseits und E-Mail sowie Internet-Zugriff andererseits verwendet wird. IP-Netze können segmentiert werden. Ein IP-Netz kann sogar ausschließlich dem Gefahrenmanagement dienen und die verschiedenen Anwendungen im Rahmen des Gefahrenmanagements integrieren, ohne dass es eine Kopplung zu anderen IP-Netzen gibt. Das ist der sicherste Schutz auch gegen solche Szenarien wie Virenausbreitung. Diese Sicherheit kann jedoch zu anderen Anforderungen wie Offenheit in Konflikt geraten: will man jedem Mitarbeiter ermöglichen, dass er von seinem Arbeitsplatz aus die jetzt mehrfach als Beispiel angeführte Türöffnung bedie-

nen kann, braucht man zwischen dem Gebäudemanagementsystem und dem Bürokommunikationsnetz eine wie auch immer geartete Kopplung. Je sicherer diese Kopplung sein und je mehr Funktionalität sie anbieten muss, umso größer ist in der Regel der Aufwand für deren Gestaltung.

Weitere diskutierte Themen im Zusammenhang mit Gefahrenmanagement

Neben Verfügbarkeit und Sicherheit spielt eine Reihe von Themen bei der Diskussion über die Eignung von IP-Netzen für Gebäude- und Gefahrenmanagement eine Rolle. Zum Beispiel sind neben Ethernet zunehmend auch drahtlose Übertragungsverfahren wie Wireless LAN im Einsatz. Sind solche Verfahren so zuverlässig und sicher, dass sie auch für kritische Anwendungen zum Beispiel im Bereich des Gefahrenmanagements eingesetzt werden können? Auch wenn Funktechniken wie WLAN das Sicherheits- und Verfügbarkeitsniveau von drahtgebundenem Ethernet noch nicht erreicht haben, hat es in letzter Zeit wesentliche Verbesserungen in diesem Bereich gegeben. Anfällig bleiben jedoch die drahtlosen Verfahren in der Regel für bewusst herbeigeführte Störstrahlungen.

Eine weiterer Diskussionspunkt ist die Stromversorgung von Geräten, auch und gerade im Zusammenhang mit drahtlosen Geräten, aber nicht nur dafür. Ein herkömmliches Telefon und eine herkömmliche Türklingel kommen ohne dedizierte Stromkabel aus. Wie können aber Webkameras, Wireless Access Points und IP-Telefone mit Strom versorgt werden, wenn sie in Bereichen zum Einsatz kommen, in denen es keine dedizierte Stromleitung gibt? Für solche Anwendungen wurde der Standard IEEE 802.3af ausgearbeitet, der zurzeit den Bereich der bislang dominierenden Nutzung für IP-Telefonie verlässt. Der Standard an sich lässt die Stromversorgung über das Ethernet-Kabel auch im wesentlich höheren Leistungsbereich als für einfache Telefone erforderlich zu. Nun müssen aber auch Komponenten auf den Markt kommen, die zu vertretbaren Preisen den Standard auch für diesen höheren Leistungsbereich zulassen.

Im Zusammenhang mit der Netzsicherheit wurde bereits auf die Thematik der Netztrennung eingegangen. Wie die Netztrennung zum Beispiel zwischen dem Bereich der Bürokommunikation und dem Gefahrenmanagementsystem realisiert wird, ist häufig Gegenstand von Diskussionen. Reichen separate Virtuelle LAN (VLAN), um das erforderliche Sicherheitsniveau für die Kommunikationsinfrastruktur zu erreichen, die für das Gefahrenmanagement genutzt wird? Ist es vertretbar, eine einzige physikalische Infrastruktur von Anwendungen mit unterschiedlichem Schutzbedarf und unterschiedlichen Sicherheitsrichtlinien nutzen zu lassen und die Trennung lediglich auf logischer Ebene zu implementieren? Nicht nur VLAN, sondern auch Virtuelle Private Netze (VPN) verschiedenster Prägung kämen als logische Segmentierungsverfahren infrage. Wie sicher und zuverlässig sind diese Methoden? Welche Restrisiken bleiben bedingt durch die Nutzung derselben physikalischen Infrastruktur?

Im engen Zusammenhang mit dem VLAN-Thema ist die Diskussion über die Layer-2- und die Layer-3-Strukturierung von Netzen zu sehen. Soll die Kommunikationsinfrastruktur, die für das Gefahrenmanagement verwendet wird, mittels eines separaten VLAN vom restlichen Netz getrennt werden, stellt sich die Frage, wie weit sich dieses VLAN erstreckt und ob das VLAN zum Beispiel gebäudegrenzenübergreifend ist. Mit einem solchen VLAN wird die typische Layer-3-Strukturierung, welche Layer-2-Broadcastdomänen (also auch VLAN) geografisch begrenzt, aufgebrochen. Es müssen dann automatisch Layer-2-Verfahren als Redundanzmechanismen eingesetzt werden, wenn das Netz ausfallsicher aufzubauen ist.

Eine weitere im Zusammenhang mit kritischen Anwendungen häufig diskutierte Thematik ist Quality of Service (QoS). Bis-

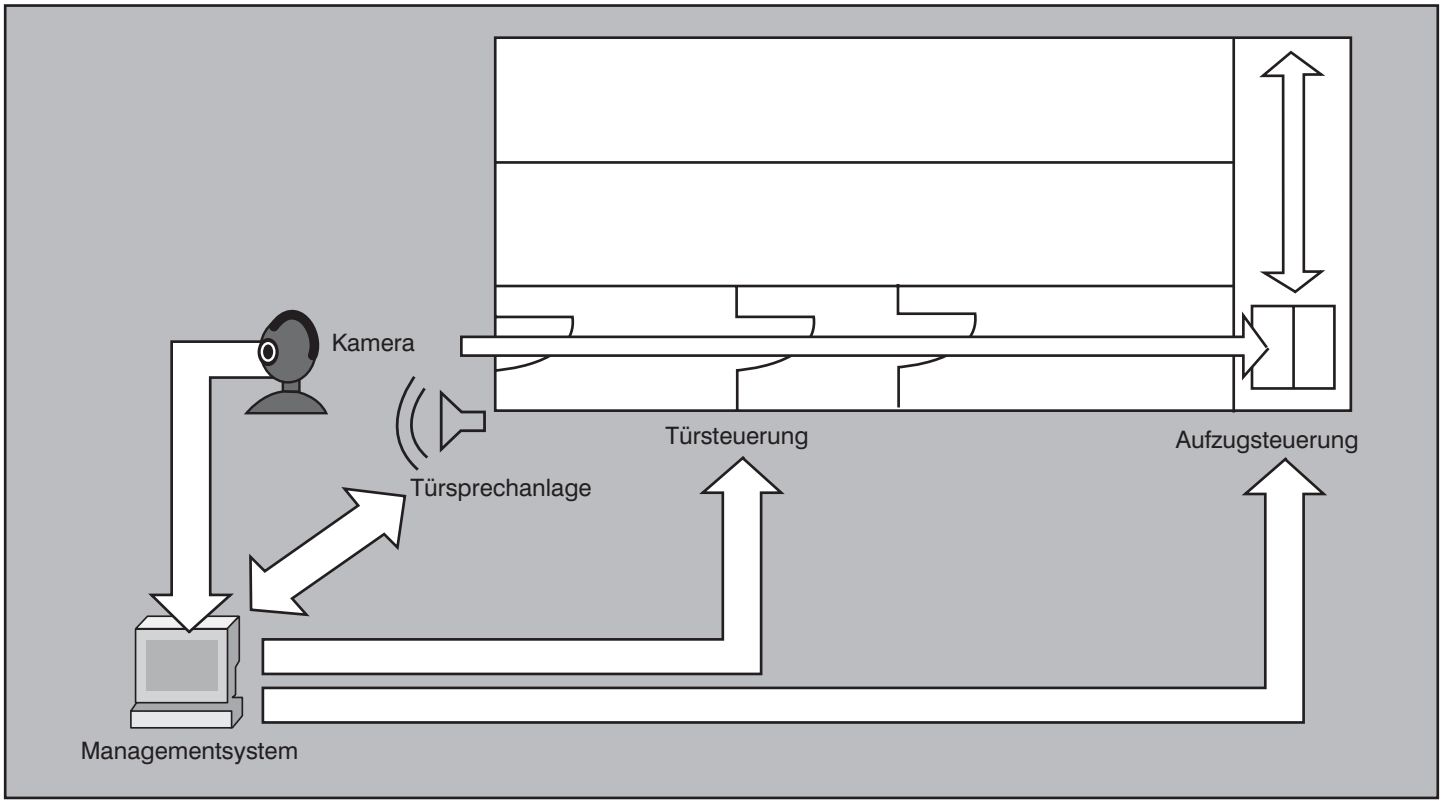


Abbildung 3: Gebäudezugangssteuerung

her differenzieren die Netze nicht zwischen verschiedenen Anwendungen oder höchstens zwischen Daten und Sprache. Jetzt kommen weitere Anwendungen wie Videoüberwachung und Gebäudeleittechnik hinzu, die wie Sprachübertragung zeitkritisch sind. Wie belastbar sind QoS-Konzepte und kann mit solchen Konzepten zwischen mehr als nur den bislang dominierenden Hauptklassen Sprache und Daten wirksam differenziert werden? Braucht man überhaupt eine differenzierte Behandlung von IP-Paketen, wenn das Netz - wie in LAN üblich - unter vertretbarem Aufwand mit einem Überangebot an Leistung arbeiten kann?

Die Gefahrenmanagementsysteme haben bislang überwiegend auf eine eigene Verkabelung aufgebaut. Die Umstellung auf IP bringt die Nutzung strukturierter Verkabelung mit sich. Zu prüfen ist auf jeden Fall, was diese Umstellung für die Anwendung Gefahrenmanagement bedeutet. Ist in allen Bereichen, die für das Gefahrenmanagement relevant sind, strukturierte Verkabelung nach den einschlägigen Normen und Standards möglich? Ist strukturierte Verkabelung in allen Kabelwegen und Trassen unterzubringen, die bisher für Anwendungen im Bereich Gefahrenmanagement eingesetzt werden?

Videoüberwachung über IP steht und fällt mit der Qualität der Bildinformationen, die mittels Kameras mit Ethernet/IP-Anschluss übertragbar sind, im Wesentlichen der Auflösung und der Zahl der pro Zeiteinheit übertragenen Bilder. Nicht zu vergessen ist der Einfluss der Lichtverhältnisse auf die Bildqualität. Kamera ist nicht gleich Kamera; hier gibt es erhebliche Qualitätsunterschiede. Eine andere Frage ist, was mit den Bildern passiert, wie und wo sie gespeichert werden, welche Datenmengen damit verbunden sind, wie eine spätere Abrufung und Auswertung ermöglicht wird.

Nicht außer Acht zu lassen sind die rechtlichen Aspekte des Gefahrenmanagements. In diesem Bereich sind noch mehr und noch striktere Gesetze, Vorschriften und Normen zu beachten als im Bereich der Telekommunikation, die ihrerseits die IP-Gemeinde mit einigen schwierigen Problemfeldern wie Notruf konfrontiert hat. Hier hat nicht nur der Gesetzgeber einen Rahmen geschaffen, in dem sich die Planer und Betreiber von Anlagen und Systemen bewegen müssen, sondern auch eine Reihe weiterer Instanzen wie beispielsweise die Versicherer. Ohne fundierte Kenntnisse dieser rechtlichen Rahmenbedingungen ist die Konzipierung von Lösungen für Gefahrenmanagement, auch Kommunikationslösungen hierfür, fahrlässig und gar nicht zulässig.

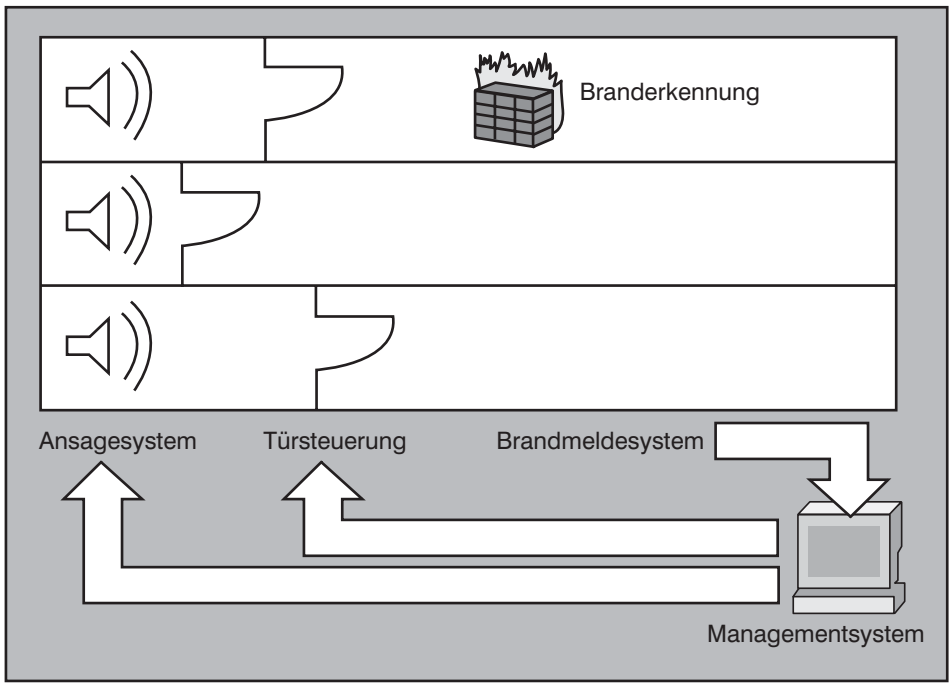


Abbildung 4: Integriertes Management im Gefahrenfall

In der nächsten Zeit werden bedingt durch die zunehmende Nutzung von IP-Netzen durch Anwendungen des Gefahrenmanagements zunehmend solche Fragen auf die Verantwortlichen für die Planung und den Betrieb von Netzen zukommen. Mit einer Reihe dieser Fragen beschäftigt sich die Veranstaltung „Gefahrenmeldetechnik und Objektüberwachung im Netz“, die vom 24. bis 25. Oktober 2005 von der ComConsult Akademie angeboten wird.

Neuer Kongress

Gefahrenmeldetechnik und Objektüberwachung im Netz Forum 2005

Die ComConsult Akademie veranstaltet vom 24. - 25. Oktober 2005 erstmalig ihren Kongress „Gefahrenmeldetechnik und Objektüberwachung im Netz“ in Bad Neuenahr.

Nachdem das IP-Protokoll den Bereich der Sprachkommunikation erfolgreich für sich gewinnen konnte und auch im industriellen Bereich nicht mehr aufzuhalten zu sein scheint, steht die nächste Eroberung an: Die Gefahrenmeldetechnik und Objektüberwachung. Dieses bisher durch klassische Analogtechniken dominierte Territorium wird im Sinne der Konvergenz moderner Netzwerke in Zukunft verstärkt von IP-basierenden Techniken beherrscht werden. Neben neuen Lösungsansätzen und der Verdeutlichung der heutigen technischen Grenzen ist eine sicherheitstechnische Bewertung dieser Techniken zwingend erforderlich.

Das ComConsult-Forum „Gefahrenmeldetechnik und Objektüberwachung im Netz 2005“ analysiert die Technologie-, Markt- und rechtliche Situation und gibt wesentliche Empfehlungen zur Einführung dieser neuen Techniken.

Im Einzelnen geht das Forum auf folgende Fragen ein:

- Was leistet eine IP-basierende Infrastruktur im Bereich der Gebäudemeldetechnik heute? Welche Akzeptanz finden diese Lösungen bei den Versicherungen oder Sachverbänden?
- Welche Grundelemente sind vorzusehen, um Überwachungs- und Meldtechnik in IP-basierenden Netzen zu implementieren? Wie sehen die Erfahrungen bei erfolgreicher Einführung dieser neuen Techniken aus?
- Sind besondere QoS-Anforderungen an moderne Datennetze zu stellen, die eine Einführung erst möglich machen?
- Was ist der aktuelle Stand der Normierung im Bereich der Brandmeldetechnik? Worin liegt die derzeit massiv geführte kontroverse Diskussion der DIN 14675 begründet? Was muss der TGA-Planer berücksichtigen und wo liegen die Zuständigkeitsgrenzen für den IT-Planer?
- Sind Wireless-Netzwerke eine Alternative im Bereich der Video-Überwachung?
- Wo liegen die qualitativen Unterschiede der verschiedenen Überwachungstechniken?
- Muss es weiterhin eine eigenständige Verkabelung für die Gefahrenmeldetechnik geben? Welche Alternative bietet eine universelle Gebäudeverkabelung basierend auf der EN 50173-1?
- Welche Anforderungen sind bei der Meldetechnik im Bereich von Rechenzentren zu stellen?
- Warum nimmt die Bedeutung von Power over Ethernet mit diesen neuen Techniken zu?

Dieses Forum bietet die ideale Basis für eine Standortbestimmung. Wer immer beabsichtigt in Gebäuden eine IP-basierende Gefahrenmeldetechnik bzw. Objektüberwachung einzuführen oder sein Netz darauf vorzubereiten, der sollte dieses Forum nicht verpassen.

Moderation: Dipl.-Ing. Hartmut Kell

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Gefahrenmeldetechnik und Objektüberwachung im Netz

☐ Ich buche den Kongress
Gefahrenmeldetechnik und Objektüberwachung im Netz
vom 24.10. - 25.10.05 in Bad Neuenahr
zum Preis von € 1.490,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____05

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

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Programmübersicht: Gefahrenmeldetechnik und Objektüberwachung im Netz 2005

Montag, den 24.10.2005

10:00 bis 11:00 Uhr
Nutzbarkeit von modernen Kommunikationsnetzen für Gefahrenmanagement
- Zentrales Managementsystem mit Integration verschiedener Gewerke (IT, TK, Haustechnik)
- Video und Zutrittskontrolltechniken auch unter Nutzung von IP - Übertragungswegen
- Praktische Beispiele
- Lösungen von morgen: Verbindungsmöglichkeiten von IP-Phones, Aufzugsteuerung, Zutrittskontrolle usw. Warum und Wie?!
- Vorschriften und Zulassungen DIN 14675, VDS

Holger Häntzschel, SSMB Service-, Sales und Managementberatungs GmbH

11:30 bis 12:15 Uhr
Nutzbarkeit von modernen Kommunikationsverkabelungen für Meldeanlagen
- Eine Verkabelung für alles?
- Nutzbare und nichtnutzbare Teilelemente der EN 50173-1
- Vor- und Nachteile der Klasse D, E und F und Glasfaser
- Produktsituation

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

12:15 bis 13:00 Uhr
Normungssituation bei Brandmeldeanlagen
- Übersicht über die derzeit gültigen Produktnormen, Planungs- und Anwendungsnormen
- Zertifizierung von Fachfirmen für Brandmeldeanlagen
- Aufschaltung von Brandmeldeanlagen auf die Empfangseinrichtungen der örtlichen Feuerwehren
- Erfahrungen beim Betrieb von Brandmeldeanlagen aus Sicht der Feuerwehr

Dipl.-Ing. Hermann Breuing, Amt für Feuer- und Katastrophenschutz der Stadt Bonn

11:00 - 11:30 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:45 - 17:15 Uhr Kaffeepause
ab 18:30 Uhr Happy Hour

14:30 bis 15:30 Uhr
Gebäudemanagement mit System
- Alarmdokumentation, Zustandsanzeigen, Brandfrüherkennungssysteme, Störmeldungen, Videobilder. Wie behält man den Überblick über die Informationsflut heutiger Gebäudemeldesysteme?
- Clevere und kostensparende Lösungen zur alltagstauglichen Integration am Beispiel bereits realisierter Lösungen
- Technik von heute: Verknüpfungen zu IT- und TK-Anlagen, Alarmierungssystemen oder Einbindung der Gebäudeleittechnik

Lothar Marth, Novar GmbH by Honeywell

15:30 bis 16:45 Uhr
WLAN-Lösungen - Video over Wireless
- Übertragungstechniken im WLAN, Abgrenzung zu anderen Funktechniken, Wireless-Lösungen im Überblick
- WLAN-Design
- WLAN-Management, Umgang mit Interferenzen und Übertragungsstörungen
- Quality of Service im WLAN, Wi-Fi Multimedia (WMM)
- Sicherheit in WLAN mit IEEE 802.11i, WPA und WPA2

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

17:15 bis 18:00 Uhr
Netzbasierende Sicherheitstechnik - Bleibt die Sicherheit auf der Strecke?
- Anforderungen der Sicherheitstechnik und Anforderungen an die Verfügbarkeit
- Sicherheitsrisiken durch IP-basierte Technologie
- Anforderungen an das Netzwerk aus der Sicht eines Sicherheitsplaners
- Einsatzmöglichkeiten und Realisierungsbeispiele
- Leistungseinschränkungen – Grenzen von Security over IP
- Ausblick: Das universelle Gefahrenmeldenetz, baldige Realität oder bleiben es zwei Welten?

Peter Loibl, TeMedia VERLAGS GmbH

Dienstag, den 25.10.2005

9:00 bis 10:30 Uhr
Moderne Architekturen konvergenter Netzwerke und die Integration von Gefahrenmeldediensten
- L2/L3-Struktur mit L3-Core
- Access-Bereich mit L2 oder L3-Technik
- Verfügbarkeits-Anforderungen von Gefahrenmeldelösungen und ihre Umsetzung im Netzwerk-Design (redundanter Access-Bereich?, Nutzbarkeit der neuen Redundanzverfahren im Access-Bereich, ...)
- Benutzertrennung
- Betrieb von Gefahrenmeldeanwendungen in Lokalen Netzwerken (Service-Definition, Service-Überwachung, Reaktion auf Service-Störungen)

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 bis 11:45 Uhr
Videoüberwachung über IP (Anforderungen, Lösungen, Grenzen)
- Motivation
- Anforderungen an die Video-Qualität, das Netz
- Welche Funktionen können implementiert werden
- Aufbau von „Video-Netzwerken“

Ralf Lange, Mobotix AG

11:45 bis 12:45 Uhr
Quality of Service
- QoS-Standards , QoS-Lösungen
- Differentiated Services (DS)
- IEEE 802.1Q, • Warteschlangenverwaltung
- Denkbare QoS-Architekturen

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause
12:45 - 14:00 Uhr Mittagspause
16:15 Ende der Veranstaltung

14:00 bis 14:45 Uhr
Sicherheitsanforderungen von Gefahrenmeldelösungen in Lokalen Netzwerken und ihre Umsetzung
- Bedrohungen im LAN und Auswirkungen auf Gefahrenmeldesysteme
- Sicherheitsmaßnahmen für die Übertragung der Überwachungs- und Meldedaten
- Verschlüsselung und Authentifizierung: Was muss sein und was ist überhaupt sinnvoll möglich?
- Absicherung des LAN-Zugangs und Schutz der Komponenten des Gefahrenmeldesystems

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr
Nutzeranforderungen zu Gefahrenmeldesysteme im RZ
- Raumüberwachung (Einbruchmeldeanlage, Türüberwachung, Kameras, Brand / Rauch, Temperatur, rel. Luftfeuchte, Wasser)
- Infrastrukturüberwachung (Klimaanlage, Stromversorgung, USV, Notstrom)
- Professionelle Lösungen für große RZ
- Kleine Lösungen für kleine RZ und wichtige Technikräume

Mark Groten, ComConsult Beratung und Planung GmbH

15:30 bis 16:15 Uhr
PowerOverEthernet
(Stand der Normung und Nutzbarkeit für Meldeanlagen)
- Funktionsweise
- Stand der Normierung IEEE 802.3af
- Planungshinweise
- Anforderungen an die Verkabelung

Dipl. Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

Änderung im Programm und Schreib-/Druckfehler behält sich der Veranstalter vor!

Report des Monats

Neuerscheinung
VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

Der komplett überarbeitete und neu aufgelegte Technologie-Report von ComConsult Research zeigt alle wichtigen Meilensteine bei Aufbau, Organisation und Betrieb einer VPN-Lösung. Die einzelnen Bausteine typischer Installationen werden anhand praxisnaher Vorgaben bewertet und ein umfangreiches Projekt- und Konfigurationsbeispiel detailliert besprochen. Insgesamt werden Sie somit in die Lage versetzt, Ihre eigene technisch und wirtschaftlich optimale VPN-Lösung zu entwerfen, in Ihr Gesamtkonzept einzubinden und zu betreiben. Lesen Sie im Folgenden einen Ausschnitt aus dieser Studie.

1.1 IPSec und das NAT-Problem

Der heute weit verbreitete Einsatz von NAT – hervorgerufen durch die Notwendigkeit, den knappen IPv4-Adressraum optimal zu nutzen, sowie aufgrund sicherheitstechnischer Vorteile bestimmter NAT-Varianten – hat beim Einsatz von VPN-Lösungen in der Vergangenheit meist für Probleme gesorgt, die erst seit Anfang 2005 durch standardisierte Mechanismen zumindest größtenteils behoben werden können. Dieses Kapitel behandelt Ursachen und Lösungsansätze dieses NAT-Problems.

1.1.1 Das NAT-Problem

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

Authentication Header

Der Authentication Header (AH) generiert eine kryptografische Prüfsumme über den Inhalt des IPSec-Pakets in Form eines Hashwerts, zu dessen Berechnung ein geheimer symmetrischer Schlüssel erforderlich ist. Dieser Hashwert umfasst alle im Paket befindlichen Daten mit Ausnahme des AH-Prüfsummenfelds und der nicht-statischen Informationen des IP-Headers. Da der Hashwert ohne Kenntnis des Schlüssels nicht gezielt gefälscht und der

Schlüssel seinerseits aufgrund der Eigenschaften der Hash-Funktion nicht aus dem Hashwert zurückberechnet werden kann, wird jegliche Manipulation am Datenpaket bei der Verifikation der Prüfsumme aufgedeckt und ein solches Paket vom Empfänger als ungültig verworfen. Der AH dient somit dem Erhalt der Integrität der übertragenen Datenpakete.

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

ESP und NAPT/PAT

Dies allein scheint nicht weiter dramatisch, wird doch der AH in vielen Szenarien gar nicht verwendet bzw. kann meist darauf verzichtet werden, da das zweite IPSec-Protokoll, ESP, ebenfalls eine – wenn auch nicht ganz so weit reichende – Integritätsprüfung beinhaltet. Doch leider löst auch der Verzicht auf den Authentication Header das NAT-Problem nicht, denn auch ESP (Encapsulating Security Payload) verursacht Probleme im Zusammenspiel mit NAT. Ein generelles Problem sind hier gemultiplexte NAT-Kommunikationsbeziehungen.

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

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

Daher ist diese Methode nicht allgemein verwendbar; es gibt allerdings Produkte (beispielsweise von Cisco Systems), die in der Lage sind, identische SPIs auf beiden Seiten der Kommunikationsbeziehung sicherzustellen, und somit ein NAPT/PAT ermöglichen, solange die VPN-Lösung homogen bleibt.

ESP im Transport-Modus
Es bliebe somit - wenn überhaupt - nur statisches NAT, d.h. die feste Zuordnung externer zu internen Adressen - ein Ansatz, der in den meisten Fällen an zu knapp bemessenem offiziellem Adressraum scheitern dürfte. Zudem ist auch der Einsatz von statischem NAT nicht unproblematisch: Schwierigkeiten treten zumindest dann auf, wenn ESP im Transport-Modus verwendet wird (dies ist beispielsweise bei der in Windows2000/2003 integrierten IPSec-VPN-Lösung der Fall). Ursächlich hierfür ist der Prüfsummenmechanismus in TCP (teilweise auch in UDP), der neben den Source- und Destination-Ports auch die jeweiligen IP-Adressen von Sender und Empfänger berücksichtigt. Ändert ein NAT-Gerät eine IP-Adresse, so muss der TCP-Header, konkret: das Prüfsummenfeld, entsprechend angepasst werden. Ohne ESP stellt dies kein Problem dar, mit ESP jedoch sehr wohl, da das Prüfsummenfeld verschlüsselt ist. Eine Korrektur ist somit nicht möglich – sie würde von der Integritätsprüfung von ESP sofort entdeckt werden – was dazu führt, dass die Prüfsummenverifikation beim Empfänger scheitert und dieser derartige Pakete verwirft.

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

IKE
Somit bliebe also ESP im Tunnel-Modus mit statischem NAT als mögliche Verfahrensweise, die in diversen DSL-Routern im Übrigen unter der Bezeichnung „IPSec-Pass-Through“ implementiert ist. Unglücklicherweise hat jedoch auch IKE Probleme mit NAT; hierfür gibt es gleich mehrere mögliche Ursachen:

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

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

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

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

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

Die meisten Hersteller generieren einen zusätzlichen UDP-Tunnel unter Verwendung verschiedenster Portnummern; eine etwas ausgefallenere Lösung bot die (mittlerweile strategisch durch die XSR-Router ersetzte) Aurorean-VPN-Lösung der Fa. Enterasys: Hier kam eine Verkapselung in HTTPS zum Einsatz, in der Hoffnung, auf dieser Basis aus vielen Netzwerken heraus ohne Anpassung einer etwaigen Firewall per VPN kommunizieren zu können. Dieser Ansatz wird im Übrigen auch von anderen Anbietern aufgegriffen, wenn auch nicht zur Behebung der NAT-Problematik: als Beispiel sei hier der so genannte Visitor Mode der Checkpoint VPN-1 genannt.

Sonderveranstaltung

Elektrische Störungen in Datennetzen und Computer-installationen erfolgreich erkennen und beseitigen

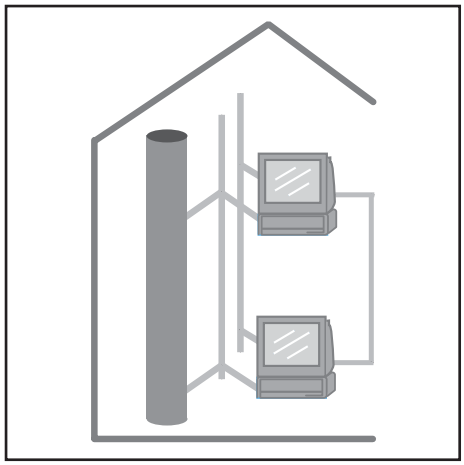
Vom 25. - 26. Oktober 2005 veranstaltet die ComConsult Akademie ihre Sonderveranstaltung „Elektrische Störungen in Datennetzen und Computerinstallationen erfolgreich erkennen und beseitigen“ in Bonn.

Sie erfahren in diesem Seminar, welche typischen Ursachen diesen Störungen zu Grunde liegen, wie gefährlich diese Störungen sind und wie sie messtechnisch erkannt und beseitigt werden können.

In den letzten Jahren lassen sich verstärkt Störungen und Schäden in Netzwerken und DV-Installationen feststellen:

- PCs und Server steigen aus
- Datennetze haben hohe Bitfehlerraten
- Auf den Schirmen von Datenkabeln lassen sich hohe Ströme nachweisen
- Switches rebooten ohne erkennbaren Grund
- Bildschirme flackern
- Festplatten zeigen erhöhte Ausfallraten

Komplexe Netzanalysegeräte, die Spannungsspitzen aufzeichnen, ergeben keine Hinweise auf den Ursprung der Störungen.



In der Sonderveranstaltung werden live beeindruckende Messungen zur Veranschaulichung der Probleme vorgeführt und es werden Videos und Fotos aus Projektsituationen gezeigt.

Die Sonderveranstaltung wendet sich an Betreiber von Datennetzen, an die Installations-Unternehmen und die betroffenen Planer.

Bringen Sie Ihren Elektromeister mit!
Es ist sinnvoll und zu empfehlen, dass Sie Ihren Werks-Elektromeister oder die Personen, die bei Ihnen für elektrische Installationen zuständig sind, mitbringen.

Unter der Leitung von Dipl.-Ing. Karl-Heinz Otto wird dieses Seminar seit 14 Jahren regelmäßig an Universitäten, beim Verband der Schadenversicherer und am Flughafen Paderborn mit großem Erfolg durchgeführt. Herr Otto ist öffentlich vereidigter und bestellter Sachverständiger für elektrische Niederspannungsanlagen, Leistungs- und EDV- Elektronik und Director vom Correct Power Institute wwww.cp-institute.de.

Gratis für Seminarteilnehmer:
Als besonderen Service im Rahmen der Thematik erhält jeder Teilnehmer ergänzend zu den regulären Seminarunterlagen bei Kursantritt kostenlos eine digitale Stromzange und das Buch aus der VDI-Schriftenreihe „Normen verständlich“: EMV-Fibel für Elektroinstallateure und Planer (16 Maßnahmen zur elektromagnetischen Verträglichkeit nach DIN VDE 0100 Teil 444: 1999-10, Autor Wilhelm Rudolph)

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Elektrische Störungen

☐ Ich melde mich zum Seminar „Elektrische Störungen in Datennetzen und Computerinstallationen erfolgreich erkennen und beseitigen“ vom 25.10. - 26.10.05 in Bonn.
zum Preis von € 1.390,- zzgl. MwSt.
die 2. teilnehmende Person
zahlt nur noch € 990,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____05

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Schwerpunktthema

Neue Wege der Netzanalyse

Fortsetzung von Seite 1

Dipl.-Inform. Dietlind Hübner ist seit mehr als 15 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 Hows und ihrer Erfahrung regelmäßig in Projekten der Netzkonzeption in Büro- und Industrieumgebungen mit.

Dr.-Ing. Joachim Wetzlar seit vielen Jahren Senior Consultant der ComConsult Beratung und Planung GmbH. Er leitet dort das Competence Center „Trouble-Shooting und Messtechnik“ und ist maßgeblich an seinem Aufbau beteiligt. Er blickt auf einen erheblichen Erfahrungsschatz mit Messgeräten und den Details der Kommunikations-Protokolle zurück. Neben seiner Tätigkeit als Trouble-Shooter führt Herr Dr. Wetzlar als Projektleiter und Senior Consultant regelmäßig Netz-Redesigns und WLAN-Planungen durch. Besucher von Seminaren und Kongressen schätzen ihn als kompetenten Referenten mit hohem Praxisbezug.

Dipl.-Ing. Hartmut Kell kann bis heute auf eine mehr als 15-jährige Berufserfahrung in Datenkommunkiation 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. Ergänzend zu diesen projektbezogenen Arbeiten vermittelt Herr Kell sein umfangreiches Fachwissen in Form von Fachpublikationen und Seminaren.

Bei aller Entwicklung hat sich das wesentliche Ziel des Netz-Betriebs bisher kaum verändert. Nach wie vor lautet das Ziel Verfügbarkeit. Netze müssen vor allem fehlerlos funktionieren. In dem Maße, wie der Computer wichtigster Produktions-bestimmender Faktor wird, müssen auch die Netze immer verlässlicher arbeiten. Die Schritte auf dem Weg dorthin sind allgemein bekannt: Redundanzen geben (meist) die ersehnte Sicherheit gegen Ausfälle von Komponenten und Leitungen. Entsprechende Protokolle wurden in den vergangenen Jahren immer weiter verfeinert, man denke nur an die allgemeine Ausbreitung von OSPF, VRRP und RSTP. Firewalls, Viren-Scanner und Intrusion-Prevention-Systeme schützen Netze vor Angriffen von innen und außen - und stellen dabei doch nur die Verfügbarkeit sicher. Die automatische und gestufte Überwachung aller Komponenten und Systeme ist heute selbstverständlich und eine Voraussetzung zur proaktiven Verfügbarkeitssicherung.

Jetzt steht uns jedoch ein wirklicher Wandel bevor: Das konvergente Netz wird allerorten zur Realität. Der Begriff bezeichnet das Zusammenwachsen bisher unabhängiger Disziplinen in einem Datennetz. So geht einerseits die Welt der Steuer- und Regelungstechnik unaufhaltsam den Weg in Richtung Ethernet, andererseits wandert die Ton- und Bildübertragung in immer mehr Bereichen von der Leitungs-vermittelten Technik zu einer Paket-vermittelten. In den Lokalen Netzen erkennen wir das am wachsenden Trend zu Voice over IP (VoIP) als Ersatz für die herkömmlichen Telefonanlagen. Aus diesem Wandel ergibt sich - neben noch höheren Anforderungen an die Verfügbarkeit – der Ruf nach Quality of Service (QoS). Netze müssen bestimmte Daten mit garantierter Güte transportieren. Diese Güte bemisst sich in den Parametern Bandbreite, Laufzeit, Varianz der Laufzeit (Jitter) und Paketverlust. Haben wir die frühen Versuche zur Verbreitung von QoS eher belächelt - ein hoher Aufwand mit fraglichem Nutzen - , so wird QoS inzwischen zu einem Merkmal moderner Datennetze.

Forderte bereits die Verfügbarkeit eine dauernde „proaktive“ Überwachung der Komponenten, gilt dies im besonderen Maße für die zusätzlichen Qualitätsparameter eines Datennetzes, das QoS zu liefern hat. Die Frage lautet, welche Messtechnik hierfür sinnvoll einzusetzen ist. Der herkömmliche SNMP-Manager ist hierfür ohne weiteres nicht geeignet. Ein Ansatz ist die Messung mit Hilfe von Simulatoren, wie Dipl.-Ing. Hartmut Kell sie im Artikel „Messung der VoIP-Tauglichkeit von Netzwerken“ im Netzwerk-Insider 05/2005 beschrieb. Hierbei werden automatisch arbeitende Agenten - die „Performance Endpoints“ - auf mehreren Endgeräten installiert, die repräsentativ im Netzwerk verteilt sind. Die Performance Endpoints simulieren den „kritischen“ Datenverkehr, das heißt eben jenen, der von einer mangelnden QoS negativ beeinflusst würde, und messen dabei fortlaufend die Qualitätsparameter. Bei diesem Verfahren handelt es sich, wie erwähnt, um eine Simulation. Eine Aussage darüber, wie einzelne Anwender durch mangelnde QoS zu bestimmten Zeitpunkten tatsächlich beein-

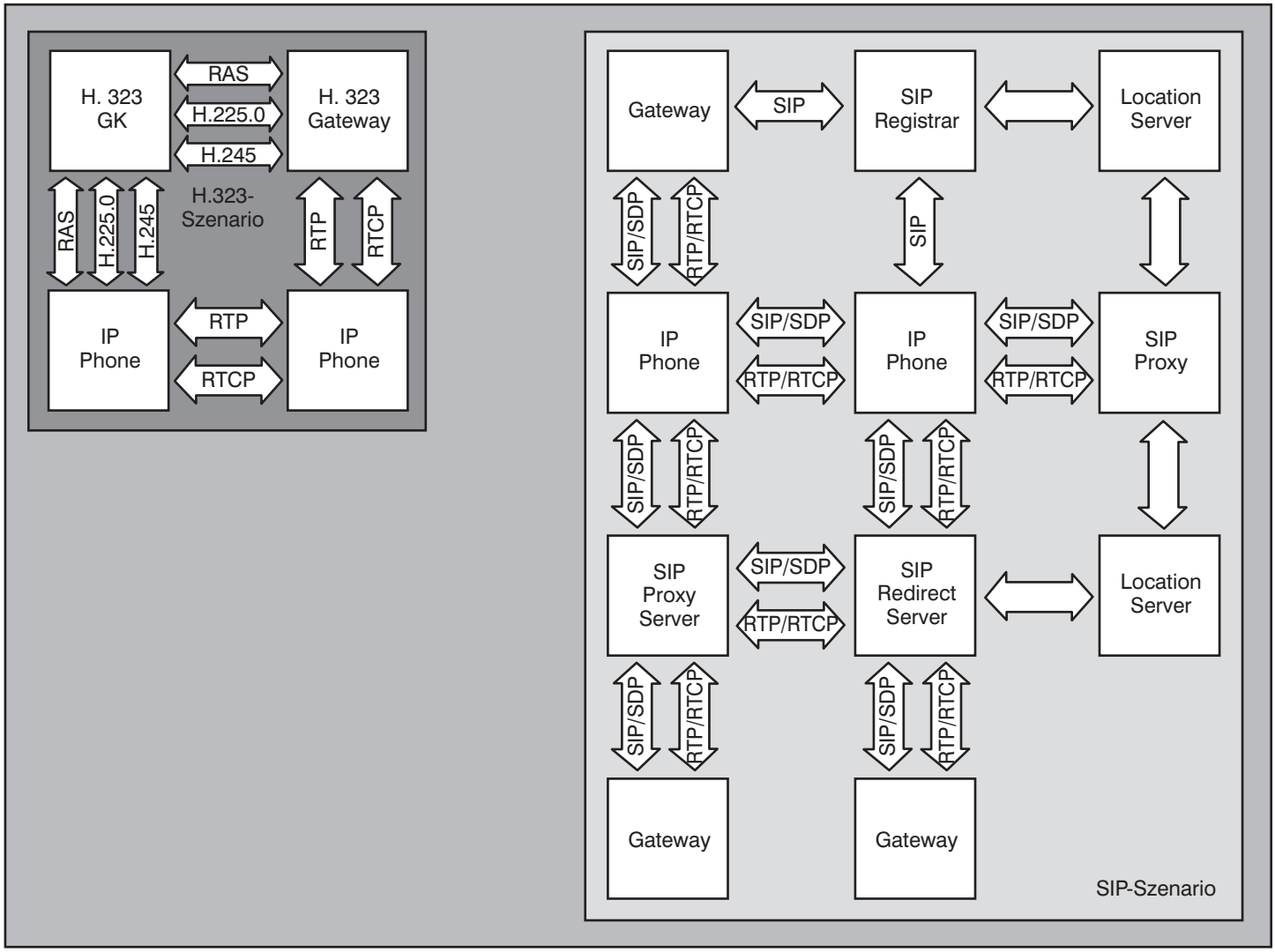


Abbildung 1: RTP/RTCP in den Welten „H.323“ und „SIP/SDP“

trächtigt wurden, ist hiermit nicht möglich. Gesucht wird also ein direktes Messverfahren für die QoS, das bestenfalls alle Transaktionen einer „kritischen“ Anwendung überwachen kann.

Dieser Artikel möchte direkte Messverfahren für die QoS am Beispiel der Telefonie mittels VoIP darstellen. Hierzu soll zunächst eine Einführung in die zu Grunde liegenden Protokolle RTP und RTCP gegeben werden, damit verständlich wird, welche Parameter sich in welcher Form überhaupt auswerten lassen.

Das Real Time Protocol (RTP)

RTP ist ein Protokoll, das für die Übertragung von „Realzeitdaten“ entwickelt wurde. Dabei ist zu beachten, dass damit nicht richtige Realtime-Daten gemeint sind - wie man es z.B. im Bereich der Produktion kennt - sondern es sind vielmehr Multimedia Daten mit Realtime-Charakteristik gemeint. Man ist den Weg gegangen, je ein Protokoll für die Echtzeitübertragung der Daten und für die Qualitätsüberwachung unterschiedlichster Multimediaanwendungen zu spezifizieren und verzichtet damit darauf, eigene Protokolle für Video- und Voice-Kommunikation zu entwickeln. Entsprechende RFC-Standardisierungen stellen sicher, dass proprietäre Implementierungen weitestgehend vermieden werden. RTP und RTCP werden als Basis beider „Welten“ der IP-Telefonie eingesetzt. Sowohl die der ITU-Empfehlung H.323 entsprechenden „Packet based multimedia communications systems“ als auch Systeme auf Basis des bei den IETF angesiedelten SIP (Session Initialisation Protocol) und SDP (Session Description Protocol) nutzen RTP und RTCP für die Übertragung von Multimedia-Daten. (siehe Abbildung 1)

Zur Nutzung von Multimedia-Anwendungen - wie Voice over IP in einem konvergenten Netz - sind neben dem Aufbau der Netzverbindung und ggf. der Reservierung benötigter Netz-Ressourcen weitere steuernde Maßnahmen erforderlich. RTP sorgt dabei für die Echtzeitdatenübertragung zwischen den Endpunkten einer Unicast- oder Multicast-Umgebung. Zu den Diensten von RTP gehören

- die Kennzeichnung der übertragenen Nutzdaten, ihrer Kodierung und ihrer Quellen,
- die Vergabe von Sequenznummern und Zeitstempeln an Datenpakete.

Die Kontrolle der zur Verfügung stehenden Dienstqualität (QoS) sowie die Übertragung von Informationen über die Teilnehmer werden nicht vom Datentransferprotokoll RTP selbst, sondern von dem zugehörigen Kontrollprotokoll RTCP (RTP Control Protocol) bereitgestellt. Dabei ist zu beachten, dass weder RTP noch RTCP für die Durchsetzung einer bestimmten Quality of Service verantwortlich ist und auch nicht

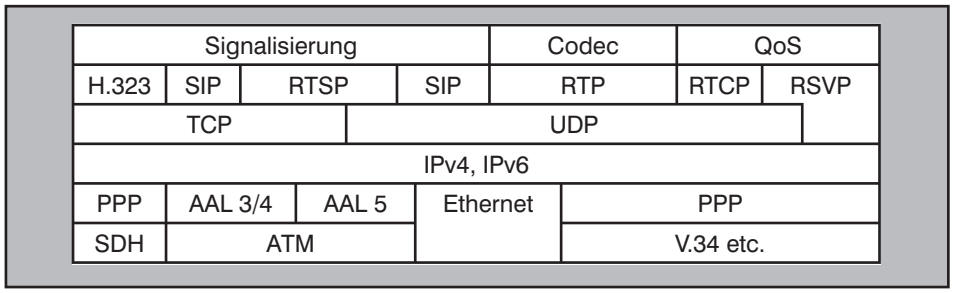


Abbildung 2: Protokoll-Einordnung RTP/RTCP

garantiert, dass Pakete in der richtigen Reihenfolge, synchron bzw. überhaupt am Empfänger eintreffen. Ersteres muss durch das Netz garantiert werden und kann z.B. durch Einsatz von RSVP (Ressource Reservation Protocol) erreicht werden, letzteres muss die Anwendung anhand der von RTP bereitgestellten Daten (Sequenznummern und Zeitstempel) selbst handhaben. RTP und RTCP müssen nicht grundsätzlich

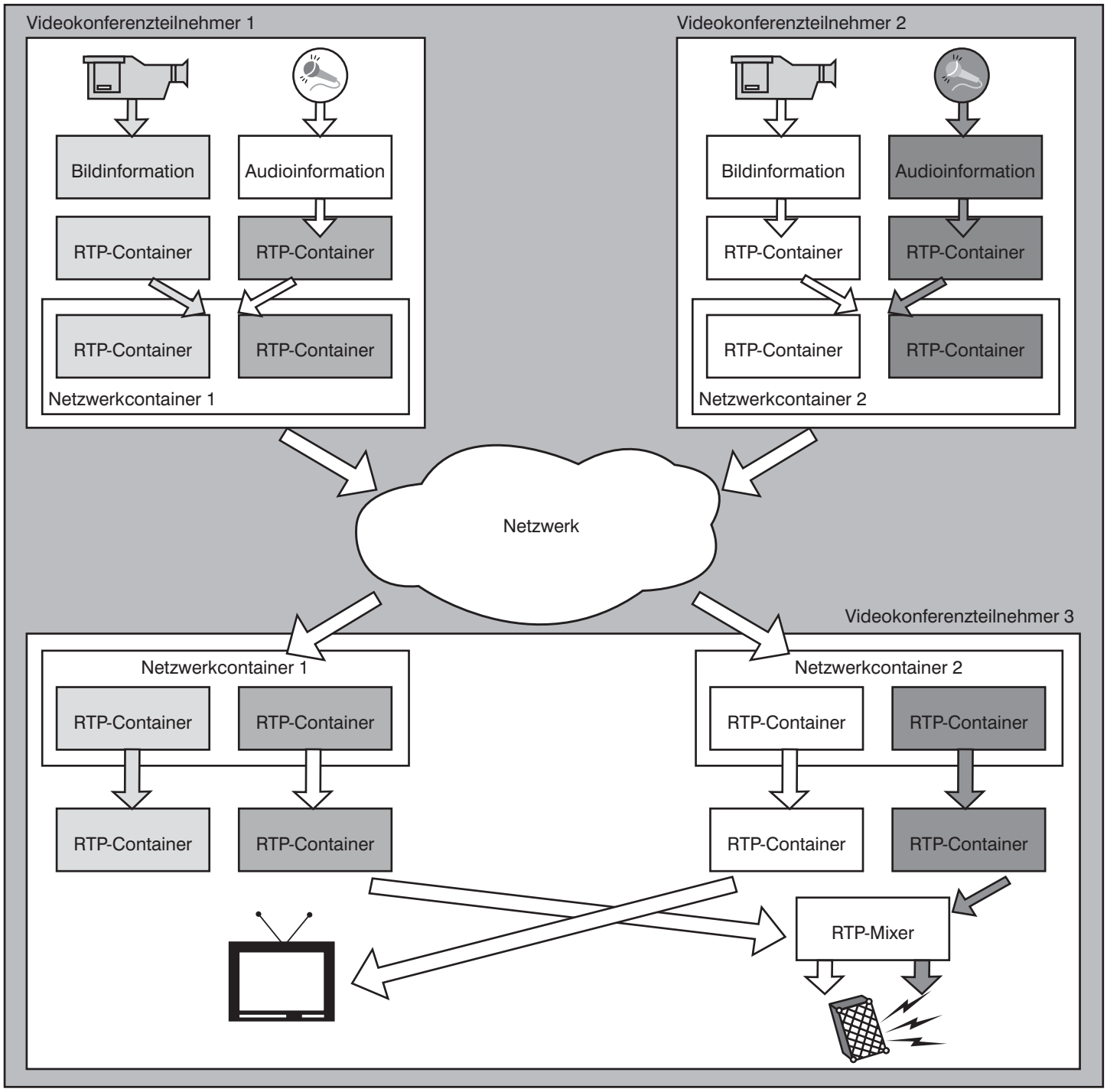


Abbildung 3: Schematische Darstellung einer Videokonferenz

kombiniert eingesetzt werden, beispielsweise könnte man eine Audio-Übertragung in einem Internet-Radio mit Hilfe von RTP realisieren, verzichtet aber auf eine Überwachung des Stromes durch RTCP.

Die Paketbildung für Voice over IP und sonstige Multimedia-Anwendungen in konvergenten Netzen ist mittlerweile umfassend standardisiert. Das dazu maßgebliche Protokoll RTP (Real-time Transport Protocol) wird bei allen VoIP-Lösungen eingesetzt. RTP wurde von der IETF (Internet Engineering Task Force) in Request for Comments (RFC) im Jahre 1996 als RFC 1889 spezifiziert und durch den RFC 3550 im Jahr 2003 als endgültiger Standard (STD0064) festgeschrieben. RTP setzt in der Regel auf UDP auf (User Datagram Protocol), ermöglicht jedoch auch die Nutzung von beliebigen anderen unterliegenden Protokollen (siehe Abbildung 2). Insbesondere bezüglich der zeitlichen Synchronisierung ist ein weiteres Protokoll zu nennen, dessen sich RTP optional bedienen kann, das Network Time Protocol (NTP), spezifiziert in RFC 1305 vom März 1992 (Draft-Standard). Dieses Protokoll verwendet eine „Uhr“ in Sekundeneinheiten, die relativ zum 1. Januar 1900 hochgezählt werden.

Protokoll-Architektur und Funktionen des RTP

Um ein Protokoll erweiterbar zu halten, wird es üblicherweise sehr allgemein spezifiziert, enthält Möglichkeiten zur Definition optionaler Felder oder ähnliche Mechanismen. Diese Flexibilität erfordert jedoch aufwendige Struktruren der Protokollheader - ein Overhead, der bei Echtzeitdaten unerwünscht ist.

Die Architektur des RTP-Protokolls unterscheidet sich daher von der anderer Protokolle: Eine Veränderung oder Erweiterung der RTP-Header zur Anpassung an bestimmte Anwendungsklassen ist ausdrücklich erlaubt. Solche Änderungen des RTP-Kerns werden in Profile Specifications definiert, die für eine bestimmte Klasse von Anwendungen gelten (z.B. Audio- und Videokonferenzen). Eine Profile Specification bildet zugleich das Bindeglied zwischen dem RTP-Kern und den Payload Format Specifications, die definieren, wie die konkreten Nutzdatenformate für ihren Transport in RTP „verpackt“ werden. RTP hat somit als Hauptaufgabe die Übertragung von Multimedia-Daten (Payload) mit Realzeit-Anforderungen, das Format und der Inhalt dieses Payload ist dagegen nicht Gegenstand des Standards.

Elementare Basis des RTP ist die Idee, dass es unterschiedliche RTP-Sessions geben wird, was je nach Anforderung der Applikation auch zu unterschiedlichen Anforderungen an die Übertragung führt. Dieser Modellansatz ist zur Realisierung einer multimedialen Übertragung notwendig und führt u.A. dazu, dass jede RTP-Session auch eine eigene RTCP-Kommunikation erfordert. Daten unterschiedlicher RTP-Sessions werden vom Sender mit unterschiedlichen Transportquelladressen an unterschiedliche Transportzieladressen geschickt. Eine Transportadresse wird aus der Kombination von IP-Adresse (eigentlich: „Netzwerkadresse“) und UDP-Port gebildet. Bei einer Applikation, die z.B. ein Fernsehprogramm überträgt, werden für Video- und Audio-Datenströme zwar die gleichen IP-Adressen, jedoch unterschiedliche UDP-Ports genutzt. Die RTP-Sessions werden sozusagen gebündelt.

Um die unterschiedlichen Sessions zu kennzeichnen werden SSRC-Identifikatoren (Synchronisation Source) verwendet, die unabhängig von den IP-Adressen sind. In einer Videokonferenzübertragung werden z.B. der Videokamera und dem Mikrofon unterschiedliche SSRC zugeordnet, beide werden sich aber möglicherweise den gleichen Netzwerkzugang teilen und damit die gleichen IP-Adressen haben. Ein weiterer Parameter ist der CSRC-Identificator (Contributing Source), dessen Funktion sich am Beispiel des Mixers verdeutlichen lässt: Bei einer Telefonkonferenz ist davon auszugehen, dass mehrere Teilnehmer gleichzeitig sprechen, und damit wird es für alle Teilnehmer ebenfalls notwendig, diese Sprachsignale gleichzeitig zu empfangen. Es muss daher eine Einheit geben, die mehrere RTP-Sessions zusammenfasst (das ist die Aufgabe des Mixers) und diese gebündelt als neues RTP-Paket mit einer neuen Absenderadresse CSRC (die des Mixers) an die Ausgabeeinheit weitergibt. (siehe Abbildung 3)

Der RFC empfiehlt, Video- und Audioübertragungen in getrennten RTP-Sessions zu übertragen; andernfalls würde z.B. der Mixer Schwierigkeiten haben bei einem eingehenden gemischten RTP-Strom eventuelle inkompatible Mediendaten mit einem anderen homogenen RTP-Strom zu kombinieren. Eine Verdeutlichung am Beispiel einer Videokonferenz: eingehende kombinierte Video/Audio-Ströme sollen über einen Mixer nur mit den anderen Audio-Strömen kombiniert werden, damit alle Teilnehmer zwar nur ein Bild von einem Teilnehmer sehen, aber alle Stimmen hören können. Bei getrennten Video- und Audio-Strömen wäre das kein Problem, bei einem gemischten RTP-Strom dagegen schon. Diese Trennung lässt sich aber auch aktiv nutzen, man denke beispielsweise daran, dass in einer Videokonferenz die Bildqualität durch mangelhafte Übertragung so schlecht wird, dass man gezielt nur noch das Audiosignal durchlässt.

Die Multimedia-Datenströme werden identisch zu anderen Applikationen als RTP-Payload in Ethernet/IP-Paketen mit entsprechend vorangestellten Headern übertragen, es ergibt sich bei IPv4 insgesamt ein Overhead für RTP/UDP/IP von 40 Byte. (s. Abb. 4)

Abbildung 5 veranschaulicht die im RTP-Header enthaltenen Informationen bezüglich Identifikation der RTP-Session, des Senders und der übertragenen Daten.

V:
Versionsnummer (aktuell die Nummer 2)

P:
Das Padding-Bit zeigt an, ob es im Packet weitere Auffüllbits gibt oder nicht.

X:
Falls dieses Extension-Bit gesetzt ist, wurde der Header um eine genau spezifizierte Header-Erweiterung mit anwendungsspezifischen Informationen ergänzt.

CC:
Der CSRC-Count enthält die Anzahl der CSRC-Identifizierungen, die dem Header folgen.

M:
Die Interpretation des Markers wird über das für die Übertragung zuständige bzw. gewählte Profil durchgeführt und ist damit in seiner Bedeutung unterschiedlich.

PT:
Der Payload Type identifiziert das RTP-Payload-Format und gibt vor, wie der Payload vom Empfänger zu interpretieren ist. Der Empfänger erkennt darüber, wie die Daten zu interpretieren sind (Verschlüsselungs- und Kodierungsverfahren), RTP kennt 128 unterschiedliche Datenformate. Der RTP-Sender verwendet immer genau ein Format. Versteht der Empfänger diesen Typ nicht, muss er das Packet ignorieren.

Sequence number:
Wie auch bei anderen Übertragungsprotokollen dient die vom Sender vergebene Sequenznummer u.A. dazu, Paketverluste durch den Empfänger festzustellen. Interessanterweise besteht für den Sender die Möglichkeit, mit zufällig gewählten Sequenznummern (Basis: 32 Byte große Zufallszahl) zu beginnen um damit die Gefahr einer Abhörbarkeit zu reduzieren, derartige Techniken sind in Diskussion. Nach dem ersten RTP-Paket wird bei jedem weiteren Paket die gewählte Sequenznummer um den Wert 1 erhöht.

Time Stamp:
Mit Hilfe des Zeitstempels erfolgt die zeitliche Synchronisierung der Pakete. Dabei lässt der Standard unterschiedliche Verfahren zur Synchronisierung zu, da die einzelnen Multimediaanwendungen hier auch unterschiedliche Anforderungen haben. Die Synchronisierungsmethode wird durch das jeweils verwendete Profil vorgegeben. Durchlaufen mehrere RTP-Pakete einen Mixer und werden hier zu einem neuen RTP-Paket zusammengefügt, so kann es sein, dass dieses Paket jetzt den Time Stamp des Mixers trägt. Der Time Stamp wird nicht in Bruchteilen von Sekunden angegeben sondern vielmehr in Vielfachen der für die Payload geltenden Sample Rate.

SSRC identifier:
Dieses Feld dient zur Identifizierung des RTP-Teilnehmers und wird vom Teilnehmer nach einem Zufallsverfahren vergeben, mit dem Ziel, dass zwei Quellen in der gleichen RTP-Session nicht die gleiche SSRC-Identifikation haben. Ein Beispiel für ein Problem bei gleichen SSRC: Zwei Audio-Ströme würden eine RTP-Session nutzen mit gleichem SSRC, und einer von beiden Audio-Strömen müsste z.B. aufgrund einer Verschlechterung der Übertragungsqualität das Kodierungsverfahren ändern, so müsste diese Änderung normalerweise im RTP-Payload-Type gekennzeichnet werden, wäre aber nur für einen von beiden Strömen gültig. Eine Differenzierung, welcher der beiden Ströme jetzt mit dem veränderten Code arbeitet, wäre nicht möglich.

CSRC list:
In diesem Feld trägt ein Mixer die einzelnen SSRC-Identifikationen ein, die er in seinem „gebündelten“ Paket aussendet.

Erkennbar ist, dass es im Unterschied zu vielen Protokollen kein Feld für die Länge des RTP-Paketes gibt. Dies liegt daran, dass der grundsätzliche Ansatz „ein RTP-Paket auf einem Netzwerkpaket“ gilt und die Protokolle der darunter liegenden Ebenen die Größe des RTP-Paketes bestimmen. Bei Bedarf kann dies über entsprechende Profile verändert werden, was zur Folge hat, dass dann doch im RTP-Header die Länge angegeben werden muss.

Zusammenfassend werden nochmals folgenden wesentlichen Funktionen des RTP aufgelistet:

- Erkennung des Typs der Information (Nutzung des Payloads)
- Identifizierung des Senders (Nutzung des SSRC und CSRC)
- Synchronisation (Nutzung des Time Stamp)
- Loss Detection (Nutzung der Sequenz-

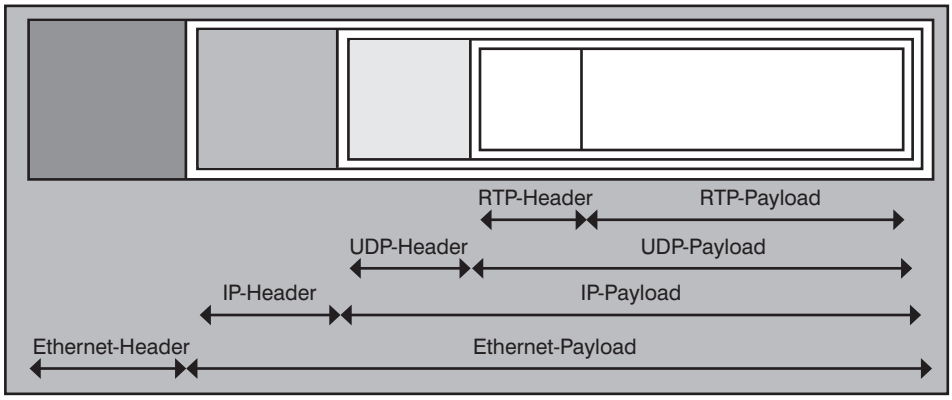


Abbildung 4: RTP im Ethernet-Paket

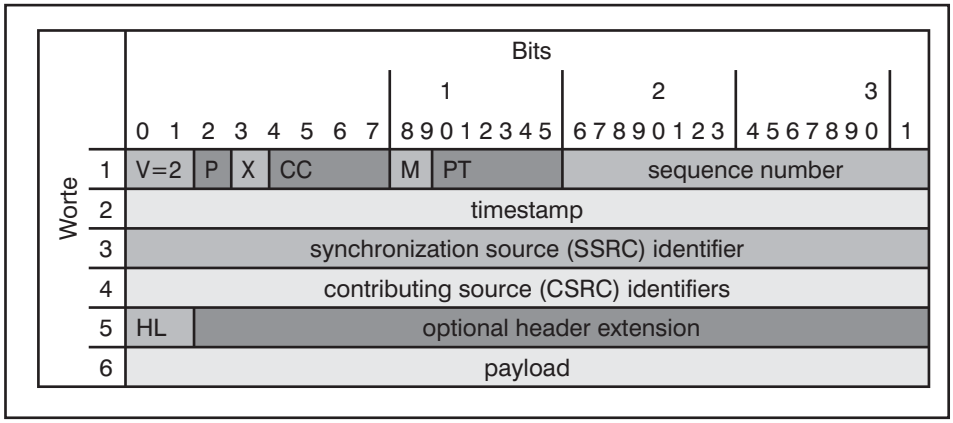


Abbildung 5: RTP-Header

nummer)
- Segmentation und Reassembly (Nutzung des Mixers und der Sequenznummer)
- Sicherheit (durch Verschlüsselung, optional)

Zusammenfassend: Was macht RTP?
Das Realtime Transport Protocol (RTP) transportiert Echtzeit-Nutzdaten in Unicast- und Multicast-Umgebungen. Zur Handhabung besonderer Netzwerkeigenschaften (geringe Bandbreite, Firewalls etc.) und spezieller Anwendungsfälle (Videokonferenzen) können dabei Mixer und Translator zum Einsatz kommen, die mehrere Datenströme zu einem zusammenfassen (Mixer) bzw. Datenströme Paket für Paket verändern (Translator).

Die Kapselung der Nutzdaten erfolgt durch Erweiterungen bzw. Veränderungen des RTP-Protokolls, die in Profile Specifications und Payload Format Specifications definiert sind.

Zusammenfassend:
Was macht RTP nicht?
RTP reserviert keine Bandbreite und garantiert keine festen Übertragungszeiten. Via RTCP wird lediglich ein Mechanismus bereitgestellt, Informationen über die Verbindungsqualität zu verteilen, sodass die Anwendungen darauf ggf. reagieren können.

Ebenso wenig garantiert RTP, dass Pakete in korrekter Reihenfolge oder überhaupt am Empfänger ankommen. Statt dessen stellt es der Anwendung Daten zur Verfügung, mit deren Hilfe diese die korrekte Paketreihenfolge wiederherstellen bzw. verlorene Pakete erkennen kann.

Darüber hinaus regelt RTP nicht das Multiplexen von Datenströmen verschiedener Quellen. Da diese in getrennten Sessions übertragen werden, muss der Empfänger anhand der Transport-Adresse (IP-Adresse und UDP-Port), auf der die Pakete eintreffen, entscheiden, zu welchem Datenstrom sie gehören.

Das Real Time Control Protocol (RTCP)

RTP wird durch das RTP Control Protocol (RTCP) ergänzt, welches den Kommunikationspartnern statistische Informationen über die versendeten RTP-Pakete liefert. Die RTCP-Kommunikation erfolgt zwischen RTP-Sender und RTP-Empfänger, bespielsweise zwischen VoIP-Endgeräten und/oder einem VoIP-Gateway. RTCP liefert den Kommunikationspartnern ein Feedback über die Qualität der Verbindung, das den Endgeräten ein Anpassen der Übertragungsparameter ermöglichen soll. Darüber

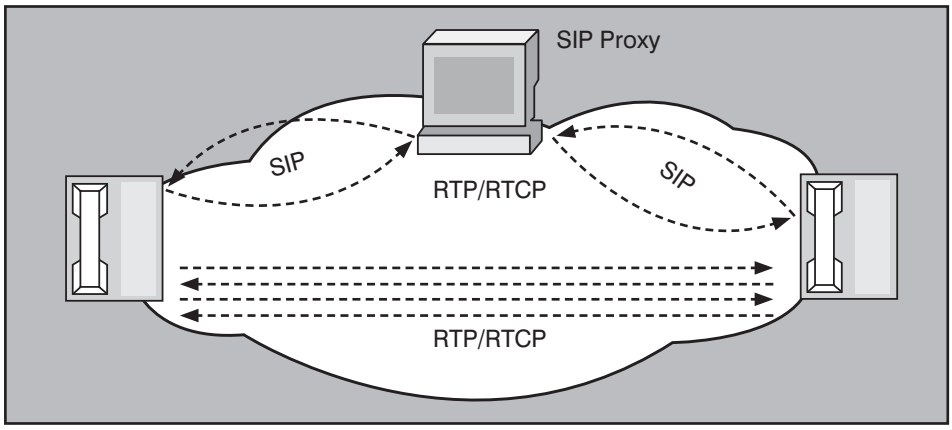


Abbildung 6: Kommunikations-Pfad via SIP und RTP/RTCP

RTCP control Packet types (PT)		
Abkürzung	**Name**	**Typ**
SR	Sender Report	200
RR	Receiver Report	201
XR	Extended Report	207

Abbildung 7: Kontrollnachrichten

hinaus bietet RTCP dem Netzwerk-Manager eine Möglichkeit, mit Hilfe der erfassten Informationen Aussagen über die Qualität des Gesamtnetzes zu treffen und gegebenenfalls Netzanpassungen vorzunehmen.

RTCP ist wie RTP im RFC 3550 standardisiert, jedoch anders als RTP nur selten in den VoIP-Komponenten implementiert. Die in RTCP erfassten Daten werden durch RTCP-XR erweitert, welches in RFC 3611 (Proposed Standard) spezifiziert ist.

RTCP hat im Wesentlichen die folgenden Aufgaben:

1. RTCP liefert mittels Sende- und Empfänger-Report aktuelle Informationen über die Qualität der laufenden RTP-Datenverbindung. Diese Reports ermöglicht den Teilnehmern, den von ihnen generierten Datenstrom an die Netzbedingungen anzupassen (z.B. durch Reduktion der Datenrate bei geringer QoS) und Fehler einzugrenzen.
2. Jeder Teilnehmer erhält eine dauerhafte, eindeutige Bezeichnung (Canonical Name, CNAME), die via RTCP im Netz bekannt gemacht wird. Diese Kennzeichnung kann vom Empfänger auch dazu verwendet werden, mehrere Datenströme eines Teilnehmers (z.B. Audio und Video), die in getrennten Sessions übertragen werden, einfacher wieder zusammenführen zu können.
3. Optional kann eine minimale Verbindungskontrolle über RTCP erfolgen, z.B. indem jeder Teilnehmer grundlegende Informationen über sich selbst versendet (Source Description, SDES), die dann z.B. in der Benutzungsoberfläche der Anwendung angezeigt werden können.

RTCP-Nachrichten werden abhängig von der zugrunde liegenden RTP-Kommunikation als Unicast – z.B. bei Einzelgesprächen - oder als Multicast – z.B. bei Telefon-Konferenzen – generiert und müssen periodisch von allen Teilnehmern gesendet werden. Der Standard empfiehlt als minimales Sende-Intervall der RTCP-Nachrichten 5 Sekunden. Zur Vermeidung eines gehäuften Eintreffens von RTCP-Paketen bei einem Empfänger, z.B. Empfänger-Reports einer Videokonferenz, sind die Sendezeiten der periodischen Pakete mit einer Varianz von 0,5 bis 1,5 des RTCP-Intervalls zu wählen; das erste RTCP-Paket muss mit einer Varianz von 0,5 des berechneten In-

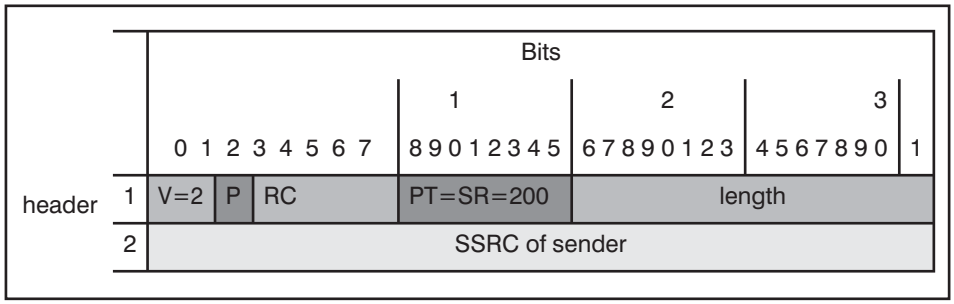


Abbildung 8: RTCP-Header

tervalls gesendet werden. Um bei steigenden Teilnehmerzahlen die Bandbreite für die RTP-Nutzdaten, lt. Standard min. 95% der Gesamtbandbreite, zu sichern, beobachtet jeder Teilnehmer auf Basis der empfangenen RTCP-Pakete die Gesamtzahl der Teilnehmer und berechnet daraus die Rate, mit der Kontrollpakete gesendet werden dürfen. Darüber hinaus kann der „Startwert" des Sende-Intervalls durch den Netzbetreiber den jeweils aktuellen Netz-Gegebenheiten angepasst werden. Insbesondere ist ein Netzbetreiber in der Lage, das Senden der RTCP-Nachrichten vollständig zu unterbinden. Als weitere Maßnahme zur Einsparung von Bandbreite ist die Versendung von zusammengesetzten Nachrichten in einem Paket zwingend vorgesehen, d.h. pro RTCP-Intervall darf maximal ein RTCP-Paket - z.B. Sende-Report kombiniert mit Source Description - generiert werden.

Zum Austausch der Informationen über Paketverluste und Verzögerungen verwendet RTCP im Wesentlichen die Kontrollnachrichten in Abbildung 7.

RTCP-Header
Der RTCP-Header sieht aus wie ein gekürzter RTP-Header. Neben Feldern für die Protokoll-Kennung und Paket-Länge enthält der RTCP-Header die eindeutige Kennung der Datenquelle. (siehe Abb. 8)

V:
Versionsnummer; derzeit festgelegt auf 2

P:
padding; Kennzeichnung für Auffüllung des Paketes auf vollständige Worte

RC:
reception report count; Anzahl der reception report blocks im Paket

PT:
Pakettyp; festgelegt auf 200 (s.o.) für einen Sende-Report

length:
Länge des Paketes in 32-Bit-Wörtern (-1) inklusive Header und Padding-Bits

SSRC:
synchronization source identifier; Identifikation des Paket-Initiators

Sender und Receiver Report
Sender- bzw. Empfänger-Reports (SR bzw. Receiver-Report RR) werden periodisch von jedem Teilnehmer an die Kommunikationspartner gesendet, um den anderen Teilnehmern Informationen über die Qualität der Datenübertragung mitzuteilen.

Grundsätzlich sind Sender- und Empfänger-Reports identisch aufgebaut. Fehlen im Report die Sender-Informationen (sender info), so stellt der Report einen Empfänger-Report dar, ansonsten handelt es sich um einen Sender-Report.

Hat ein VoIP-Teilnehmer seit dem letzten Report-Versand Nutzdaten via RTP versandt, so folgt nach dem RTCP-Header zu-

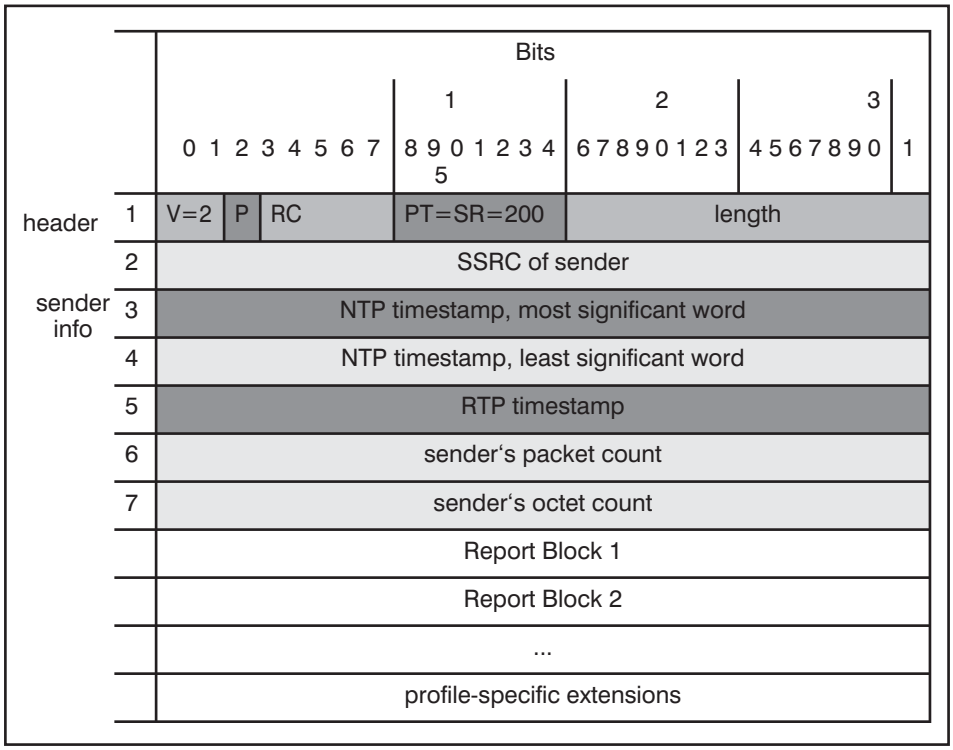


Abbildung 9: RTCP Sender-Report

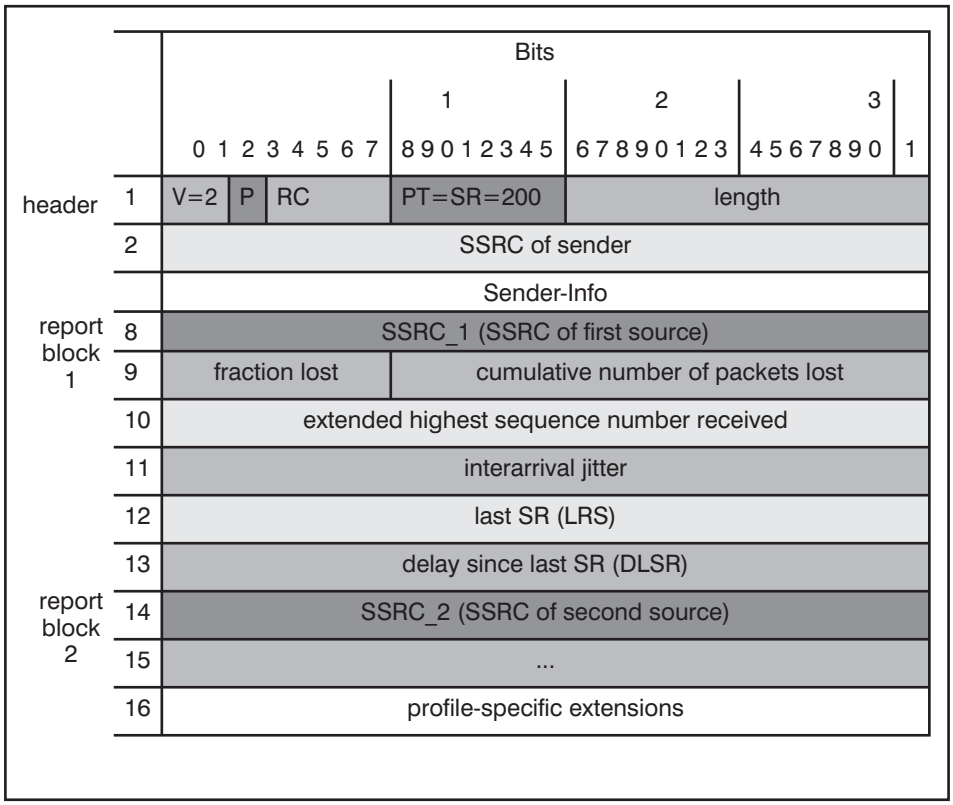


Abbildung 10: RTCP Report-Block

nächst der „sender info“-Block. Er enthält zunächst NTP-Zeitstempel mit der Sendezeit des Reports sowie einen äquivalenten RTP-Zeitstempel, der der Synchronisation dient. Außerdem wird die kumulierte Anzahl der seit Übertragungsbeginn gesendeten Pakete bzw. Bytes angegeben.

Felder des „sender info“-Blocks:

NTP timestamp:
Übertragungszeitpunkt des Reports im NTP-Datenformat; nicht zwingend synchronisiert.

RTP time-stamp:
Übertragungszeitpunkt des Reports im RTP-Datenformat, dient der Synchronisation.

sender’s packet count:
kumulierte Anzahl der übertragenen RTP-Datenpakete seit Beginn der Datenübertragung der laufenden Session (kann bei Wechsel des SSRC zurückgesetzt werden).

sender’s octet count:
kumulierte Anzahl der übertragenen RTP-Nutzdatenbytes seit Beginn der Datenübertragung der laufenden Session (kann bei Wechsel des SSRC zurückgesetzt werden).

Für jede Datenquelle, von der ein Teilnehmer seit dem letzten Versand eines Reports Nutzdaten erhalten hat, folgt anschließend ein Report Block, d.h. ein Report enthält abhängig von der Anzahl der Kommunikationspartner mehrere Empfänger-Reports. Zu jeder durch ihre SSRC identifizierte Datenquelle werden die wichtigsten statistischen Qualitätsmerkmale dokumentiert:

- Prozentsatz und Anzahl der fehlenden Nutzdatenpakete,
- die höchste bereits empfangene Sequenznummer,
- die statistische Varianz (Jitter) des Zeitintervalls zwischen dem Eintreffen zweier Datenpakete,
- Zeitstempel des letzten empfangenen Sender-Reports sowie das seitdem verstrichene Zeitintervall. (siehe Abbildung 10)

Felder des Report-Blocks:
SSRC_n:
Identifizierung der Datenquelle, auf die sich die Angaben beziehen

fraction lost:
Verlustrate der Datenpakete, d.h. Anzahl verlorener Datenpakete / Anzahl empfangener Datenpakete, seit Versand des letzten Reports

cumulative number of packets lost:
kumulierte Gesamt-Anzahl der verlorenen Datenpakete seit Beginn der Datenübertragung

extended highest sequence number received:
höchste empfangene Sequenz-Nummer von Sender SSRC-n (niederwertige 16 Bits); Ergänzung um Empfänger-spezifische Informationen in den höherwertigen 16 Bits

interarrival jitter:
geschätzte statistische Varianz der Paketankunftszeiten der empfangenen RTP-Pakete seit Beginn der Datenübertragung

last SR:
NTP Timestamp des zuletzt empfangenen Sender-Reports

delay since last SR:
Zeit zwischen Empfang des letzen Sende-Reports und dem Versenden dieses Empfänger-Reports

RTCP sieht im Rahmen der Reports optional weitere anwendungsspezifische Felder vor, die abhängig von den Profile Specifications definiert und genutzt werden können.

Mit dem Feedback-Informationen der RTCP-Reports werden die wesentlichen in der Einleitung erwähnten QoS-Paramter auf dem Netzwerk verfügbar:

- Die genutzte Bandbreite
- Paketverlust
- Die mittlere Laufzeit der Pakete
- Die Varianz der Laufzeit (Jitter)

Der Jitter ergibt sich aus der Varianz der Ankunftszeit der RTP-Pakete (interarrival jitter). Sein Wert wird mit Hilfe einer Formel aus dem RFC 3550 berechnet; diese lässt sich relativ einfach an Abbildung 11 (Quelle: www.gandalf.interest.de) erläutern.

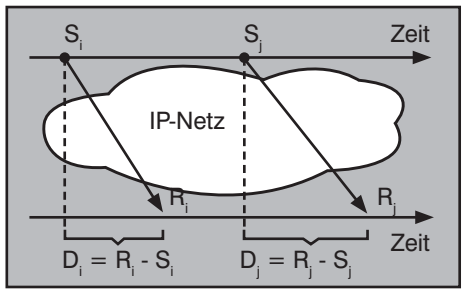


Abbildung 11: Formel aus dem RFC 3550

Die obere Zeitachse kennzeichnet die Sendezeitpunkte der Signale S, die untere Zeitachse deren Empfangszeitpunkte R. Der Wert D beschreibt jeweils den Zeitunterschied zwischen Senden und Empfang. Bei zwei unterschiedlichen Signalen kann dieser Wert D ebenfalls unterschiedlich sein. Die Differenz des Wertes D für beide Signale ergibt die Abweichung der Laufzeit zweier Signale (Packet Spacing) D(j,i):

$$D(i, j) = Dj - Di = (Rj - Sj) - (Ri - Si) = (Rj - Ri) - (Sj - Si)$$

Hieraus errechnet sich der “interarrival jitter” als mittlere Abweichung der Laufzeiten von aufeinander folgenden Paketen.

$$J(i) = J(i-1) + (|D(i-1,i)| - J(i-1))/16$$

Der „interarrival jitter” muss für jeden Report entsprechend dieser Formel gebildet werden, um von speziellen Profilen unabhängige Auswertungen zu ermöglichen.

Zur Unterstützung eines zentralen Monitoring von Multimedia-Daten ist derzeit eine Erweiterung der RMON-MIB für Realzeit-Anwendungen in der IETF-Working Group “Remote Network Monitoring” in Entwicklung. Diese “Real-time Application Quality of Service Monitoring (RAQMON) MIB“ umfasst unter anderem die QoS-Parameter der RTCP Reports. (siehe Abb. 12)

```
RaqmonQoSEntry ::=
      SEQUENCE {
         raqmonQoSTime          Unsigned32,
         raqmonQoSEnd2EndNetDelay          Integer32,
         raqmonQoSInterArrivalJitter       Integer32,
         raqmonQoSRcvdPackets     Integer32,
         raqmonQoSRcvdOctets      Integer32,
         raqmonQoSSentPackets     Integer32,
         raqmonQoSSentOctets      Integer32,
         raqmonQoSLostPackets     Integer32,
         raqmonQoSSessionStatus  SnmpAdminString
         }
```

Abbildung 12: QoS-Parameter der RAQMON-MIB

Das Real Time Control Protocol Extended Reports (RTCP XR)

Die Spezifikation RTCP Extended Report in RFC 3611 definiert weitere Paket Typen für das RTCP zur Generierung detaillierter Statistiken. Darüber hinaus legt der Standard die Nutzung von XR-Paketen durch Applikationen basierend auf dem SDP (Session Description Protocol) fest.

Die Extended Reports werden weiterhin als Sender-Report (SR) oder Empfänger-Report (RR) in regelmäßigen Zeitabständen versendet; diese Zeitabstände sind deutlich höher fest zu legen als die Intervalle zur "normalen" Report-Generierung.

Der Paket-Aufbau des RTCP XR entspricht dem des RTCP mit veränderten Report Blocks. Hier werden sieben verschiedene Report Blocks definiert:

- Loss RLE Report Block: Detaillierte Informationen über einzelne RTP-Pakete und Paketverluste
- Duplicate RLE Report Block: Detail-Informationen über duplizierte RTP-Pakete
- Packet Receipt Times Report Block: Liste der Empfangszeitstempel von RTP-Paketen
- Receiver Reference Time Report Block: Aktuelle Zeit des Empfängers zum Zeitpunkt des gesendeten Reports
- DLRR Report Block: Delay seit dem letzten empfangenen Receiver Reference Time Report Block; hieraus lassen sich in Kombination mit dem Packet Receipt Times Report Block die Round-Trip-Zeiten des Netzes berechnen.
- Statistics Summary Report Block: Die definierten erweiterte Statistiken umfassen die folgenden Parameter:
  - Sequenz-Nummer des ersten betrachteten RTP-Paketes (begin_seq)
  - Sequenz-Nummer des letzten betrachteten RTP-Paketes (end_seq)
  - Anzahl der fehlende Pakete in der betrachteten Paket-Menge (lost_packets)
  - Anzahl der duplizierten Pakete in der betrachteten Paket-Menge (dup_packets)
  - Statistik-Werte bzgl. Jitter: Minimum, Maximum, Mittelwert und Abweichung (min_jitter, max_jitter, mean_jitter, dev_jitter)
  - Statistik-Werte bzgl. TTL bzw. Hop Limit: Minimum, Maximum, Mittelwert und Abweichung (min_ttl_or_hl, max_ttl_or_hl, mean_ttl_or_hl, dev_ttl_or_hl)

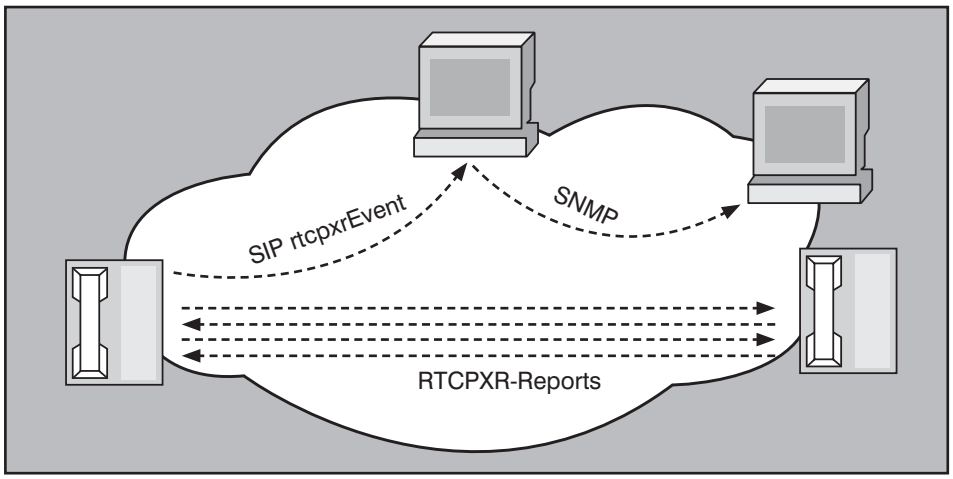


Abbildung 13: SIP RTCP XR Event

- VoIP Metrics Report Block: Die definierten Metriken für Monitoring von Voice over IP-Verbindungen umfassen folgende Parameter-Gruppen:
  - Packet Loss and Discard Metrics
  - Delay Metrics
  - Signal Related Metrics
  - Call Quality or Transmission Quality Metrics
  - Configuration Metrics
  - Jitter Buffer Parameters

Die XR-Spezifikation sieht die Möglichkeit vor, eine „SIP rtcp xr Event"-Nachricht an eine zentrale Komponente zu senden und so eine Analyse der Parameter an zentraler Stelle durchzuführen.

Auch für RTCP Extended Reports ist zur Unterstützung eines zentralen Monitoring von Multimedia-Daten eine MIB in Entwicklung, die jedoch keine Erweiterung der RMON-MIB darstellen wird. Diese ist unter dem Namen "RTP Control Protocol Ex-

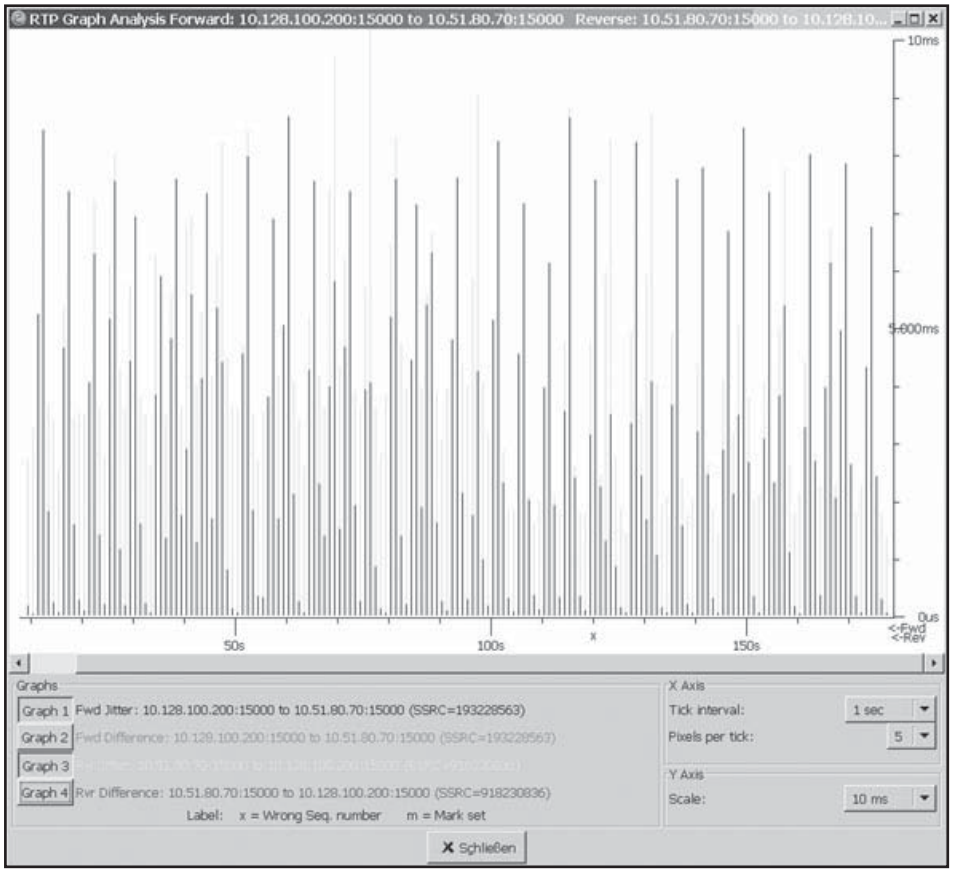


Abbildung 14: Jitter-Analyse von RTP-Paketen in Ethereal

tended Reports (RTCP XR) VoIP Metrics Management Information Base (MIB)“ veröffentlicht und umfasst die wesentlichen RTCP XR-Parameter.

Zusammenfassend:
Bewertung von RTCP-XR
Die Extended Reports bieten im Vergleich zu RTCP erheblich erweiterte Informationen über die Qualität der zu Grunde liegenden RTP-Ströme. Insbesondere bezüglich Paketverlusten, Delay und Jitter sind genauere Aussagen möglich, als mit den Informationen des RTCP.

RFC 3611 erwähnt zum ersten Mal die Möglichkeit, dass die Statistiken nicht nur von den beteiligten Kommunikationspartnern selbst zur Anpassung ihrer Übertragungsparameter an die festgestellte Verbindungsqualität verwendet werden, sondern diese Informationen einem Dritten zur Verfügung gestellt werden. Dabei hat man bereits den Einsatz im Zusammenhang mit VoIP-Lösungen im Sinn.

Beim RFC 3611 handelt es sich um einen „proposed Standard“; es ist die erste Veröffentlichung zu diesem Thema. Man muss daher davon ausgehen, dass der Standard möglicherweise noch nicht stabil ist und noch Änderungen zu erwarten sind. Die RTCP XR-MIB liegt erst in ihrem 2. Draft (Veröffentlichung Juli 2005) vor und ist somit wahrscheinlich ebenso noch Gegenstand von Änderungen. Die entsprechenden Veröffentlichungen sollte man daher im Auge behalten.

Die Messung von RTP und RTCP in der Praxis

Nach so viel detaillierter Information sei die Frage erlaubt, ob sich die beschriebenen Parameter tatsächlich mit einfachen Mitteln messen lassen. Dabei interessiert uns in diesem Zusammenhang noch nicht einmal die Frage, was sich mit den Messwerten schließlich anfangen lässt, wie man also die Qualität eines Multimedia-Streams anhand solcher Messwerte bewertet. Es soll an dieser Stelle nur betrachtet werden, ob und auf welche Weise man die erforderlichen Messwerte gewinnen kann. Prinzipiell sind zwei verschiedene Varianten der Messung denkbar:

1. Direkte Messung eines RTP-Stroms. Das Messgerät ermittelt Delay, Jitter und Paketverlust unmittelbar aus den RTP-Daten und bereitet diese Werte statistisch auf.
2. Indirekte Messung durch Beobachten der RTCP-Meldungen der Endgeräte. Das Messgerät extrahiert Delay, Jitter und Paketverlust unmittelbar aus den Datenfeldern der RTCP Receiver Reports.

Die Variante 1 wird von verschiedenen Messsystemen unterstützt. Ein gutes Beispiel ist der Protokollanalysator Ethereal (Open-Source, siehe http://www.ethereal.com). Er bietet verschiedene Statistiken im Zusammenhang mit RTP-Strömen und erlaubt es sogar, RTP-Ströme in einem Format abzuspeichern, das sich von der Soundkarte eines Rechners abspielen lässt. Probieren Sie es aus! Für unsere Tests haben wir Messdaten herangezogen, die wir zuvor an verschiedenen Terminen „live“ in Netzen unserer Kunden aufgezeichnet hatten.

Das folgende Beispiel zeigt eine typische Auswertung, die mittels Ethereal erstellt wurde (siehe Abbildung 14). Sie stellt den Verlauf des Interarrival Jitter über der Zeit dar. Der Jitter wird - wie wir anhand einer manuellen Auswertung der Paketdaten verifizieren konnten - tatsächlich anhand der Formel aus RFC 3550 errechnet. Die Formel ergibt einen Wert pro RTP-Paket, in der Graphik wird jedoch nur ein Wert pro Sekunde angegeben („Tick interval“). In der Tat ermittelt Ethereal den Jitter pro Paket und wählt für die Anzeige in der Graphik das Maximum im betrachteten Intervall. Hier werden Werte zwischen 1 und 10 ms gemessen. In der Graphik kann man die Werte beider Richtungen anhand der Farbe voneinander unterscheiden; in der Legende ist entsprechend der SSRC angegeben. Der aufmerksame Betrachter entdeckt noch ein kleines „x“ bei 120 Sekunden. Das ist der Hinweis auf einen Paketverlust; betroffen ist die mit „Rev“ bezeichnete Richtung, d.h. Pakete von SSRC 918230836.

Mit dem gleichen Messgerät lassen sich selbstverständlich auch die von den beteiligten Endgeräten erzeugten RTCP-Meldungen auswerten und graphisch darstellen. Die Auswertung der selben Messdaten ist in Abbildung 15 gezeigt. Offensichtlich hat das Messgerät alle 5 Sekunden ein RTP-Paket von jedem der per Filter ausgewählten zwei Endgeräte erhalten. Das entspricht der Norm, da RTCP-Meldungen höchstens alle 5 Sekunden gesendet werden sollen. Angezeigt werden Werte zwischen 60 und 80, eine Einheit ist nicht angegeben. Auch das entspricht der Norm, da RTCP den Interarrival Jitter in Timestamp Units angibt, d.h. mit genau der Granularität, die auch im Timestamp verwendet wird. Bei Sprachübertragung beträgt die Sample Rate 8000

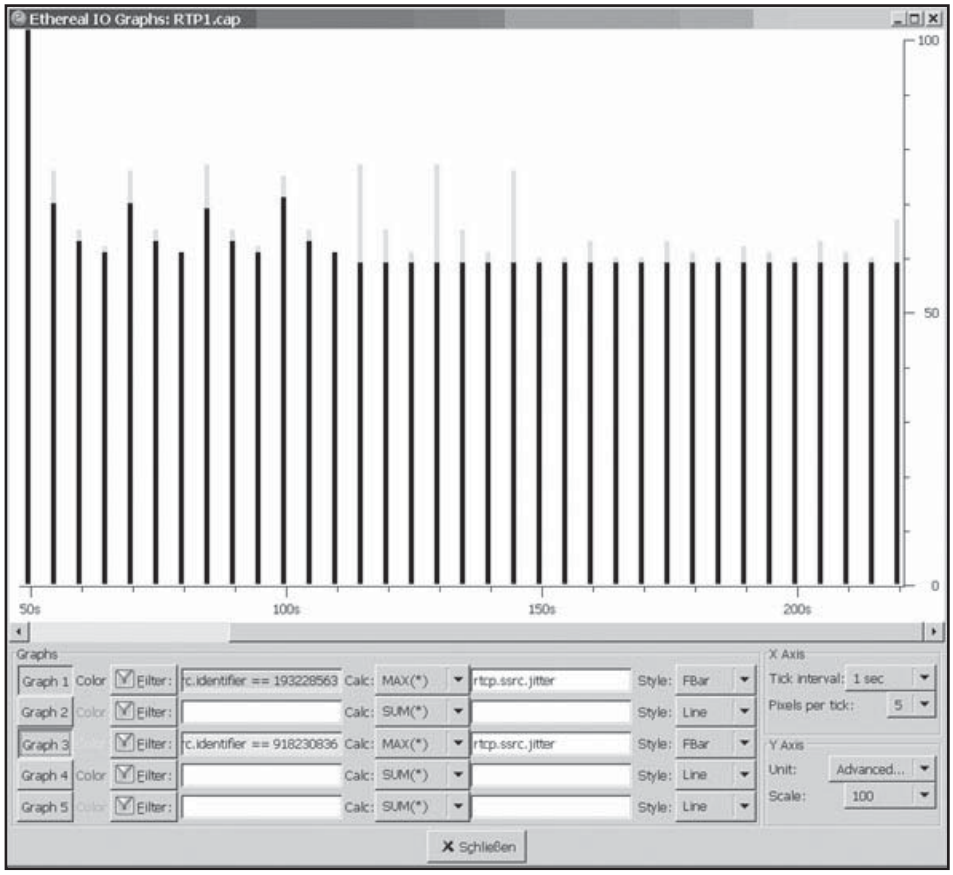


Abbildung 15: Analyse von RTCP-Inhalten in Ethereal

pro Sekunde, eine Timestamp Unit beträgt also 125 μs. Anders ausgedrückt zählt der Timestamp pro Millisekunde um den Wert 8 weiter. Werte zwischen 60 und 80 entsprechen somit tatsächlichen Zeiten zwischen 7,5 und 10 ms. Das liegt immerhin in der Größenordnung des vom Messgerät aus den RTP-Paketen ermittelten Jitter.

Vergleicht man beide Graphiken, so fällt auf, dass RTCP im vorliegenden Fall keine Werte kleiner als 60, entsprechend 7,5 ms anzeigt. Die Norm sagt, dass der zum jeweiligen Sendezeitpunkt vorliegende Wert des Jitter in den Receiver Report einzusetzen sei, anscheinend wird hier jedoch ein Wert eingesetzt, der etwa dem Maximum im vorangegangenen 5-Sekunden-Intervall entspricht. dieser Sachverhalt führt uns zu den Problemen und möglichen Messfehlern der beiden beschriebenen Varianten:

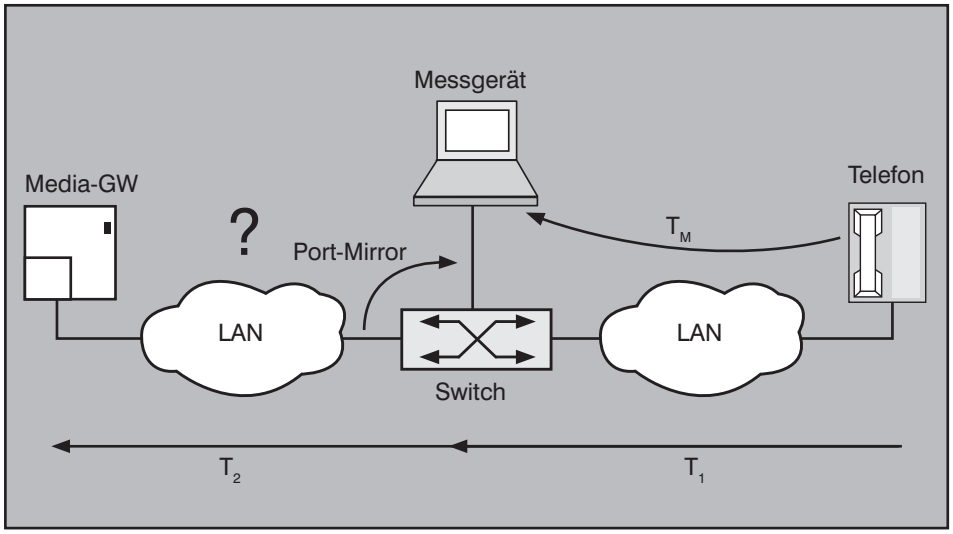


Abbildung 16: Laufzeiten bei der Messung per Port-Mirror

- Variante 1:
  Die Ermittlung von Delay, Jitter und Paketverlust kann per Beobachten eines RTP-Datenstroms durch ein Messgerät genau und nachprüfbar erfolgen. Die Werte sind insofern verlässlich, als ein spezialisiertes Messgerät die tatsächlichen Verhältnisse an seinem Netzwerkadapter messen und bewerten kann. Leider jedoch kann hieraus keine Aussage über die Verhältnisse beim Ziel des jeweiligen Datenstroms getroffen werden. Es ist immerhin denkbar, dass der verbleibende Weg der RTP-Daten zwischen Messgerät und Ziel die Qualität der Daten verschlechtert. Die Abbildung 16 zeigt diesen Sachverhalt. Die Laufzeit T_1 von der Quelle (hier: ein Telefon) bis zu dem Switch, an dem das Messgerät per Port-Mirror angeschlossen ist, wird von diesem erfasst ($T_M \approx T_1$). Die Laufzeit T_2 vom Switch zum Ziel (hier: ein Media-Gateway) kann dagegen vom Messgerät nicht erfasst werden. (siehe Abbildung 16)

- Variante 2:
  Die Auswertung der Datenfelder des RTCP ergibt ein Bild der Verhältnisse am Ziel des Datenstroms. Alle Einflüsse auf die Daten zwischen Quelle und Ziel werden durch diese Messung erfasst. Allerdings ist man bei dieser Variante auf die Genauigkeit der Datenerfassung durch das Zielsystem angewiesen. Schwächen in der Implementierung oder gar Fehler in der Software des Zielsystems können die Messwerte unvorhersehbar verfälschen.

Das obige Beispiel zeigt dieses Dilemma. Es bestehen Unterschiede zwischen den Messergebnissen. Diese Unterschiede können durch in Variante 1 nicht erfasste Effekte zwischen Messgerät und Zielsystem entstanden sein. Andererseits könnte bei Variante 2 eine nicht Standard-konforme Implementierung des RTCP in den beteiligten Endgeräten für die Unterschiede verantwortlich sein. In der Tat fanden wir in einem Softphone für die Internet-Telefonie eine RTCP-Implementierung, die ein mit der Gesprächsdauer linear ansteigendes Jitter vermeldete. Nach ca. 3 Minuten wurde bereits ein Jitter von 200 ms (!) im RTCP-Receiver Report angezeigt, während die Analyse der entsprechenden RTP-Pakete keine Werte größer 1 ms zeigte. Ein weiteres Problem ergibt sich aus der Tatsache, dass RTCP derzeit nicht in allen Endgeräten implementiert ist, die RTP-Streaming durchführen. So sucht man RTCP-Pakete beispielsweise bei der IP-Telephonlösung auf Basis des „Callmanager“ von Cisco vergebens.

Wo wird gemessen?

In der Praxis wird man sich also genau überlegen müssen, wo man ein Messgerät anschließt. Gleiches gilt für die Bewertung von Lösungen, die nicht mit einem separaten Messgerät arbeiten sondern Messwerte von Agenten ermitteln lassen. Verschiedenen Möglichkeiten für die Erhebung von Messdaten sollen den Abschluss dieses Artikels bilden.

1. Die Probe-Lösung:
Ein Messgerät wird, wie in der Abbildung 16 gezeigt, im Datennetz angeschlossen. Dabei wird es sich im Allgemeinen um ein automatisch arbeitendes Gerät zur Überwachung der Verbindungsqualität, also um eine „Probe“ handeln. Die Probe wird, da es sich um ein „geswichtes“ Netz handelt, per Port-Mirror mit einem Switch verbunden und sieht den Datenverkehr eines anderen Ports auf diesem Switch. Man wird dieses Port so auswählen, dass möglichst viele RTP-Datenströme darüber laufen. Optimal wäre der Anschluss in unmittelbarer Nähe des Media-Gateway; dann sieht die Probe jegliche Kommunikation, die über das Gateway führt. Prinzipiell ist die Probe in der Lage, die Qualität beider Richtungen zu beurteilen: Die Richtung vom Telephon zum Gateway wird über die unmittelbare Auswertung der RTP-Pakete bewertet. Da die Probe in unmittelbarer Nähe des Gateway angeschlossen ist, kann der Einfluss der verbleibenden Übertragungsstrecke vom Switch zum Gateway (ein Fast- oder Gigabit-Ethernet-Link) vernachlässigt werden. Die Richtung vom Gateway zum Telefon wird erfasst, indem die Probe die Inhalte der RTCP Receiver Reports auswertet, die von den Telefonen zum Gateway gesandt werden. Voraussetzung ist natürlich, dass die Telephone RTCP unterstützen und die entsprechenden Parameter korrekt errechnen.

2. Die Agenten-Lösung:
Der RTP/RTCP-Stack der Endgeräte wird derart modifiziert, dass die Informationen über die Verbindungsqualität nicht nur an den Kommunikationspartner sondern auch an andere Systeme gesandt werden. Hier sind zwei Ansätze denkbar. Zum einen werden die RTCP-Informationen, die von dem Endgerät erzeugt werden, an ein Logging-System umgeleitet. Zum anderen werden die Informationen in anderes Format gewandelt und mit dem entsprechenden Protokoll übertragen. So lässt sich die Implementierung der RAQMON-MIB auf dem Endgerät denken; die Messwerte lassen sich dann als Inhalte der MIB-Variablen per SNMP von einer „herkömmlichen“ Management-Station lesen.

3. Die Der-Switch-hilft-mit-Lösung:
Die LAN-Switches erhalten ein spezielles Stück Software, dass RTP und RTCP auswertet. Wie bei der Agenten-Lösung kann sich der Switch selbst des Protokolls RTCP bedienen, um die Messergebnisse an ein Logging-System weiterzuleiten, oder er füllt die Variablen einer internen MIB und stellt die Werte so per SNMP zur Verfügung.

4. Die Multicast-Lösung:
Besonders elegant wäre es, wenn die an einer RTP-Kommunikation beteiligten Stationen ihre RTCP-Meldungen nicht per Unicast an den Kommunikationspartner sendeten sondern per Multicast verteilten. Dann wären sie an beliebiger Stelle im Netz von einem Logging-System aufzuzeichnen, das sich zuvor der entsprechenden Multicast-Gruppe angeschlossen hätte. Spannend ist hierbei die Frage, wie stark ein Netzwerk durch solche Multicasts belastet würde. Wie bereits erwähnt, sendet ein einzelner RTP/RTCP-Knoten höchstens alle 5 Sekunden eine Meldung aus. Bei einer mittleren Paketgröße solcher Meldungen von 130 Byte ergibt sich eine mittlere Datenrate von ca. 200 Bit/s. Angenommen, es telefonieren 200 Personen gleichzeitig (100 Paare), ergibt sich eine Multicast-Rate von 40 pro Sekunde bei einer Datenrate von 40 KBit/s. In einem Lokalen Netz wäre das zu vernachlässigen, liegt doch dieses Daten- und Paketaufkommen in der Größenordnung eines einzelnen Telefongesprächs, welches im Rahmen einer Konferenz ebenfalls auf Basis von Multicasts betrieben würde.

Welche der vorgeschlagenen Möglichkeiten zum Einsatz kommt, hängt sicherlich davon ab, was die Hersteller entsprechender Systeme anbieten werden. Die Variante 2 scheint geeignet zu sein, von den Herstellern der Kommunikationssysteme als „Add-on“ angeboten zu werden, da es ihnen naturgemäß leicht fällt, entsprechende Software auf Endgeräten und Gateways zu integrieren. Die Varianten 1 und 3 bieten sich dagegen für herstellerneutrale Lösungen an, da sie sich auf Standard-Funktionen abstützen, die in den Kommunikationssystemen sowieso vorhanden sind - bzw. sein sollten. Variante 4 verlangt nach einem Netz, das Multicast-fähig ist, Multicasts also nicht einfach nur auf alle Ports „flutet“ sondern in geregelten Bahnen lenkt. Solche Netze sind heute noch eher selten anzutreffen. Daher bleibt es abzuwarten, wann Hersteller sich die Implementierung einer solchen Variante „trauen“ werden.
Fertige Produkte gibt es derzeit erst in geringer Zahl. Einige Hersteller veröffentlichen Ideen, diese sind jedoch häufig noch großen Änderungen unterworfen. Das entspricht im übrigen dem frühen Stadium, in dem sich die entsprechenden Normen derzeit noch befinden. Für einen Praxistest von Produkten ist es daher noch zu früh. Wer Multimedia-Systeme aufbaut oder dies in Zukunft plant, sollte die entsprechenden Veröffentlichungen beobachten und/oder die vorgesehenen Hersteller nach entsprechenden Lösungen befragen. Auch kann es lohnend sein, die zukünftigen Ausgaben dieser Zeitschrift weiterhin zu beobachten - wir werden zu gegebener Zeit über Produkte und Testergebnisse berichten.

Zusammenfassung

Multimedia-Anwendungen verlangen die Übertragung von „Realzeit-Daten“. Die Messung und Überwachung der Übertragungsqualität (QoS) solcher Daten ist für den Betrieb von Multimedia-Anwendungen unabdingbar. Wichtige Parameter sind in diesem Zusammenhang Bandbreite, Laufzeit, Varianz der Laufzeit (Jitter) und Paketverluste. Das von den Anwendungen genutzte Real Time Protocol (RTP) erlaubt es, die genannten Parameter direkt durch Beobachtung des Datenstroms zu ermitteln. Das Real Time Control Protocol (RTCP) ermöglicht im Unterschied dazu eine indirekte Ermittlung der Parameter aus Reports, die von den beteiligten Endgeräten generiert werden. Ein Erweiterung des RTCP, die RTCP Extended Reports (RTCP-XR), bietet zusätzliche Informationen und hat die Bereitstellung von Daten mit dem Ziel der QoS-Überwachung im Auge. Eine neue MIB mit der Bezeichnung RAQMON erlaubt die Integration von QoS-Daten in SNMP-Managementsysteme.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
12.09. - 16.09.05 in Aachen
28.11. - 02.12.05 in Aachen
06.02. - 10.02.06 in Aachen
03.04. - 07.04.06 in D'dorf
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Stuttgart
04.12. - 08.12.06 in Aachen

Internetworking
26.09. - 30.09.05 in Aachen
28.11. - 02.12.05 in Aachen
06.03. - 10.03.06 in Aachen
08.05. - 12.05.06 in Bonn
11.09. - 15.09.06 in Aachen
13.11. - 17.11.06 in Aachen

TCP/IP und SNMP
14.11. - 18.11.05 in Bonn
13.02. - 17.02.06 in Bonn
15.05. - 19.05.06 in Stuttgart
27.11. - 01.12.06 in Berlin

Ethernet Technologien - neuester Stand
19.09. - 23.09.05 in Aachen
14.11. - 18.11.05 in Aachen
20.02. - 24.02.06 in Aachen
29.05. - 02.06.06 in Aachen
25.09. - 29.09.06 in Aachen
27.11. - 01.12.06 in Aachen

Paketpreis für alle vier Seminare € 8.170.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
12.09. - 16.09.05 in Aachen
07.11. - 11.11.05 in Aachen
20.03. - 24.03.06 in Aachen
08.05. - 12.05.06 in Bad Neuenahr
04.09. - 08.09.06 in Aachen
06.11. - 10.11.06 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
17.10. - 21.10.05 in Aachen
28.11. - 02.12.05 in Aachen
27.03. - 31.03.06 in Aachen
19.06. - 23.06.06 in Aachen
18.09. - 22.09.06 in Aachen
13.11. - 17.11.06 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
24.10. - 28.10.05 in Aachen
30.01. - 03.02.06 in Aachen
24.04. - 28.04.06 in Aachen
16.10. - 20.10.06 in Aachen

Paketpreis für alle drei Seminare, das Fluke Nettool, die Prüfung und den Report „Trouble Shooting" € 7.500.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
26.09. - 30.09.05 in Nürnberg
06.02. - 10.02.06 in Köln
15.05. - 19.05.06 in Stuttgart
11.09. - 15.09.06 in Bonn

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
19.09. - 21.09.05 in Bonn
07.11. - 09.11.05 in Köln
20.03. - 22.03.06 in Bad Neuenahr
19.06. - 21.06.06 in Weimar
25.09. - 27.09.06 in Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
17.10. - 21.10.05 in Aachen
05.12. - 09.12.05 in Aachen
03.04. - 07.04.06 in Bonn
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Aachen

Paketpreis für alle drei Seminare und Report „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung" € 5.330.-- zzgl. MwSt. (Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.-- / Report 398.--)

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

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 5444632
Fax: 0064 3 5444237

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen