ComConsult Research

Der Netzwerk Insider

September 2008

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Digitale Kameras im Netzwerk

von Dipl.-Ing. Hartmut Kell

Die Erkenntnis, dass ein Lokales Netzwerk sehr einfache Möglichkeiten bietet, visuelle Beobachtungswerkzeuge wie Netzwerk-Kameras anzuschließen und zu nutzen, ist mit Sicherheit nicht neu. Zunehmend setzt man einzelne Kameras insbesondere im unmittelbaren Zuständigkeitsbereich der Netzwerkverantwortlichen, wie z.B. dem des IT-Verteilers, ein. Dabei geht der Beschaffung und dem Einsatz in vielen Fällen keine wirkliche Projektierung voraus.

Es wird einfach eine Netzwerk-Kamera gekauft, montiert und in Betrieb genommen und dann in vielen Fällen mit Hilfe eines Standard-Browsers als verlängertes Auge genutzt. Die Möglichkeiten, welche

die Kamera bietet, aber auch die Grenzen, welche das Netzwerk festlegt, spielen bei solchen Einzelkameras keine große Rolle. Anders sieht es dagegen aus, wenn eine höhere Anzahl von Netzwerk-Kameras vorgesehen ist und dann auch die Möglichkeiten von zentraler Videoanalyse-Software genutzt werden sollen. Spätestes jetzt werden die Grenzen dieser visuellen Medien deutlich, und eine Projektierung ist unumgänglich. Der nachfolgende Artikel wird auf die wichtigsten, im Rahmen einer solchen Projektierung relevanten technischen Aspekte eingehen und fokussiert dabei in erster Linie die Aspekte, die unmittelbar Einfluss auf die Netzwerk-Planung haben.

weiter auf Seite 16

Zweitthema

Vermaschte Wireless Netze:
Funktionsweise, Technologien, Standardisierung unter IEEE 802.11s - Teil 3

von Dipl.-Inform. Petra Borowka

3.3 IEEE 802.11s Frame Forwarding

Die Adressierung und Weiterleitungs-Funktion von Frames in Mesh Netzen muss es ermöglichen, ein Frame innerhalb einer Masche über mehrere Hops zu transportieren.

Hierfür stehen ausschließlich die MAC-Adressen zur Verfügung, da eine Masche ja eine Layer-2 Domäne ist und „Mesh Routing“ somit keine Layer-3 Strukturen (unterschiedliche IP Netze und IP Adressen) nutzen darf. Dadurch entsteht das Problem, Multihop-Routing in einer eigentlich flachen Layer-2-Struktur zu implementieren. Die Lösung des Multihop-Problems wurde darin gefunden, dass der Mesh Header mehr als nur ein Quell-/Ziel-Adresspaar enthalten kann. So ist es möglich, die Ende-zu-Ende Quell- / Ziel-MAC-Adresse und zusätzlich die jeweilige Punkt-zu-Punkt Quell- / Ziel-MAC-Adresse (Next Hop) einzutragen. Im Grunde genommen ist der Unterschied zum „normalen“ Routing gar nicht so groß wie es scheint: Anstelle der Ende-zu-Ende IP Adresse wird eine Ende-zu-Ende MAC-Adresse eingetragen - das kostet Flexibilität, da es weniger große Netze ermöglicht, aber die Definition einer Masche beinhaltet ja auch keine zigtausend sondern nur einige hundert bis etwa eintausend angebundene Stationen (dies entspricht der Größe einer LAN Broadcast-Domäne).

weiter auf Seite 10

Aktueller Kongress

Rechenzentrum Infrastruktur-Redesign Forum 2008

Seite 4

Geleit

Rechenzentren: neue Architekturen erfordern neue Infrastrukturen, Netzwerke sind unter Druck

ab Seite 2

Sonderartikel

Technische Leitlinie Sichere TK-Anlagen des BSI

Seite 9

Zum Geleit

Rechenzentren: neue Architekturen erfordern neue Infrastrukturen, Netzwerke sind unter Druck

Die Ausgangslage erscheint klar. Rechenzentren befinden sich weltweit in der Konsolidierung. Zu viele einzelne Server, hoher Stromverbrauch, Klima-Probleme und hohe Betriebskosten treiben die Entwicklung.

Die dabei alles entscheidende Frage ist, wohin sich die Lösungen in den nächsten drei Jahren bewegen. Diese Frage muss gestellt werden, da bei der Konsolidierung der Rechenzentren nicht nur eine 1:1 Konvertierung von alter zu neuer Welt erfolgt. Konsolidierung bedeutet auch, dass neue Technologien und IT-Architekturen ins Spiel kommen. Auf den ersten Blick erscheint das gar nicht komplex, aber bei näherer Analyse ist das Spektrum möglicher zukünftiger Lösungen erheblich. Die Auswirkungen auf die Infrastrukturen dürfen dabei nicht unterschätzt werden. Speziell die Netzwerk-Infrastrukturen im LAN und im WAN könnten schnell über die Grenze ihrer Leistungsfähigkeit hinaus belastet werden. Vordenken und das Entwickeln einer eigenen Linie ist hier gefordert.

Einige wenige Beispiele zeigen, wie vielfältig und verschieden die neuen Technologien und Architekturen sind und wie weit dabei über das traditionelle Verständnis von Virtualisierung hinaus gegangen wird:

- VMware hat seit einiger Zeit Vmotion geschaffen. Damit können virtuelle Maschinen zwischen physikalischen Servern wandern (wenn diese Server ein ähnliches Profil haben). Damit entstehen völlig neue Perspektiven für Lastverteilung, Kostensenkung, desaster recovery und Change Management. Aber es entstehen auch neue Anforderungen an das Netzwerk und das Security-Design

- SOA und Virtuelle Maschinen gehören zusammen. Virtuelle Maschinen realisieren SOA-Domains. SOA-Domains kommunizieren untereinander. Es entsteht eine starke und realzeit-sensitive Kommunikation zwischen virtuellen

Servern. Was muss das Netzwerk hier leisten?

- Desktop- und Applikations-Virtualisierung sind die am schnellsten wachsenden Technologien. Die weitere Senkung der Kosten für den Desktop, Integration mobiler Mitarbeiter und eine deutliche Erhöhung der Daten- und Applikations-Sicherheit sind die Versprechungen. Je nach Ausprägung verändern sich Lastprofile speziell im WAN-Bereich deutlich. Was bedeutet das?

- Speicher-Konsolidierung verdrängt immer mehr Speicher weg vom physikalischen Server und hin zu SANs und virtuellem Speicher (logische Laufwerke losgelöst von ihrem physikalischem Ort). Parallel dazu wird der Zugriff über das Netzwerk konsolidiert. Nur noch eine Infrastruktur in Form von 10 Gigabit-Ethernet soll hier in Zukunft alle Nutzungsformen unter ein technisches Dach bringen. Welche Anforderungen generiert das an Netzwerke, wo ist hier die Grenze zwischen Netzwerk und System?

Es ist sofort erkennbar, dass diese Technologien erhebliche Auswirkungen auf Netzwerke haben:

- Ein nicht unerheblicher Teil der Kommunikation erfolgt zwischen virtuellen Maschinen, SOA wird dies deutlich verstärken. Aber virtuelle Maschinen auf einer Hardware werden über den Hipervisor-internen Softswitch verbunden. Wie harmonisiert das mit dem Rest des Netzwerkes, wie passieren Security und Redundanz-Konzepte zusammen? Wer ist eigentlich für diesen Softswitch zuständig, die Serverbetreiber oder die Netzwerker? Und warum ist eigentlich sofort alles anders, wenn zwei virtuelle Maschinen auf verschiedenen physikalischen Servern ablaufen? Ist dann wieder der Netzwerker zuständig? Nun bewegen sich virtuelle Maschinen zwischen physikalischen Servern, woher weiß man eigentlich, wie die Kommunikation gerade statt findet und wer zuständig ist?

- Ein Teil der Probleme wird heute über Server gelöst, die viele einzelne Gigabit-Adapter haben. Diese können exklusiv einzelnen Anwendungs-Bereichen (z.B. iSCSI, VM-Management, VMs) zugeordnet werden. Doch je mehr virtuelle Machinen auf einem physikalischen Server konzentriert werden, desto mehr skaliert das nicht mehr. 10 Gigabit-Ethernet ist hier klar der Trend. Aber die Kosten pro Port sind nun so hoch, dass nicht mehr einzelne Ports physikalisch Anwendungsbereichen zugeordnet werden können. Nun teilen sich im schlimmsten Fall iSCSI und VMs einen Port. Wer konfiguriert die Regeln hierfür? Wie passt das alles zusammen?

- Überhaupt bereitet die Fähigkeit virtueller Maschinen, zwischen physikalischen Server zu wandern (mit Umschaltzeiten im Bereich weniger Millisekunden) einiges an Kopfzerbrechen. Welche Datenraten entstehen hier?

- Applikations- und Desktop-Virtualisierung muss jedem Netzwerk-Betreiber wie sein schlimmster Alptraum vorkommen. Die Spannbreite der mögli-

chen Lösungen ist erheblich, die Auswirkung auf Netzwerk-Lasten und Delay-Anforderungen erheblich. Man stelle sich dazu nur Realzeit-Anwendungen oder Video in virtuellen Applikationen auf einem zentralen physikalischen Server vor. Oder besser, man stellt es sich nicht vor.

Diese wenigen Beispiele zeigen, wie komplex die Welt ist, in die wir uns hinein bewegen. Wir lösen eben die bestehende Server-Landschaft nicht 1:1 ab, wir schaffen neue Architekturen.

Direkt im Rechenzentrum stellt sich zum Beispiel die Frage, ob wir spezialisierte Ethernet-Switches brauchen, um den Anforderungen gerecht zu werden. Der sehr hohe Bandbreitenbedarf verbunden mit sehr leistungsstarken Backplanes, spezieller Puffertechnik und kombiniert mit neuen Switching und Redundanz-Verfahren deutet in diese Richtung. Mindestens mit dem Wechsel in den 10 Gigabit-Bereich wird dies ein Thema.

Mit der Technologie-Änderung geht unvermeidbar eine nicht unerhebliche Änderung in den Betriebsabläufen einher. Zum einen ist dies für Virtualisierungs-Projekte ja auch ein Teil der Zielsetzung, zum anderen verschieben sich Grenzen zwischen Technologien. Zuständigkeiten liegen nun teilweise im Überlappungsbereich von Technologien. Hier muss geklärt werden, wie entsprechende Betriebsprozesse sinnvoll umgesetzt werden können.

Ein weiteres Problem, mit dem wir dabei sofort konfrontiert sind, ist die Vorhersagbarkeit der Entwicklung, die ja für Investitions-Entscheidungen in die Infrastruktur entscheidend ist. Dazu vier Beispiele, die zeigen, warum diese Entwicklung schwierig in der Prognose ist:

Beispiel 1:
Der Markt für Virtualisierung wird bisher schon fast monopolistisch von VMware beherrscht. Von daher könnte man meinen, dass eine Orientierung an VMware-Technologien wie VDI, Vmotion oder StorageMotion der beste Weg ist. Aber es entstehen neue Virtualisierungs-Märkte, in denen sich die Marktanteile neu ergeben. Gerade Desktop- und Applikations-Virtualisierung werden den Markt verändern. Hinzu kommt, dass VMware-Lizenzen extrem teuer sind.

Hier setzt Microsoft mit seinen Virtualisierungs-Produkten an. Gerade für Server mit vielen CPUs und vielen VMs hat Microsoft die Karten komplett in seiner Hand. Windows Server 2008 und speziell die Datacenter Edition haben ein anderes Lizenzmodell als VMware, das Einsparungen bis zu 70% möglich macht. Zwar hat VMware einen technischen Vorsprung von vielleicht einem Jahr (speziell im Bereich Vmotion), doch angesichts der erheblichen Kostenvorteile auf der Microsoft-Seite wird es Kunden geben, die bereit sind, hier zu warten. Auch Citrix schläft nicht und wird gerade bei Applikations- und Desktop-Virtualisierung ein erhebliches Wort mitreden wollen. Immerhin kommen hier auch eine ganze Reihe von Bestandskunden aus der Virtuellen Terminal-Technologie ins Spiel. Also an welcher Technologie soll sich der Planer orientieren, unterscheiden sich zum Beispiel diese Hersteller in ihren Anforderungen an Netzwerke und Security?

Beispiel 2:
Cisco versucht, mit Macht den Fiber Channel over Ethernet Standard im Markt zu etablieren. FCoE ist auf den ersten Blick überzeugend, wird hier doch scheinbar eine ähnliche Konsolidierung wie auf der Server-Seite auf der Netzwerk-Ebene angeboten. Doch Ethernet ist nicht Fiber-Channel. Um Paketverluste in den Puffern von Netzwerk-Switchen zu vermeiden, muss das Protokoll erweitert werden. Wenn man die dabei entstehende Congestion Notification zu Ende denkt, dann greift diese Lösung weit in den Anwendungsbereich virtueller Maschinen hinein. Wo hier die Grenze zwischen Server und Netzwerk liegt, bleibt komplett unklar.

Dies wird noch dadurch verstärkt, dass diese Technologie nur mit 10 Gigabit-Ethernet Sinn macht. Hier müssen sich zumindest vorübergehend die verschiedenen Anwendungsbereiche im Server einen einzelnen Adapter/Port teilen. In Kombination mit einem Engpass-Vermeidungsprotokoll wird dies spannend. Nimmt man nun noch Sicherheit und wandernde VMs dazu, wird es geradezu prickelnd. Also hat FCoE eine Chance oder nicht? Wenn nein, was dann? Auf Dauer wird der Fiber Channel gegenüber 10 Gigabit-Ethernet keine Chance haben. Was ist dann die Antwort?

Beispiel 3:
Aus dem Bereich der Telekommunikation kommt die Diskussion über Unified Communications und Unified Collaboration. Die Idee dahinter ist, die Effizienz wichtiger Geschäftsprozesse maßgeschneidert verbessern zu können. Jederzeit, an jedem Ort erreichbar sein und eingebunden werden können, dies ist die Vision. Bei näherer Betrachtung überschneiden sich UC und die neuen aus dem Rechenzentrum kommenden Technologien. Soll zum Beispiel ein mobiler Mitarbeiter oder Entscheidungsträger in einen Prozess eingebunden werden, dann liefern zum Beispiel SUN und VMware mit der Virtual Desktop Infrastructure eine Lösung, mit der an jedem Ort und mit jedem Endgerät auf jede Applikation oder Information zugegriffen werden kann. Ähnliche Ansätze kommen von Microsoft und Citrix. Derartige Technologien müssen ohne Frage im Design von Kollaboration berücksichtigt werden. Im Gegensatz dazu wirken einige UC-Ansätze der TK-Hersteller wie Spielzeug.

Hier muss ohne Frage eine sinnvolle Integration beider Welten gefunden werden. Dies ist durchaus nicht trivial, da Desktop-Virtualisierung nicht jede Form von Realzeitdienst unterstützen muss.

Beispiel 4:
Die Netzwerk-Entwicklung im direkten Umfeld von hoch verdichteten Servern wird stark durch die Preisentwicklung von 10 Gigabit-Ports beeinflusst. Je schneller hier die Preise fallen, desto mehr Kunden werden in diese Technologie wechseln.

Sie sehen, der Umbau unserer Rechenzentren ist ein komplexes Projekt. Dieses Projekt braucht einen roten Faden, will man sich nicht in den verschiedenen Technologien und Hersteller-Strategien verhaspeln.

Hier setzt das ComConsult Rechenzentrum-Infrastruktur-Redesign Forum im November an. Wir analysieren:

- Welche Technologien werden in Zukunft relevant sein?
- Was bedeutet das für die Infrastrukturen, speziell für Netzwerke?
- Wie kann eine Strategie für einen typischen Kunden für die nächsten 3 Jahre aussehen?

Wir stehen ohne Frage vor einer spannenden Entwicklung, die vieles verändern wird, was wir in der Vergangenheit als richtig angesehen haben. Im Kern haben wir gute Chancen, unsere Kosten zu senken und gleichzeitig die Effizienz unserer Geschäftsprozesse deutlich zu verbessern. Dieses Ziel rechtfertigt auch die Auseinandersetzung mit dieser durchaus komplexen technischen Entwicklung.

Ihr
Dr. Jürgen Suppan

Neuer Kongress

Rechenzentrum Infrastruktur-Redesign Forum 2008

Die ComConsult Akademie veranstaltet vom 24.11. - 26.11.08 erstmalig ihren Kongress „Rechenzentrum Infrastruktur-Redesign Forum 2008“ in Königswinter.

Unsere Server und Rechenzentren befinden sich in der größten und umfassendsten Redesign-Phase der letzten 20 Jahre! Die bestehenden Infrastrukturen werden dabei erheblich unter Druck gesetzt.

Die wesentlichen Treiber dieses Redesigns sind:

- Server-Konsolidierung und Virtualisierung
- Applikations- und Desktop-Zentralisierung/Virtualisierung
- Speicher-Konsolidierung
- Neue IT-Architekturen: Dezentralisierung mit zentralen Bausteinen
- Web-basierte Applikationen und Software as a Service

Die Vorteile und Versprechungen sind klar: drastische Senkung der Betriebskosten, optimale Kapazitätsnutzung und 100% Verfügbarkeit. Auf der Kehrseite der Medaille steht die damit verbundene extreme Belastung der Infrastrukturen. Analysiert man den Bedarf der nächsten 3 Jahre, dann wird schnell klar: ohne ein Redesign der Infrastrukturen wird die Konsolidierung der Rechenzentren nicht möglich sein.

Das ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2008 stellt sich diesem herausragenden Thema. Dabei werden folgende Themenblöcke im Mittelpunkt stehen:

1)
Brauchen wir einen neuen Typ Netzwerk?

Dies ist ohne Frage eine der zentralen Fragen des Forums. Wesentliche Hersteller wie Cisco gehen den Weg, spezielle Switching-Technik für das Rechenzentrum zu entwickeln. Speicher-Hersteller wie Brocade und EMC kaufen sich in den Netzwerk- und Virtualisierungs-Markt ein und verändern die Bedarfsparameter. Die alte Standardfrage stellt sich erneut: brauchen wir wirklich neue Technologien oder reicht pure Bandbreite aus?

2)
Wird Virtualisierung am Netzwerk scheitern?

Immer neue Virtualisierungs-Konzepte drängen auf den Markt. Der zunehmende Wettbewerb setzt den Marktführer VMware unter Druck, die Preise werden fallen. Server, Desktop, Applikation: Virtualisierung wird zum Kern eines neuen Architektur-Verständnisses. Hier ist das Potenzial des größten IT-Umbruchs der letzten 20 Jahre gegeben. Die hohe Flexibilität und die neuen Ansätze für Performance- und Kapazitäts-Management haben ihren Preis. Sie erfordern extrem hohe Leistungen im Netzwerk. Werden Netzwerke das leisten können? Wo liegen die kritischen Stellen?

3)
Speicher-Virtualiserung: Ethernet verdrängt Fiber Channel und Infiniband?

Der nächste große Schritt der Netzwerk-Konsolidierung ist die Integration des Speichers. Fiber Channel und Infiniband haben ohne Frage ihre Qualitäten, aber ein nur geringer Wettbewerb hält die Preise dieser Technologien extrem hoch. Mit 10/40/100 Gigabit-Ethernet entsteht demgegenüber der Marktdruck der alles integrierenden Ethernet-Technik. Doch Fiber Channel und Infiniband sind völlig andere Netzwerk-Typen, die eine sehr hohe Qualität und Verfügbarkeit auf Layer-2 sicherstellen. Dem steht die traditionelle Ethernet-Krücke gegenüber, eine eigentlich eher schlechte Technologie, die sowieso nur durch Tricks überleben konnte. Kann das die Basis-Infrastrukur für unsere wichtigen Unternehmens-Daten sein?

4)
Management und Trouble Shooting im Rechenzentrum

Die neue Netzwerk-Welt im Rechenzentrum ist komplex. Viele virtuelle Maschinen müssen auf engstem Raum integriert werden. Viele TCP/IP-Stacks mit unterschiedlichen Implementierungen laufen parallel. Softswitches in den Hypervisorn laufen im Wettstreit mit den externen physikalischen Switch-Systemen. Fehlkonfigurationen und Detailprobleme sind gerade zu vorprogrammiert. Was bedeutet das für Trouble Shooting und Management? Ist unsere Analyse-Fähigkeit in Gefahr?

5)
Netzwerk-Sicherheit ist in Gefahr

Nahezu unbemerkt bedroht Virtualisierung unsere Netzwerk-Sicherheit. Die Fähigkeiten virtueller Server und Desktops, inkl. dem zugeordneten Speicher dynamisch im Netzwerk zu wandern, ist eine echte Herausforderung für die Netzwerke. Softswitches und physikalische Switches müssen schlüssig in einem integrierten Sicherheits-Konzept kombiniert werden. Wo stehen wir und was ist zu beachten?

6)
Erneuerung physikalischer Infrastrukturen: Elektro, Kabel, Klima

Rechenzentrum- und Server-Konsolidierung erfordert auch neue Elektro-Kabel, neue Datenkabel, neue Verteilerschränke. Dabei ist einiges zu beachten. Auf der Elektroseite gibt es eine ganze Reihe neuer gesetzlicher Auflagen, die Datenverkabelung muss sich mit verschiedenen Konzepten den hohen Anschlussdichten stellen. Bandbreite + Anschlussdichte + Gewicht + neue Standards = Kupfer oder Glasfaser? Das ist die Kernfrage. Verteilerschränke müssen Klima-technisch optimal aufgestellt werden, Klima-Probleme müssen schon in der Planung vermieden werden. Welche Alternativen bestehen und wie kommt man zu einer zukunftssicheren Lösung?

Durch das Forum führt Dr. Jürgen Suppan, unter dessen Leitung in den letzten 25 Jahren diverse Projekte aller Größenordnungen erfolgreich umgesetzt wurden.

Programmübersicht Rechenzentrum Infrastruktur-Redesign Forum 2008

Montag, den 24.11.08

9:30 - 11:00 Uhr
Bedarfs-Analyse: Netzwerke im virtualisierten Rechenzentrum
- Server- und Speicher-Konsolidierung: wohin geht der Weg?
- Virtualisierungs-Konzepte im Vergleich
- Umfeld-Parameter: CPU-Leistung und WAN-Bandbreite
- Analyse: Netzwerk-Bedarf virtualisierter Rechenzentren
- Warum Standard-Switching-Technik überfordert ist
- Analyse: mobile Mitarbeiter und ihre Integration
- Wo ist die Grenze zwischen Server und Netzwerk? Konsequenzen für den Betrieb

Dr. Jürgen Suppan, ComConsult Research

11:30 - 13:00 Uhr
Neue Struktur von RZ-Netzen
- Verschiebung der Grenzen zwischen Layer-2- und Layer-3-Strukturen
- Notwendigkeit mehrstufiger Netzhierarchien in Rechenzentren
- Redundanz mit Routing, Link Aggregation, Spanning Tree oder proprietäre Verfahren?
- Active-Standby oder Load Balancing?
- Pro und contra Blade Switches
- Virtuelles Switching

Dr. Behrooz Moayeri, ComConsult Beratung & Planung GmbH

14:30 - 15:15 Uhr
RZ-Verkabelung 2008: wo stehen wir?
- Aus wie vielen Stufen sollte die RZ-Verkabelung bestehen?
- Kupfer oder Glasfaser?
- Stand der Normierung für die Verkabelung von Rechenzentren nach der Neufassung der EN 50173-5 vom Dezember 2007, der ISO/IEC 11801 Adm.1+2 vom Februar 2008 und dem aktuellen Entwurf der ISO/IEC 24764 vom Juni 2008
- Weiteres Vorgehen in den Gremien, insbesondere im Hinblick auf alternative Steckgesichter und den neuen 10/100 GBit Ethernet Standards für Kupferkabel und Lichtwellenleiter
- Bestrebungen zur Rationalisierung / Vereinfachung der Verkabelungsstrukturen in Rechenzentren
- Anpassung der Verkabelungsinfrastruktur an die Bedürfnisse der unterschiedlichen Bereiche in Rechenzentren im Hinblick auf Flexibilität, Packungsdichte und Kabelvolumen
- Änderung der Verkabelungsinfrastruktur beim Umbau oder bei Erweiterungen bestehender Rechenzentren

Stefan Ries, Reichle & De-Massari AG

15:15 - 16:00 Uhr
RZ-Infrastruktur: Schränke, Stromverbrauch, Klima, Green-IT
- Immer mehr Server und Komponenten auf immer weniger Raum
- Wie sollten Schränke angeordnet sein?
- Wie lassen sich Stromverbrauch und Klimaleistung minimieren?
- Was bedeutet Green IT für die RZ-Planung?
- Gefahrenmanagement und Überwachung für Rechenzentren

Dipl.-Inform. Matthias Egerland, Mark Groten, ComConsult Beratung & Planung GmbH

16:30 - 17:30 Uhr
Elektrische Sicherheit beim Redesign von RZ-Infrastrukturen
- Renovierung bestehender Kabel- und Stromsysteme
- Leitlinien für eine sichere Installation
- Gesetzliche Auflagen
- Vorgehensweise

Dipl.-Ing. Karl-Heinz Otto, Sachverständigenbüro Otto

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

Dienstag, den 25.11.2008

9:00 - 10:00 Uhr
10/40/100 Gigabit in der Analyse
- 10 Gigabit-Ethernet: Varianten und Technologie-Situation
- 40 kontra 100 Gigabit: wer wird sich durchsetzen
- Wie die neuen Technologien arbeiten
- Wann sie nutzbar sind
- Empfehlungen

Dr. Franz-Joachim Kauffels, unabhängiger Unternehmensberater

10:00 - 11:00 Uhr
Konvergenz im Rechenzentrum: muss das Ethernet neu erfunden werden?
- Konvergenz von LAN und SAN im Data Centre
- Fibre Channel versus iSCSI versus Fibre Channel over Ethernet
- Was bedeutet FCoE für Data Center Ethernet (DCE)?
- Rolle von Blockübertragung und Congestion Notification
- Staumeldungen oder breite Autobahnen?
- Trends in der Standardisierung

Dr. Franz-Joachim Kauffels, unabhängiger Unternehmensberater

11:00 - 11:30 Uhr Kaffeepause
12:25 - 13:55 Uhr Mittagspause
15:20 - 16:10 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

11:30 - 11.45 Uhr
Request for Proposal an Hersteller
- Beispielszenario eines Rechenzentrums vor dem Redesign
- Redesignziele:
  - Converged I/O
  - Virtualisierung von Servern und Speichersystemen
  - Reduzierung von Beschaffungs- und Betriebskosten
  - Kriterien für die Bewertung der Herstellerlösungen

Dr. Behrooz Moayeri, ComConsult Beratung & Planung GmbH

Herstellerblock
Cisco, Nortel, Enterasys, Juniper, Foundry/Brocade stellen sich dem Szenario

11:45 - 12:25 Uhr
Cisco

13:55 - 14:35 Uhr
Foundry/Brocade

14:35 - 15:20 Uhr
Juniper

16:10 - 16:50 Uhr
Nortel

16:50 - 17:30 Uhr
Podiumsdiskussion

Programmübersicht Rechenzentrum Infrastruktur-Redesign Forum 2008

Mittwoch, den 26.11.2008

9:00 - 10:30 Uhr
Sicherheit neuer Netz- und Serverstrukturen
- Sicherheitsherausforderungen der Servervirtualisierung
- Sicherheit auf Applikations-, System- oder Netzebene?
- Mandantenfähige Rechenzentren und die Voraussetzungen
- Wachsende Rolle von Sicherheitskomponenten in RZs: Firewalls, IPS & Co.
- Ende-zu-Ende- oder segmentweise Verschlüsselung?
- MACsec vs. IPsec vs. TLS vs. Applikationsverschlüsselung

Dr. Simon Hoff,
ComConsult Beratung & Planung GmbH

11:00 - 11:45 Uhr
Lösungsansatz: Security in Virtuellen Umgebungen
- Sicherheits-Herausforderungen im Szenario
- Typische Probleme
- Lösungsansätze

Dipl.-Ing. Markus Nispel,
Enterasys Networks/Siemens Enterprise Communications

11:45 - 12:30 Uhr
Lastverteilung auf und in Rechenzentren
- Hochverfügbarkeitskonzepte zwischen und innerhalb von Rechenzentren
- Alternativen für Load Balancing
- Load Balancing auf Betriebssystemebene oder dedizierten Switches?

Dr. Behrooz Moayeri,
ComConsult Beratung & Planung GmbH

14:00 - 14:45 Uhr
WAN-Anbindung von Rechenzentren
- Layer 2 vs. Layer 3 im WAN
- WAN-Anbindung von Rechenzentren: MPLS versus Ethernet
- Disaster Recovery, RZ-RZ-Kopplung

Dr. Joachim Wetzlar,
Dr. Behrooz Moayeri,
ComConsult Beratung & Planung GmbH

14.45 - 15:30 Uhr
Netzanalyse in Rechenzentren
- Herausforderung der Netzanalyse bei steigenden Bitraten
- Stand der Technik bei der Messtechnik und Analyse
- Blockübertragung: was bringt es wirklich?
- TCP und seine Grenzen

Dr. Joachim Wetzlar,
ComConsult Beratung & Planung GmbH

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
ca. 16:00 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor!

10% Frühbucherrabatt bis zum 30.09.2008

Noch diesen Monat bieten wir eine Vorbuchungsphase für das Rechenzentrum Infrastruktur-Redesign Forum 2008. Profitieren Sie von der rabattierten Teilnahmegebühr und melden Sie sich rechzeitig an.

Fax-Antwort an ComConsult 02408/955-399

Frühbucher-phase bis 30.09.2008

Anmeldung

Rechenzentrum Infrastruktur-Redesign Forum 2008

Frühbucher-phase bis 30.09.2008

Ich buche den Kongress **Rechenzentrum Infrastruktur-Redesign Forum 2008**
☐ 24.11. - 26.11.08 in Königswinter
zum Preis von € 1.690,- * zzgl. MwSt.
*gültig bis 30.09.2008
(dann regulär € 1.890,- zzgl. MwSt.)

☐ Bitte reservieren Sie für mich ein Hotelzimmer

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

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

Voice- und Video-Forum 2008

Die ComConsult Akademie veranstaltet vom 10.11. - 13.11.08 ihr „Voice- und Video-Forum 2008“ in Königswinter.

Die nächsten Monate werden den TK- und Kommunikationsmarkt weiter stark verändern. Neue Produkte, neue Hersteller-Strategien und ein neues Verständnis von Kommunikation prägen die Trends.

Das ComConsult Voice- und Video-Forum 2008 analysiert diese aktuellen Entwicklungen und bewertet sie in einer Mischung aus Marktanalyse, Technologie-Positionierung und Projekt-Erfahrungsberichten.

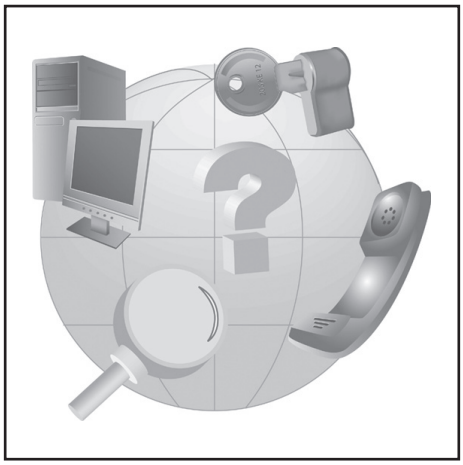
Folgende Kernthemen werden das Forum u.a. prägen:

1) Die Situation bei Siemens

Hier geht es nicht nur um 50% der installierten Basis in Deutschland. Die Entwicklung bei Siemens mit der Zusammenführung mit Enterasys und der damit verbundenen Neuausrichtung wird prägend für den gesamten deutschen Markt sein. Die Frage, was aus den traditionellen Produkten wird und wie stark die neuen Produktlinien gepuscht werden, wird die Marktposition aller traditionellen Produkte und Hersteller beeinflussen. Wir werden auch die Frage analysieren, welche Potenziale speziell aus der Fusion mit Enterasys entstehen. Nicht umsonst besteht im Hause Cisco eine gewisse Nervosität. Wir präsentieren unsere Einschätzung der Siemens-Situation auf dem Forum.

2) Die Situation bei Cisco

Bei Cisco bereitet sich nicht nur alles auf den CallManager 7 vor, der der Abschluss der Übergangsentwicklung vom CallManager 4 zu einer SIP-basierten Architektur ist. Auf dem Prüfstand steht auch Ciscos Gesamt-Strategie. Mehr als das bei den traditionellen Anbietern Alcatel, Avaya, Nortel und Siemens der Fall ist, steht Cisco auch in einem direkten Wettbewerb mit Microsoft und IBM. Cisco ist deshalb sehr früh in Unified Communications eingestiegen. Speziell der Einstieg Microsofts hat aber die Lücken in der Cisco-Strategie offen gelegt. Zur vollständigen kommunikationstechnischen Unterstützung der Geschäftsprozesse kommt man an einer Kollaborations-Plattform nicht vorbei. Präsenz und SIP reichen nicht aus, um den UC-Bedarf der Unternehmen wirklich abzudecken. Cisco hat das klar erkannt und weitet seine Strategie entsprechend aus. Wir analysieren Cisco´s Strategie mit den neuesten Entwicklungen und positionieren sie speziell im Vergleich zu Microsoft und Siemens.



3) Die Situation bei Microsoft

Vor einem Jahr noch war der Office Communications Server OCS eine Sensation. Aber schon damals haben wir klar gesagt, dass dies nur der Einstieg Microsofts ist. Die wahre Bedeutung des Produkts für den Markt wird sich erst mit den Folgeversionen zeigen. An dieser Stelle stehen wir nun. Die nächsten Versionen stehen vor der Tür. Gleichzeitig haben die Konkurrenten, speziell Cisco und Siemens, auf den Angriff reagiert. Wir analysieren auf dem Voice- und Video-Forum: wo steht Microsoft mit seinen Produkten im Vergleich zur Konkurrenz?

4) Unified Communications

UC ist ohne Frage das Mega-Schlagwort 2008. Aber jeder Hersteller versteht etwas anderes darunter. ComConsult Research hat eine Hersteller-neutrale Definition des Begriffs entwickelt, die sich eng an den Bedarf der Unternehmens-Geschäftsprozesse anlehnt. Wir stellen unser Verständnis vor und positionieren die wesentlichen Hersteller zu diesem Verständnis. Wir werden klar Stellung beziehen, in welches Verständnis von UC sich Investitionen lohnen und in welches nicht.

5) Video- und Webkonferenzen

Die Mischung aus mehr Bandbreite im Internet und der Weiterentwicklung der Videotechnik und Konferenztechnik hat eine einmalige Ausgangslage geschaffen. Hier kommt ein völlig neues Verständnis von Konferenztechnik auf den Markt zu. Der Preisverfall von HD-Technik wird dies in den nächsten 24 Monaten zu dem vielleicht momentan spannendsten Markt machen. Cisco hat es mit seiner High-End Telepresence-Lösung vorgelebt: Videokonferenzen können hochgradig effizient und wirtschaftlich sein. Jeder Vergleich mit traditioneller Videokonferenztechnik ist praktisch sinnlos. Mit HD-Video ist ein völlig neues Konferenz-Erlebnis entstanden. In Konsequenz amortisieren sich diese Lösungen in wenigen Monaten. Aber der Markt ist extrem in Bewegung. Auf Dauer werden nur Produkte überleben, die in Gesamtlösungen eingebunden sind. Auch die Offenheit zu anderen Unternehmen gewinnt immer mehr an Bedeutung. Wir analysieren, wo der Zug hinfährt und welche Kriterien bei der Produktentscheidung wichtig sind.

6) Session Initiation Protocol SIP

Auch wenn es nicht jeder wahrhaben will: SIP ist ein elementarer Baustein auf dem Weg in ein anderes Kommunikations-Verständnis. Die Trennung von Signalisierung und Medienstrom und die Reduzierung der Zustandsmenge im Vermittlungsknoten schaffen völlig neue Architekturen. Wesentliches Merkmal ist die Offenheit dieser Welt. Dies ist nicht reduzierbar auf Telefone von Drittanbietern, hier geht es um eine völlig andere Art der Integration von Applikationen und Kommunikation. Wer SIP auf eine Diskussion von Leistungsmerkmalen reduziert, der hat nicht verstanden, wohin SIP wirklich will. Wir analysieren die Fortschritte der letzten Monate und geben den Ausblick auf 2009: wo steht SIP und welche Vorteile bietet es!

7) Die Rolle der traditionellen Anbieter

Alcatel, Avaya, Nortel und viele andere mehr haben den TK-Markt in den letzten 20 Jahren geprägt. Diese Hersteller haben international eine erhebliche Marktmacht und dürfen nicht unterschätzt werden. Die Zukunft der Kommunikation wird international entschieden. Der Übergang zur Software beinhaltet auch die Abnahme der Bedeutung regionaler Märkte. Das Voice-Forum 2008 stellt die Strategien von Alcatel, Avaya und Nortel vor.

Die Liste ist zum jetzigen Zeitpunkt nicht vollständig. Wesentliche Arbeiten und Diskussionen laufen noch. Beachten Sie die Information der nächsten Wochen, um auf dem Laufenden zu bleiben.

Die aktuellen Gespräche und Vorbereitungs-Arbeiten zeigen: das ComConsult Voice- und Video-Forum 2008 wird auch in diesem Jahr der Treffpunkt der Kommunikations-Branche.

Voice- und Video-Forum 2008

10% Frühbucherrabatt bis 15.09.08

Voice- und Video-Forum 2008

10.11. - 13.11.08 in Königswinter

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir auch in diesem Jahr exklusiv eine Vorbuchungsphase für das Voice- und Video-Forum 2008 bis zum 15. September 2008 für eine rabattierte Teilnahmegebühr an.

Voice- und Video-Forum 2008
zum Preis bei Buchung bis 15.09.08 von € 2.090,-
statt regulär € 2.290,- zzgl. MwSt.

Teilnehmer am Forum können die Studie von Dr. Jürgen Suppan „Analyse der Strategie und Marktposition von Siemens Enterprise Communications“ zum Sonderpreis von € 149,- statt regulär € 198,- zzgl. MwSt. erwerben

Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Voice- und Video-Forum 2008

Ich buche den Kongress
Voice- und Video-Forum 2008

☐ 10.11. - 13.11.08 in Königswinter
zum Preis von € 2.090,- * zzgl. MwSt.
*gültig bis 15.09.2008
(dann regulär € 2.290,- zzgl. MwSt.)

☐ mit Report „Analyse der Strategie und Marktposition von Siemens Enterprise Communications“
zum Preis von € 149,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Zimmer im Maritim Hotel Königswinter

vom_____ bis_____ 08

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Technische Leitlinie Sichere TK-Anlagen des BSI

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung und Betrieb im Bereich lokaler Netze, mobiler Kommunikationssysteme und deren Anwendungen zurück.

Moderne Telekommunikationssysteme sind untrennbar mit der IT verbunden. VoIP und IP-basierte TK-Applikationen bilden die Basis für diesen Integrationsprozess, und zusammen mit der Konvergenz von Festnetzen und der mobilen Kommunikation ermöglicht Unified Communications eine medien- und systemübergreifende Nachrichtenübertragung. Diese grenzüberschreitenden Kommunikationsmöglichkeiten haben jedoch signifikante Auswirkungen auf die Sicherheit. Gefährdungen der IT springen auf die Telekommunikation über, und durch das Zusammenwirken der vernetzten Komponenten entstehen unerwartete neue Bedrohungen.

Beispielsweise können ungesicherte (Sprach-)Übertragungen in IP-basierten Netzen mit einem vergleichsweise geringeren Aufwand aufgezeichnet und manipuliert werden, und außerdem sind Schnittstellen und Datenübertragung bei TK-Applikationen oft nur ungenügend abgesichert. Schadenstiftende Software kann nicht nur PCs und Server im Netz befallen. Die Angriffsziele sind dabei unter anderem IP-Telefone, Softphones, Smartphones und die Server, die auf konventionellen Betriebssystemen aufbauend Telekommunikationsdienste und -anwendungen unterstützen.

Auf diese komplexe, systemübergreifende Gefährdungslage muss mit einem ganzheitlichen, auf die konkrete Nutzungsweise der Telekommunikation flexibel zugeschnittenen Maßnahmenkatalog reagiert werden. Dabei muss insbesondere berücksichtigt werden, dass bei der Übertragung und Verarbeitung von Sprachinformationen und der zugehörigen Teilnehmerdaten oft erhöhte Anforderungen an die Sicherheit bestehen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die ComConsult Beratung und Planung GmbH haben hierzu die Technische Leitlinie Sichere TK-Anlagen erarbeitet.

Diese Technische Leitlinie analysiert unter besonderer Berücksichtigung eines erhöhten Schutzbedarfs die Gefährdungslage, beschreibt Sicherheitsmechanismen und gibt konkrete, praxisorientierte Empfehlungen für Planung, Aufbau und Betrieb von privaten Telekommunikationssystemen. Dabei wird die gesamte Palette der modernen privaten Telekommunikation bestehend aus ISDN TK-Anlagen, VoIP- und Hybrid-Systemen (inklusive IP-Anlagenanschluss bzw. SIP Trunking) und der Nutzung von mobilen und drahtlosen Kommunikationssystemen betrachtet. Einen Schwerpunkt bildet dabei die Analyse der Sicherheitslage und die Erarbeitung von Sicherheitsmechanismen für TK-Applikationen und Mehrwertdienste, da hier wesentliche Elemente für Unified Communications zusammenlaufen und die systemübergreifenden Gefährdungen durch die Vielfalt der Schnittstellen zwischen TK-System und IT-Landschaft besonders ausgeprägt sind.

Die Technische Leitlinie beinhaltet auch einen Beschaffungsleitfaden, der sicherheitsspezifische Anforderungen an die Komponenten einer TK-Anlage (inklusive Endgeräte, Netzelemente, Server, Gateways und Management-Werkzeuge) beschreibt. Zur Unterstützung der Produktauswahl und der Abnahme werden weiterhin Prüfkriterien entwickelt, die neben Prüfungen der Konfiguration insbesondere auch Tests auf Ebene der Protokollschnittstellen spezifizieren.

Die Technische Leitlinie Sichere TK-Anlagen ist auf den Web-Seiten des BSI unter http://www.bsi.de/literat/doc/tkanlagen/TL02103.htm verfügbar.

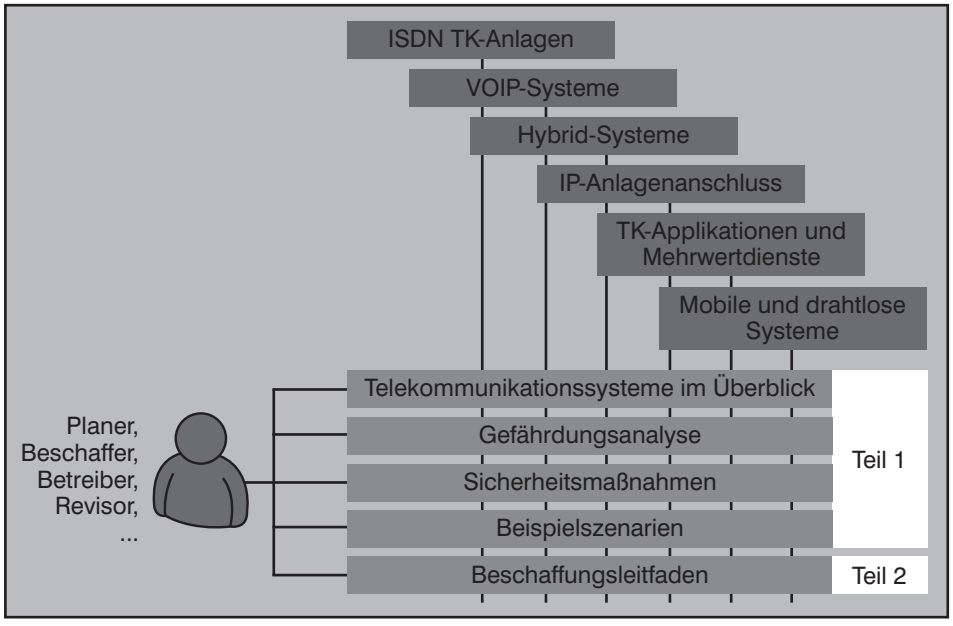


Abbildung 1: Aufbau der Technischen Leitlinie Sichere TK-Anlagen

Zweitthema

Vermaschte Wireless Netze:

Funktionsweise, Technologien, Standardisierung unter IEEE 802.11s -

Teil 3

Dipl. Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Fortsetzung von Seite 1

Punkt-zu-Punkt wird dann wie beim Routing die MAC-Adresse des Next Hop eingetragen - hier hat sich also nichts geändert.

Adressierung

Nehmen wir als Beispiel die Abbildung 3.7. Beide Endgeräte Hugo und Otto sind nicht am Mesh Dienst beteiligt. Der Sender Hugo ist an einem Mesh AP (MAP) assoziiert. Das Ziel Otto ist ein System außerhalb der Masche, das über ein Portal erreichbar ist. Hugo und Otto sind 3 Hops voneinander entfernt: Auf dem Weg vom Sender Hugo zum Empfänger Otto ist Hop1 der MAP, Hop 2 ein reiner Relay Mesh Point (MP), Hop 3 das Portal (MPP). Die Abbildung zeigt die jeweilige Punkt-zu-Punkt Kommunikation (Link), den Gesamtweg durch die Masche (Mesh Path), dessen Endpunkte Mesh Ingress / Mesh Egress heißen und den Ende-zu-Ende Weg (Ende-zu-Ende-802 Kommunikation). Im Beispiel ist der Mesh Ingress der MAP, an dem Hugo assoziiert ist. Der Mesh Egress ist das Portal (MPP), über das Otto erreichbar ist. Die Punkt-zu-Punkt Adressen sind bei Link(1) Sender-Station / MAP, bei Link(2) MAP / MP, bei Link(3) MP / MPP und bei Link(4) MPP / Empfänger-Station.

Das Beispiel zeigt, dass in einem Header maximal drei Adresspaare erforderlich sind: Punkt-zu-Punkt (Link(1) bis Link(4)), Mesh Ingress / Mesh Egress (Mesh Path) und Sender / Empfänger (Ende-zu-Ende-802). Nach guter MAC-Tradition ist jeweils die Zieladresse die erste und die Quelladresse die zweite Adresse eines Pärchens. Diese Adress-Paare sind nach dem LIFO Stack-Prinzip geordnet.

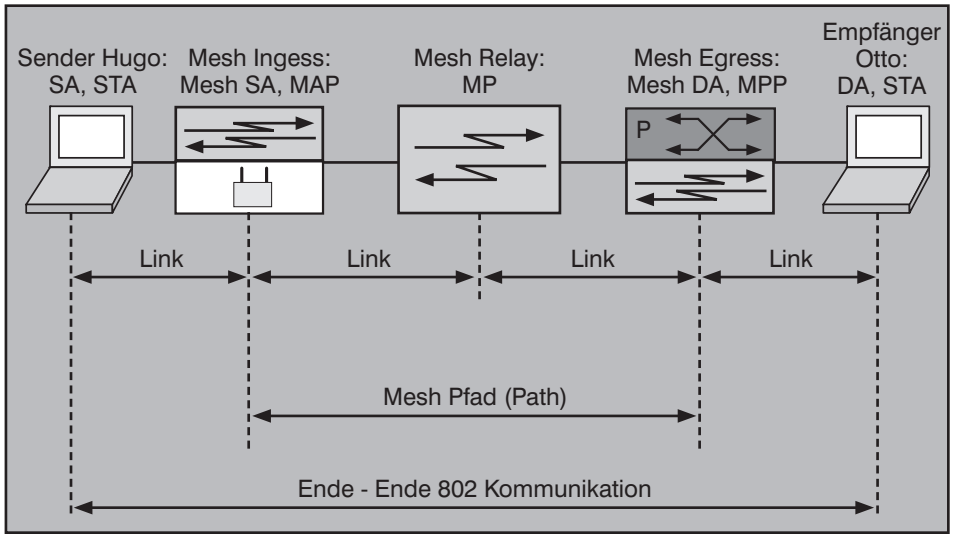


Abbildung 3.7: Mesh WLAN als Layer-2 Dienst nach außen

Adresse 1 und Adresse 2 sind die Punkt-zu-Punkt-Adressen, sie gehören zum Next Hop Mesh Point und sendenden Mesh Point und heißen RA (Receiver Address) und TA (Transmitter Address).

Adresse 3 und Adresse 4 heißen Mesh DA und Mesh SA. Sie gehören zu dem Mesh Egress und Mesh Ingress. Der Begriff Mesh-Quelle (Mesh SA) bezieht sich dabei auf den ersten Mesh Point, der das Frame in die Masche weiterleitet. Dieser kann gleichzeitig der Original-Sender für das Frame sein, ansonsten ist er ein Proxy MP, der das Paket von außerhalb der Masche oder von einer assoziierten Station erhalten hat. Das Mesh-Ziel (Mesh DA) ist der letzte Mesh Point auf dem Weg durch die Masche. Dies ist der MP, der die finale Zielstation assoziiert (Proxy MP) oder ein Portal zur finalen Zielstation hat oder der das Frame auf einen anderen Mesh Pfad innerhalb oder außerhalb der Masche weiterleitet (z.B. ein Root MP).

Adresse 5 und Adresse 6 sind Empfänger-Station (DA) und Sender-Station (SA). Sie werden nicht in jedem Frame, sondern nur in zwei Fällen benötigt:

- Fall 1: Sender und Empfänger sind non-Mesh Endgeräte, die den Mesh-Dienst selbst nicht unterstützen sondern über Proxy Mesh Points (MP's) kommunizieren (typischerweise eine

assoziierte WLAN-Station) oder die außerhalb der Masche liegen (z.B. ein Server hinter einem Portal oder aber die MAC-Adresse des Next Hop Routers, der die Kommunikation der Masche mit der Serverfarm ermöglicht)

- Fall 2: Sender und Empfänger sind Mesh Points, die über einen Root MP kommunizieren, der im HWMP Proactive Mode arbeitet; in diesem Fall werden zwei Mesh Pfade genutzt, der erste vom Quell-MP zum Root-MP und der zweite vom Root-MP zum Ziel-MP

Da Adresse 5 und 6 nicht immer vorhanden sind, gibt es das Address Extension Mode Feld, ein 2-Bit Wert, der im ersten Bit anzeigt, ob 4 oder 6 Adressen im Header stehen, d.h. ob der Weg zwischen zwei MP's derselben Masche verläuft oder ob non-Mesh Stationen außerhalb der Masche beteiligt sind (wie z.B. Hugo und Otto). Im zweiten Bit zeigt das Extension Mode Feld an, ob das Frame ein Daten- oder ein Kontrollframe (Multihop Action) ist. Die möglichen Headerformate für Adressierung sowie die zugehörigen Extension Mode Werte sind in Abbildung 3.8 zusammengefasst.

Weiterleitung

Was tut ein Mesh Point, wenn er ein Frame erhält? Er ist dann die Mesh-Source und somit derjenige Mesh Point, der vor der Weiterleitung des Datenframe in die Masche entscheiden muss, welches Adressformat in den Header eingefügt wird. Hier gilt die Regel: Wenn beide Endpunkte MP's auf einem gemeinsamen Mesh Pfad sind, dann verwendet er das 4-Adress-Format und setzt das Address Extension Mode Feld auf „00". Sind ein oder beide Endpunkte kein MP, nimmt er das 6-Adress-Format und setzt das Address Extension Mode Feld auf „10". Ist einer der Endpunkte ein MP und einer nicht, so erscheint die Adresse des MP, der gleichzeitig Endpunkt ist, zweimal, in Adressfeld 3 und 5 oder in Adressfeld 4 und 6.

Wenn ein Mesh Point ein Unicast Mesh Frame empfängt, soll er es im ersten Schritt entschlüsseln und eine Authentizitäts-Prüfung durchführen. Ist der Absender kein Peer-MP, so soll er das Frame ohne weitere Rückmeldung verwerfen (silently discard). Diese Regelung ist schlüssig, da ja jeder MP beim Weiterleiten (wie ein Router) seine eigene MAC-Adresse als RA-Adresse in den Header einträgt. Somit können gültige Frames nur RA-Adressen von einem Peer-Mesh Point enthalten.

Im zweiten Schritt prüft der Mesh Point die Mesh DA im Adressfeld 3. Kennt er sie nicht, kann er das Frame entweder stillschweigend verwerfen oder eine Path Discovery starten. Ob der Mesh Point das Frame verwirft oder nicht, ist abhängig von dem Path Selection Protokoll, das aktiviert ist: Nutzt er ein Proaktives Verfahren, verwirft er das Frame (weil er schon Wege zu allen möglichen Zielen aufgebaut hat), nutzt er ein On-demand Verfahren, startet der Mesh Point eine Path Discovery (diese Zusammenhänge wurden in Teil 2 im Netzwerk-Insider Ausgabe Mai 2008 beschrieben).

Schritt drei prüft auf Duplikate: Anhand der Quell-MP Adresse (Adressfeld 4) und der Mesh Sequenznummer erkennt der Mesh Point duplizierte Frames. Diese darf er verwerfen oder weiterleiten. Im letzteren Fall ist es Sache des Portals oder der Zielstation, Duplikate zu erkennen und zu verwerfen.

Schritt 4 ist die eigentliche Entscheidung, wohin der Mesh Point das Frame weiterleitet: Falls Adresse 3 (Mesh DA) nicht die eigene MAC Adresse, aber eine bekannte MAC-Adresse ist, muss das Frame an den Next Hop Mesh Point weitergeleitet werden. Hierfür reduziert der MP die TTL um 1. Ergibt der Wert dann „0", so wird das Frame verworfen. Andernfalls ändert der MP die Adressen entsprechend der Next Hop Weiterleitung: Adresse 1 wird die Adresse des Next Hop MP (RA), die er seiner Forwarding Tabelle entnimmt. In das Adressfeld 2 (TA) schreibt er seine eigene MAC Adresse. Danach geht das Frame zur Weiterleitung in die Sende-Queue und muss warten, bis der Kanal frei ist.

Ist die Adresse 3 eines empfangenen Frames die eigene MAC Adresse des Mesh Points, entscheidet er anhand des Address Extension Mode Feldes, ob es ein Kontroll-Frame (Multihop Action) oder ein Datenframe ist. Die Werte „00" oder „01" bedeuten Kontrollframe, in dem Fall reicht der Mesh Point das Frame an seine eigenen höheren Protokollschichten weiter. Die Werte „10" oder „11" bedeuten Datenframe, hier ist die Entscheidung über die weitere Bearbeitung etwas komplexer.

Ist der Mesh Point selbst das Ziel (Mesh DA = DA), wird verfahren wie bei Kontrollframes: er reicht es nach oben durch und leitet nicht weiter. Ist die DA nicht die MAC Adresse des MP aber er ist ein Proxy (z.B. ein MAP mit assoziierten WLAN-Clients oder ein Portal), so soll der Mesh Point als erstes prüfen, ob die Adresse 5 (DA) einer Station gehört, für die er als Proxy arbeitet. In diesem Fall entfernt er den Mesh Header, formatiert das Frame entsprechend neu und gibt es in die Sende-Queue in Richtung Zielstation.

Ist der Mesh Point ein Root MP, so muss er entscheiden, ob er das Frame auf einen anderen Mesh Pfad weiterzuleiten ist. In diesem Fall setzt der Root MP zusätzlich zu den Next Hop MAC Adressen auch die Mesh DA und Mesh SA Adressen neu. Ist ein Mesh Point gleichzeitig Root MP und Proxy MP, so soll er zuerst prüfen, ob die Proxy Weiterleitung anzuwenden ist, danach soll er die Weiterleitung auf einen neuen Mesh Pfad prüfen.

3.4 IEEE 802.11s Überlastkontrolle

Überlastprobleme in Mesh Netzwerken erfordern besondere Aufmerksam-

Unterstützte Frames	Adress Extension Mode Wert (binär)	Adresse 1	Adresse 2	Adresse 3	Adresse 4	Adresse 5	Adresse 6
Mesh Data	00	RA	TA	DA = Mesh DA	SA = Mesh SA	Nicht vorhanden	Nicht vorhanden
Multihop Action	01	RA	TA	DA = Mesh DA	SA = Mesh SA	Nicht vorhanden	Nicht vorhanden
Mesh Data	10	RA	TA	Mesh DA	Mesh SA	DA	SA
Multihop Action	11	RA	TA	Mesh DA	Mesh SA	DA	SA

Abbildung 3.8: Gültige Adress-Formate für Mesh Datenframes und Multihop Protokollframes

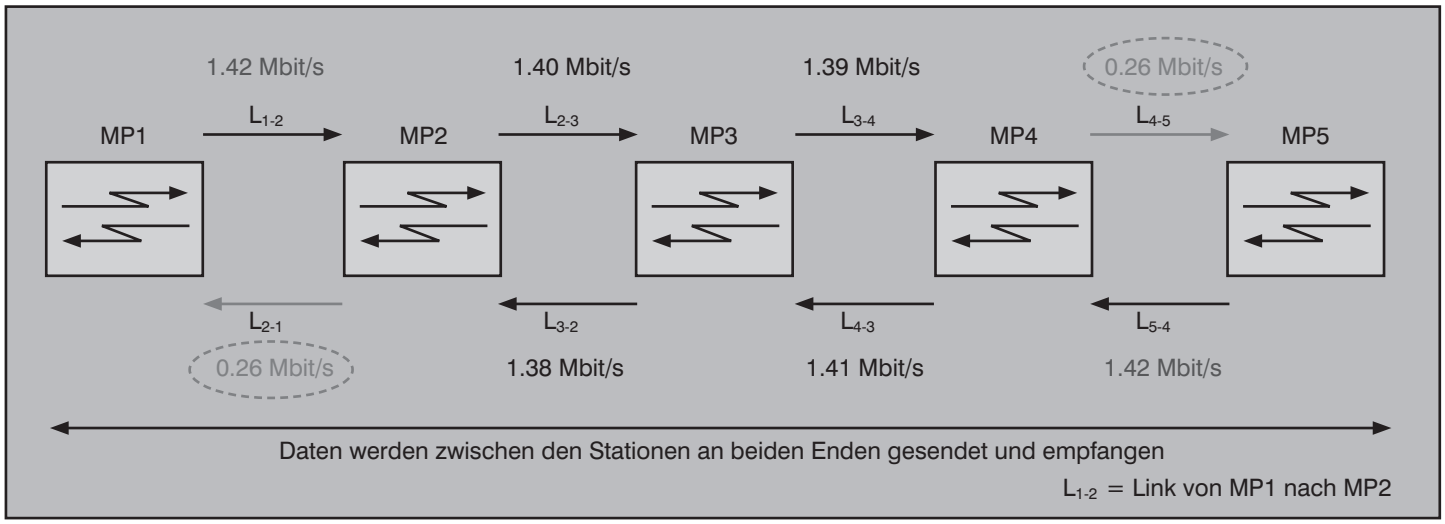


Abbildung 3.9: Überlast an unterschiedlichen Punkten in Sende- und Empfangsrichtung

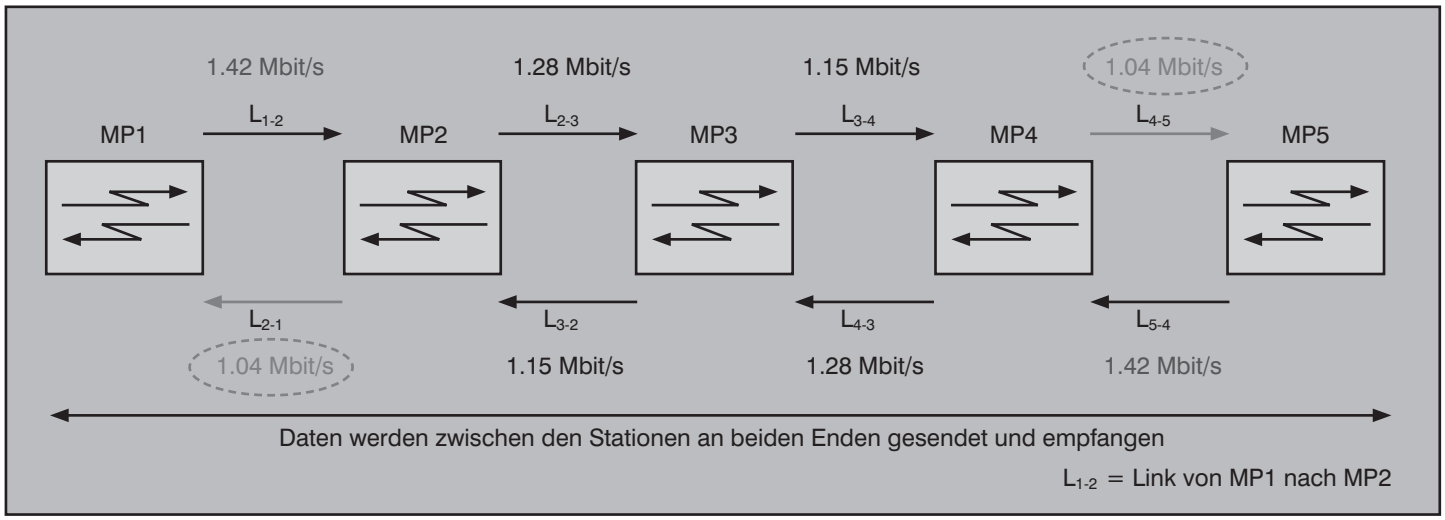


Abbildung 3.10: Gleichmäßige Degradierung bei Hochlast und Kollisions-Overhead

keit, da ein einzelner überlasteter Mesh Point mitten in einer Masche die Durchsätze auf allen Ende-zu-Ende-Wegen, die über ihn verlaufen, massiv nach unten drückt. Dies gilt unabhängig in Sende- und Empfangsrichtung, wie Abbildung 3.9 zeigt. In diesem Beispiel haben beide Richtungen Ende-zu-Ende nur einen Durchsatz von 0,26 Mbit/s. Weist die Masche insgesamt eine hohe Last auf, so entsteht aufgrund der Shared LAN Technik an jedem Knoten durch Kollisionen zusätzlicher Overhead. So ergibt sich eine schleichende Degradierung, die sich Ende-zu-Ende aufsummiert. Im Beispiel der Abbildung 3.10 sinkt der Durchsatz bei 10% Hochlast-Overhead je Knoten auf einem Weg mit 5 Hops von 1,42M auf 1,28M, dann auf 1,15M und schließlich mit 1,04M schon auf 73% des Eingangs-Durchsatzes. Überlastkontrolle ist also eine ganz wichtige Anforderung für Mesh WLANs. Um zu vermeiden, existierende IEEE 802.11 Basis-Standards abzuändern, wurde ein Verfahren entwickelt, das darauf basiert, die Senderaten zwischen jeweils zwei benachbarten Mesh Points anzupassen.

Überlastkontrolle nutzt drei Elemente:

- Lokales Monitoring auf Überlast
- Erkennen von Überlast und Signalisierung (Anzeige) der Überlast
- Lokale Kontrolle der Senderate

IEEE 802.11s spezifiziert ein Default Überlast-Protokoll (Congestion Control Protocol), das eine Signalisierung von Überlast ermöglicht. Der Einsatz beliebiger herstellereigener Protokolle ist zusätzlich erlaubt. Innerhalb einer Masche darf jedoch nur ein gemeinsames Protokoll aktiv sein, die Mesh Points müssen sich entsprechend einigen, welches Protokoll sie nutzen.

Die Spezifikation, „wie“ die Überlast erkannt wird, d.h. lokale Monitoring Parameter, Überlast-Bedingungen und Trigger-Werte ist aktuell bei IEEE 802.11s „out of scope“ und muss von den Herstellern selbst implementiert werden.

Ein Mesh Knoten, der eine Überlast erkennt, kann (nicht: muss) ein Kontrollframe, mit folgenden Angaben senden

- geschätzte Dauer der Überlast je Access Kategorie (AC gem. IEEE 802.11e)
- weitere herstellereigene Informationen sind erlaubt

Erhält ein Knoten eine Überlast-Anzeige, so kann er eine Ratenanpassung in Richtung des überlasteten Knotens durchführen. Auch hier sind derzeit keine Parameter-Regelungen bei IEEE 802.11s

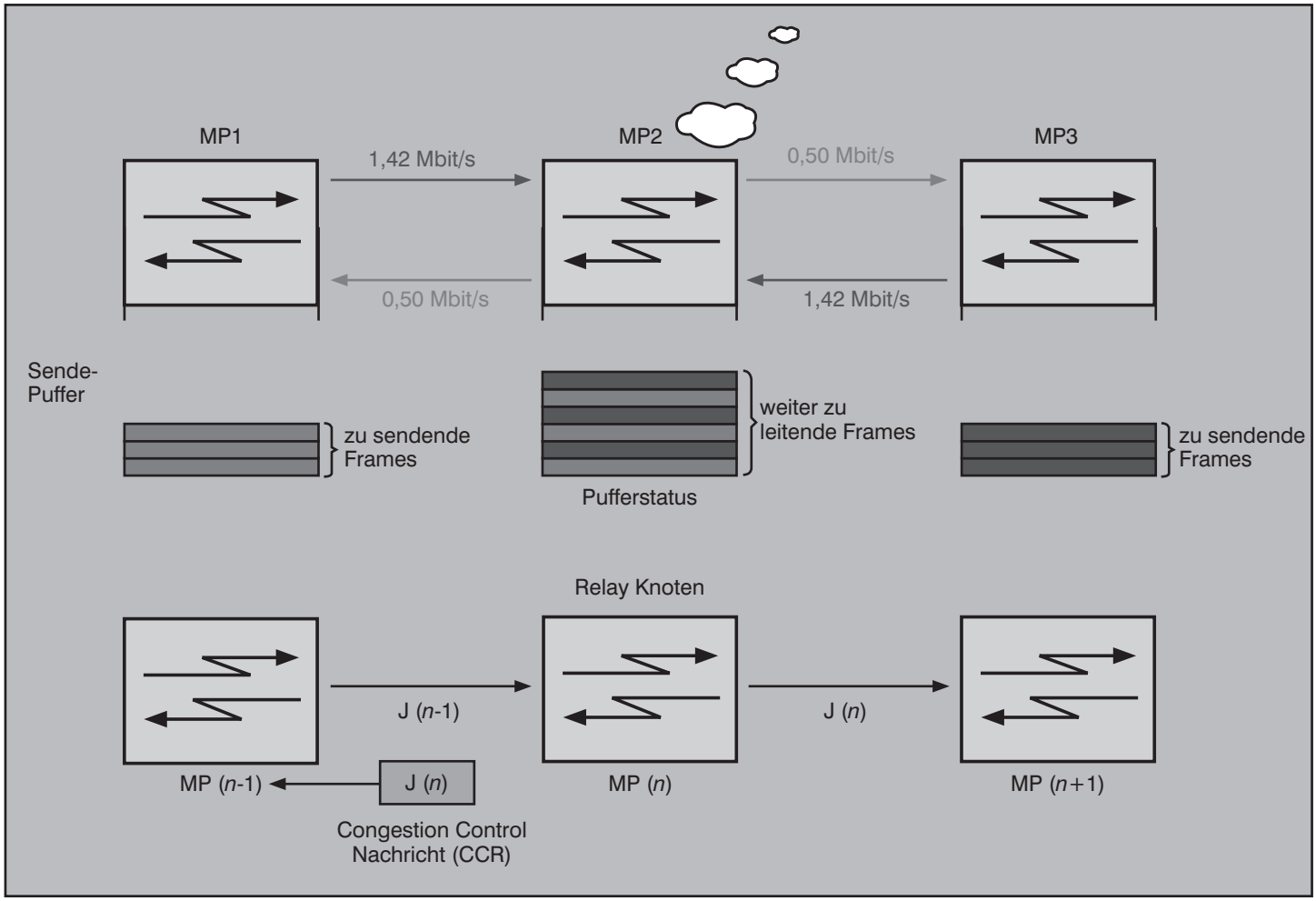


Abbildung 3.11: Überlastkontrolle nach IEEE 802.11s

getroffen, die Anpassungs-Schritte muss der Hersteller selbst festlegen.

Das Prinzip der so festgelegten Überlastkontrolle ist in Abbildung 3.11 verdeutlicht: Der Mesh Point 2 hat in beide Richtungen eine Überlast. Er sendet Congestion Control Requests in der Hoffnung, dass seine Nachbar-Knoten daraufhin ihre Senderate drosseln. Das Drosseln kann leider bei den Nachbarknoten zu einer Überlast führen, da sie ihre eigenen Frames nicht mehr so schnell loswerden. In der Folge senden sie ihrerseits an die weiter außen liegenden Nachbarknoten Congestion Control Requests. So wird die Überlast immer weiter an den Rand der Masche zurückgedrängt und vom Zentrum der Überlast aus nach außen erfolgt die gewünschte Entlastung. Insbesondere bei höheren Datenraten zeigen Messungen deutlich bessere Durchsatz-Ergebnisse bei aktivierter Überlastkontrolle (siehe Abbildung 3.12).

3.5 Power Management

Zur Energie-Einsparung und Erhöhung der Betriebszeiten spezifiziert IEEE 802.11s optional Power Management Funktionen wie Power Save und Automatic Power Safe Delivery (APSD).

Der Standard unterscheidet hier aktive und passive Knoten: Power Save Capability bedeutet: Der Knoten kann in den PS Modus gehen. Power Save Support Capability bedeutet: Der Knoten unterstützt es, dass sein(e) Nachbar(n) in den PS Modus gehen.

Ein Knoten, der in den PS Modus geht, muss vorher alle seine Nachbarn informieren. Er darf nur dann tatsächlich in diesen Modus gehen, wenn alle seine Nachbarn dies unterstützen. Um seinen Wunsch anzuzeigen, sendet er per Unicast ein Null-Data Frame an alle Peers. Danach muss er die Bestätigung durch ALLE Nachbarn abwarten (im Bestätigungs-Frame ist das PS Support Enable Bit = 1 gesetzt).

Knoten, die PS-Nachbarn sind, wählen eine intervallmäßige „Aufwach-Periode“ aus (mit APSD TSPEC). Ein Knoten mit einem Power Save Nachbarn, der gerade im PS Modus ist, puffert alle zu sendenden MAC Frames (MSDU‘s) und kündigt zum „Aufwachzeitpunkt“ das Senden mit einem DTIM Beacon an (Delivery Traffic Indication Message). Der Knoten im PS Modus muss zum Aufwach-Zeitpunkt auf entsprechende Beacons lauschen und bei Erhalt eines DTIM Beacons auf Datenempfang gehen.

4. Offene Punkte und Fazit

Alle aktuell verfügbaren Lösungen sind proprietär. Soweit Client Systeme als Mesh Points integriert werden, sind deren Leistungsparameter im Regelfall eine starke Limitierung des Mesh Netzwerks hinsichtlich Durchsatz, Reichweite / Sendeleistung, Stromversorgung / Stromleistung (Lebensdauer), Verarbeitungskapazität für Routing Informationen, Forwarding Kapazität für Fremdpakete. Die auftretende Verkehrslast am einzelnen Mesh Point durch Autodiscovery, Routing Updates für alle Nachbarn (ggf.

Vermaschte Wireless Netze: Funktionsweise, Technologien, Standardisierung unter IEEE 802.11s - Teil 3

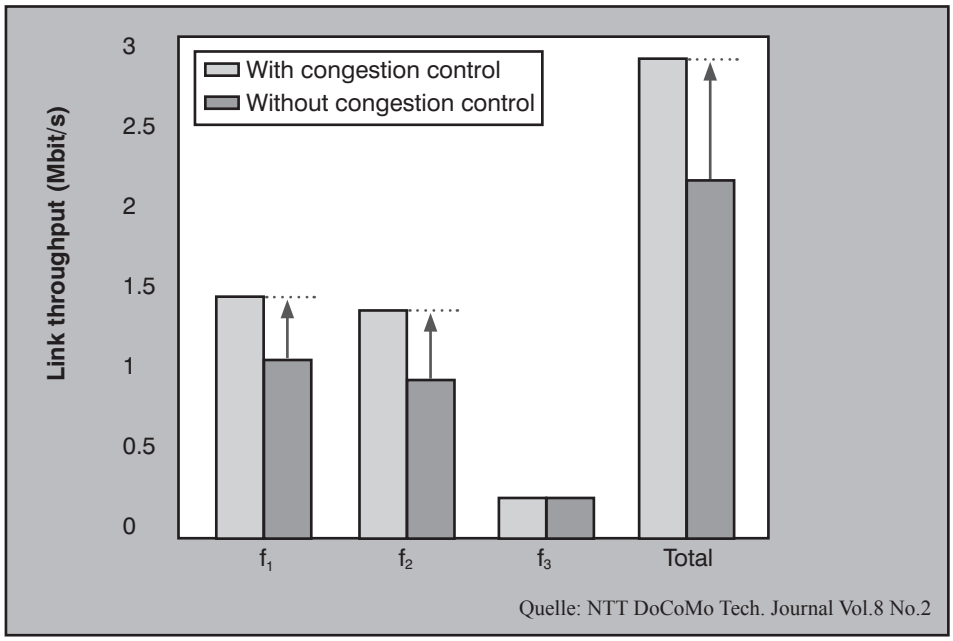


Abbildung 3.12: Durchsatz-Messungen mit und ohne Überlastkontrolle

auch noch auf einem gemeinsamen Kanal) und Forwarding kann zu Leistungsengpässen führen und in der Folge den Durchsatz Ende-zu-Ende beeinträchtigen. Bei Einsatz einer zu niedrigen Anzahl Radios entstehen solche Leistungsengpässe sehr schnell.

Insbesondere Outdoor AP's sind mit bis zu 4.500,- EUR sehr teuer, indoor AP's liegen bei Faktor 2 bis 3 im Vergleich zu non-Mesh AP's.

Fazit

Mesh WLAN's sind in vielfältigen Einsatzszenarien denkbar, insbesondere für City-Netze, ad hoc Szenarien und Standortbereiche, die gar nicht verkabelbar sind. Für die Zukunft entsteht mit dieser Technologie ein hohes Potenzial, Verkabelungsstrukturen durch Funkverbindungen zu ersetzen. Aktuell ist die Technik allerdings noch jung, und alle verfügbaren Produkte arbeiten mit proprietärem Mesh Routing. Die Standardisierung IEEE 802.11s wird noch bis mindestens 2009 auf sich warten lassen.

Die erreichbaren Datenraten sind vor einer breiten Verfügbarkeit von 802.11n keinesfalls vergleichbar mit verkabelten Inhaus-Technologien. Sie sind jedoch als alternative Last Mile Technologie interessant, insbesondere um etablierte Verkabelungs-Provider oder Neuverkabelungs-Kosten zu umgehen.

Abkürzungen

AC	Access Category
AP	Access Point
APSD	Automatic Power Save Delivery
DA	Destination Address
DTIM	Delivery Traffic Indication Message
HWMP	Hybrid Wireless Mesh (Routing) Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
LIFO	Last In First Out
MAC	Media Access Control
MAP	Mesh Access Point
MP	Mesh Point
MPP	Mesh Point & Portal
MSDU	MAC Service Data Unit
PS	Power Save
RA	Receiver Address
SA	Source Address
TA	Target Address
TSPEC	Transmission Specification

Links

www.accton.com
www.belairnetworks.com
www.cisco.com
www.dlink.de
www.firetide.com
www.interdigital.com
www.motorola.com
www.motorola.com/mesh
www.nexthop.com
www.nortel.com
www.packethop.com
www.sohoware.com
(TrueMesh technology)
www.strixsystems.com
www.thomson.net
www.tropos.com
www.ieee.org/11
www.ieee.org/16
www.wimaxforum.org
www.wi-mesh.org

Kongress

Voice- und Video-Forum 2008
10.11. - 13.11.08 in Königswinter

Das ComConsult Voice- und Video-Forum ist die ComConsult-Spitzenveranstaltung des Jahres 2008. Wir analysieren die technische Entwicklung der IP-Telefonie hin zu neuen Architektur-Formen, bewerten die Strategien der führenden Hersteller und geben einen tiefen Einblick hinter die Kulissen von Markt und Produkten. Auch in diesem Jahr wird das ComConsult-Voice-Forum von exklusiven Untersuchungen von ComConsult-Research begleitet, die nur den Teilnehmern dieses Forums zugänglich sind.

Moderation: Dr. Jürgen Suppan
Preis: € 2.090,- zzgl. MwSt.* (*gültig bis 15.09.08 - dann regulär € 2.290,- zzgl. MwSt.)

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

EMV-Seminare

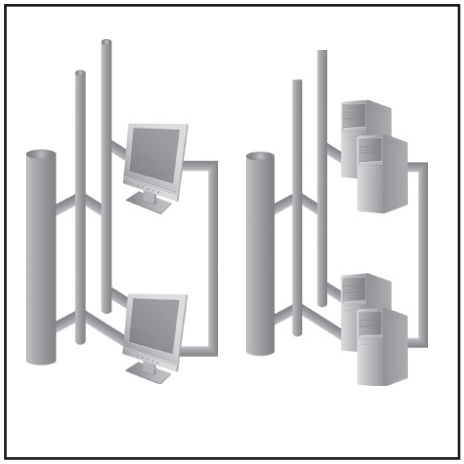
Seminare zur Elektromagnetischen Verträglichkeit

Die ComConsult Akademie veranstaltet vom 29.10. - 30.10.08 ihr Seminar „Elektrische Störungen in Datennetzen und Computerinstallationen erfolgreich erkennen und beseitigen“ in Bonn.

In den letzten Jahren lassen sich verstärkt Störungen und Schäden in Netzwerken und DV-Installationen feststellen. Komplexe Netzanalysegeräte, die Spannungsspitzen aufzeichnen, ergeben keine Hinweise auf den Ursprung der Störungen.

Sie erfahren in diesem 2-tägigen Seminar, welche typischen Ursachen den in den letzten Jahren festgestellten Störungen und Schäden in Netzwerken und DV-Installationen zu Grunde liegen, wie gefährlich diese Störungen sind und wie sie messtechnisch erkannt und beseitigt werden können.

Sie lernen in der Praxis, wie Neubauten mit EDV-Räumen geplant werden können und bestehende Anlagen so zu ertüchtigen und anzupassen, dass die zu betreibenden EDV-Anlagen einwandfrei funktionieren. In kleinen Trainings-Gruppen werden die praktischen Erfordernisse an Modellen vorgeführt und sofort in bestehenden realen Anlagen gemeinsam untersucht.



Die ComConsult Akademie veranstaltet vom 02.12. - 03.12.08 ihr Seminar „EMV-gerechte Planung der Elektroinstallation für Rechnerräume und Rechenzentren“ in Bonn.

Das Zusammenspiel von allgemeiner Stromversorgung, Computer- und Nachrichtentechnischen Anlagen, Beleuchtungen und Sicherheitssystemen ist heute eine komplexe Aufgabe geworden. Vergleichsweise kleine Installations- und Wartungsfehler können unvermutet große Wirkungen zeigen. Diese reichen von instabilen Stromversorgungen, unklaren Ausfallerscheinungen von Netzwerken und Servern bis hin zu korrodierenden Rohrleitungssystemen.

Dieses Seminar zeigt, wie eine EMV-gerechte, hochverfügbare und störungsarme Elektroinstallation mit gleichzeitig hoher Betriebssicherheit geschaffen werden kann. Es vermittelt mit engem Bezug zur Praxis wie ausgehend von Analyse und Messtechnik bestehende Mängel beseitigt werden und ein wartungsoptimierter Betrieb aufgebaut wird.

Jeder Teilnehmer erhält ergänzend zu den regulären Seminarunterlagen bei Kursantritt kostenlos das Handbuch „Design, Planung und Installation“ von 3M Telecommunications.

Der Referent dieser Seminare ist Dipl.-Ing. Karl-Heinz Otto, Elektroinstallateurmeister, Elektro-Ingenieur und Dipl.-Wirtschafts-Ingenieur. Öffentlich bestellt und vereidigt seit 1981, tätig als Berufssachverständiger Leiter der Bundesfachgruppe „Elektronik und EDV“ im BVS. Herr Otto ist öffentlich vereidigter und bestellter Sachverständiger für elektrische Niederspannungsanlagen, Leistungs- und EDV- Elektronik.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche das Seminar

Elektrische Störungen in Datennetzen und Computerinstallationen erfolgreich erkennen und beseitigen
☐ 29.10. - 30.10.08 in Bonn
zum Preis von € 1.390,- zzgl. MwSt.

EMV-gerechte Planung der Elektroinstallation für Rechnerräume und Rechenzentren
☐ 02.12. - 03.12.08 in Bonn
zum Preis von € 1.390,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Zimmer
vom_____ bis_____ 08

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

Ab der 2. teilnehmenden Person zahlen Sie nur noch 990,-- € zzgl. MwSt.

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift
Vorname (2. Person)	Nachname (2. Person)
eMail	Telefon/Fax

Schwerpunktthema

Digitale Kameras im Netzwerk

Fortsetzung von Seite 1

Im Anschluss an sein Studium als Nachrichtentechniker spezialisierte sich Dipl.-Ing. Hartmut Kell auf die Datenkommunikation in lokalen Netzen und kann bis heute auf eine mehr als 15-jährige Berufserfahrungen in diesem Bereich 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.

Eine Diskussion der Vor- und Nachteile der Netzwerk-Video-Technik im Vergleich zur klassischen analogen Technik soll dabei weniger im Vordergrund stehen, da hierzu bereits ausreichende Informationen in einschlägiger Literatur zu finden sind.

Die Videoüberwachungstechnik oder „Closed Circuit Television" CCTV besteht in der klassischen wie auch in der „digitalen" Technik grundsätzlich aus den Elementen der Bildaufnehmer, also den Kameras, einem Medium zum Transport des Bildes bzw. Videos zu einer auswertenden Einheit, der oder den auswertenden Einheiten und Medien zur längeren Speicherung der Bilder und Werkzeugen zur Steuerung oder Konfiguration der Kameras, jeweils inklusive zugehöriger Software. Der Primärunterschied zwischen den Netzwerk-Lösungen und der klassischen besteht im Wesentlichen darin, dass unterschiedliche Transportmedien verwendet werden. Die „ursprüngliche" Variante sah bzw. sieht die Verwendung von Koaxialkabel vor, in der „modernen" Variante dagegen wird dieses durch Medien ersetzt, die im lokalen Netzwerk üblich sind. Dazu gehören natürlich Kupfer- sowie Glasfasermedien, alternativ auch drahtlose Technik. Zwischen diesen beiden Lösungen existiert eine Mischvariante, die Hybrid-Lösung. Diese ist gerade in Umgebungen mit vorhandenen analogen CCTV-Lösungen von Bedeutung; im Falle einer sanften Migration wird zur netzwerkbasierenden Technik häufig ein Parallelbetrieb häufig erforderlich sein. Die aufgelisteten Elemente, die im Rahmen einer netzwerkbasierenden Lösung notwendig sind, und deren Einfluss auf das Netzwerk selbst werden nachfolgend beschrieben.

Kamera

Beginnend mit dem offensichtlichsten Element einer Videokameraüberwachung, der Kamera selber, ist in Zusammenhang mit den typischen, innovativen Schlagwörtern „Digitale Videoüberwachung" zunächst einmal festzustellen, dass der Begriff „digital" nicht eindeutig genug die Art der Technik beschreibt, die derzeit im Zusammenhang mit der weiten Verbreitung von Netzwerken vermarktet wird. Digitale Kameras gab es schon vor der Möglichkeit der Nutzung der Videoübertragung über Lokale Netzwerke, denn auch Kameras mit Koaxialkabelanschluss verwenden eine interne digitale Bildverarbeitung (z.B. zur Rauschunterdrückung oder auch Bewegungserkennung). Das Bild bzw. Video wird bei dieser digitalen Variante jedoch nicht auf eine Netzwerk-Schnittstelle ausgegeben, sondern in einer analogen Form auf einem Koaxialkabelanschluss. In dem Bemühen um eine eindeutige Definition muss festgestellt werden, dass in der Literatur bereits Fachautoren häufig daran scheitern, den Begriff „digitale CCTV-Kamera" klar zu begrenzen. Deshalb beschränkt sich auch dieser Artikel auf die folgende, nur unzureichende Festlegung:

Digitale CCTV-Kameras stellen an ihrem Ausgang Bilder in digitaler Form zur Verfügung, wobei die „digitale Variante" weiter auf eine paketbasierende Form festgelegt werden kann, wie sie z.B. Lokale Netzwerktechnik mit Hilfe des Internet-Protokolles anbietet.

Jedes Videosystem kann logischerweise nur so gut sein, wie die Aufnahme und auch die Weitergabe der Kamera es zulässt. Die meisten Leser haben sich bereits im Umfeld der privaten digitalen Fotografie mit dem Begriff der Bildauflösung beschäftigt. Beispiele zur Unterscheidung

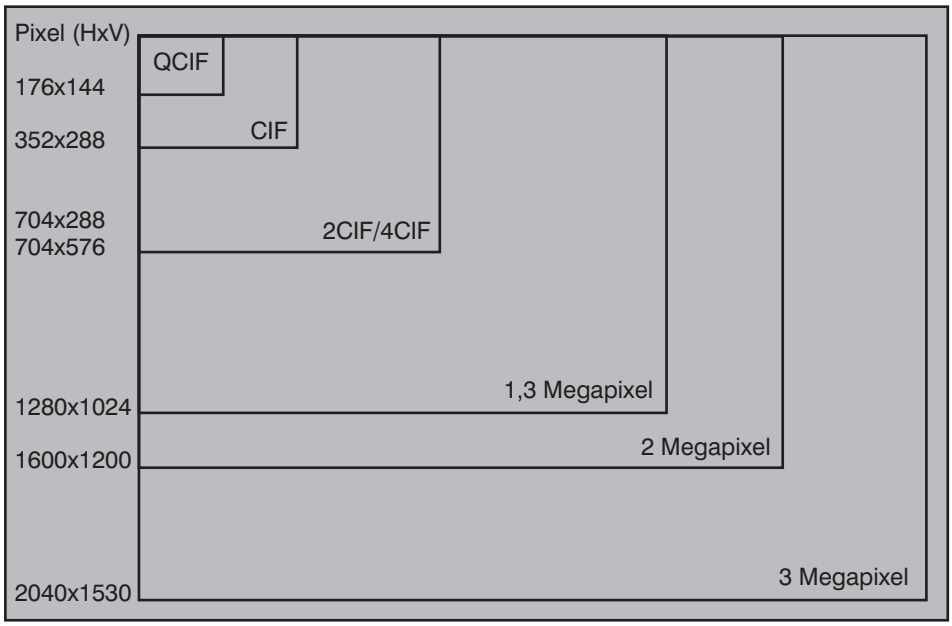


Abbildung 1: Typische Bildformate – PAL und Megapixel

der Formate QCIF, CIF, 2CIF, 4CIF etc. sind im Internet vielfältig vorhanden und eine Bewertung der Leistungsfähigkeit des „richtigen“ Formates soll im vorliegenden Artikel weitestgehend vermieden werden. (siehe Abbildung 1)

Eine pauschale Leistungsbewertung und Vergleichbarkeit ist ohne den Kontext der konkreten Anforderung und der zum Teil subjektiven Bewertung durch die das System nutzenden Personen nur schwer möglich. Zur Erzielung einer den analogen Kameras vergleichbaren Studionorm-Qualität wird das 4CIF-Format (704 x 576) mit einer Bildrate von 25 Bildern/s (fps) zumeist als Basis definiert. Dabei bedeutet diese Aussage aber nicht, dass genannte Auflösung und Bildrate grundsätzlich zur sinnvollen Nutzung von Videoüberwachung gefordert werden muss (weitere Erläuterungen später). (siehe Tabelle 1)

Unterschiedliche Formate führen zu unterschiedlichen Informationsmengen und damit zu divergierenden Anforderungen an die Übertragungskapazität des Netzes bzw. die Speicherkapazität der Server. Die durch die interne Digitalisierung der Kamera erzeugten „Rohdaten“ lassen sich mittels Komprimierungstechniken innerhalb der Kamera noch weiter reduzieren; im Beispiel des hochauflösenden 4CIF-Formates von 116 Mbit/s (Annahme: 25 Bilder/s) auf unter 6 Mbit/s. Bei den Kompressionsverfahren können zwei Hauptgruppen unterschieden werden: vereinfacht formuliert wird bei „Einzelbildverfahren“ jedes Bild autark für sich von der Kamera komprimiert und übertragen; bei „Bewegtbildverfahren“ erfolgt eine Komprimierung einer kompletten zusammenhängenden Sequenz.

Der bekannteste Vertreter der Einzelbildverfahren ist das M-JPEG-Verfahren (Motion Joint Expert Group). Dieses codiert jedes einzelne Bild auf Basis des bekannten JPEG-Verfahrens, unabhängig von dem vorausgehenden oder nachfolgenden Bild. Dabei kann bei höchstwertigen Systemen in Abhängigkeit des beobachteten Ereignisses die Komprimierung variiert werden; schlägt ein Bewegungsmelder im überwachten Bereich nicht an, so erfolgt eine hohe Komprimierung, bei Verfolgung eines erfassten Objektes wird die Komprimierung reduziert. Dies ist auf der einen Seite eine Stärke des Verfahrens, denn jedes Bild ist autark und der Verlust der vorausgehenden/nachfolgenden Bilder hat keinerlei Einfluss auf die Nutzbarkeit der Informationen dieses Bildes. Da die Rechenfunktion in der Kamera diese Bildabhängigkeiten nicht mit berechnen muss, ist das M-JPEG-Verfahren innerhalb

Format	Auflösung (HxV)	Komprimierte Bitrate
SQCIF	128 x 96	0,16 Mbps
QCIF	176 x 144 (PAL)	0,36 Mbps
CIF	352 x 288 (PAL)	1,45 Mbps
2CIF	704 x 288 (PAL)	2,8 Mbps
4CIF	704 x 576 (PAL)	5,8 Mbps
16CIF	1408 x 1152 (PAL)	23 Mbps
VGA	640 x 480	8,8 Mbps
SVGA	800 x 600	14 Mbps

Tabelle 1: Vergleich der Übertragungsrate (Basis: MJPEG-Kompression 1:20)

der Kamera sehr schnell. Der Nachteil besteht darin, dass redundante Informationen von aufeinander folgenden Bildern nicht berücksichtigt werden. Bewegt sich z.B. das zu beobachtende Objekt vor einem gleich bleibenden Hintergrund, so wird sich Letztgenannter im Prinzip bei allen Bildern kaum verändern. Man könnte diese „Hintergrundinformation“ einmal übertragen und anschließend durch einen Rechenprozess zu mehreren Einzelbildern hinzupacken, um damit die Bewegung darzustellen. Diese fehlende Berücksichtigung von redundanten Bildinformationen bei M-JPEG führt dazu, dass die Komprimierung nicht so effektiv ist wie bei Bewegtbildverfahren der Variante MPEG (Motion Picture Expert Group).

Bei diesen werden aufeinander folgende Bilder in der Kamera verglichen, und die Informationen, die innerhalb einer Sequenz von Bildern identisch sind, nur einmal übertragen. Der Empfänger setzt dann aus den Informationen der Gesamtsequenz ein Video zusammen, welches alle Informationen im bewegten Bild wiedergibt. Dies erhöht die Kompressionsrate und reduziert damit die benötigte Datenrate im Netzwerk und den Speicherbedarf. Auf die Beschreibung der Unterschiede der verschiedenen Bewegtbildverfahren (MPEG-1, MPEG-2, MPEG-4, H.264) wird verzichtet, es soll bei dem Hinweis belassen sein, dass das MPEG4-Verfahren eine Qualität wiedergibt, die für den Studio-Bereich entwickelt worden ist und von den Herstellern von CCTV-Kameras als Standard für Bewegtbildverfahren angeboten wird. Größere Bedeutung als die bessere Komprimierung kommt demgegenüber den weiteren Vorteilen des Einzelbildverfahrens zu:

- Da bei der Videoüberwachung in den meisten Fällen nicht die Bewegung im

Kongress

Rechenzentrum Infrastruktur-Redesign Forum 2008
24. - 26.11.08 in Königswinter

Unsere Rechenzentren befinden sich inmitten einer der größten Redesign-Phasen der letzten 20 Jahre. Die wesentlichen Treiber dieses Redesigns sind: Server-Konsolidierung, Speicher-Konsolidierung, neue IT-Architekturen, mehr und mehr Web-basierte Applikationen.
Rechenzentren-Redesign bedeutet dabei vor allem ein Redesign der Infrastrukturen. Im Mittelpunkt stehen dabei: Netzwerke, Speicher-Systeme, Verkabelung, Strom und Klima

Das ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2008 stellt sich diesem herausragenden Thema.

Moderation: Dr. Jürgen Suppan
Preis: € 2.290,- zzgl. MwSt.

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

Vordergrund steht, sondern die Informationsdetails der einzelnen Bilder, ist es nahe liegend, dass gerade den CCTV-Anwendungen die Abspeicherung der Einzelbilder auf dem Videoserver entgegenkommt. Jedes einzelne Bild kann geladen werden und in jedem stecken sämtliche Informationen. Die Recherche und Bearbeitung von Bildinhalten bei Einzelbildverfahren, wie z.B. dem M-JPEG-Verfahren, wird vereinfacht. Selbst Standard-Windows-Programme erlauben die einfache Betrachtung von abgespeicherten JPEG-Bildern.

- Verluste von einzelnen Bildern durch Netzwerkübertragungsfehler erlauben weiterhin die Auswertung des Videos, im Extremfall hat man kurze „Ruckler" im Bewegtbild. Bei MPEG-Verfahren lässt der Verlust ganz bestimmter Bilder der Videosequenz eine Wiederherstellung letzterer am Empfänger gar nicht mehr zu.

- Jedes M-JPEG-Bild kann mit Textdaten ergänzt werden, die weitere Informationen zum aufgezeichneten Ereignis liefern und bei der Speicherung der Videos in eine eigene Datenbank übernommen werden. Die Ergänzung eines flüssigen MPEG-Videostromes mit derartigen Zusatzdaten und die anschließende Recherche im Bewegtbildstrom bringen einen höheren technischen Aufwand mit sich. MPEG2 lässt nur grafikbasierende Zusatzinformationen zu und Software-Werkzeuge für die Nutzung der textbasierenden Zusatzinformationen bei MPEG4 sind kaum verbreitet.

- Nachvollziehbar ist, dass die Zusammenfassung und Bewertung von mehreren Einzelbildern innerhalb der Sequenz und der Kamera und einer erst dann erfolgenden Übertragung zu höheren spürbaren Latenzzeiten führen kann. Man stelle sich bei Betrachtung eines Live-Videos mit einer bewegbaren Kamera vor, dass diese Bewegung durch den Nutzer immer dem eigentlichen realen Bewegungsablauf vor der Kamera „hinterherhinkt".

- Gerade im Zusammenhang mit Kameras, die bewegt werden sollen, verliert natürlich das Bewegtbildverfahren einen Teil seiner Vorteile: Durch die Bewegung der Kamera verändert sich der Hintergrund und damit auch ein Großteil der redundanten Informationen. Die Komprimierung verliert an Effektivität.

Auf der anderen Seite darf der Fall nicht vergessen werden, dass neben der visuellen Übertragung von Informationen bei Bedarf auch der Transport akustischer Daten sinnvoll sein kann. In diesem Falle spielen gerade die für die Belange des TV-Bereiches entwickelten MPEG-Verfahren ihre Stärke aus. Eine Lösungsumsetzung mit reiner M-JPEG-Technik ist kaum denkbar.

Zusammenfassend kann gesagt werden, dass MPEG-Verfahren bei hohen Bildraten von Vorteil sind, da sich in diesem Fall die bessere Komprimierung auszahlt; der Hersteller Axis gibt z.B. als Grenzwert eine Bildrate von mehr als 5 fps an. Deshalb kommt häufig bei Live-Bildern das MPEG- und bei im Hintergrund ablaufender Abspeicherung von wenigen Einzelbildern pro Sekunde das M-JPEG-Verfahren zum Einsatz. Die Betrachtung durch mehrere Nutzer gleichzeitig kann optional mit Hilfe von IP-Multicast-Verfahren durchgeführt werden, auch in diesem Zusammenhang kommt den MPEG-Verfahren eine höhere Bedeutung zu. (siehe Abbildung 2)

M-JPEG und auch die MPEG-Verfahren sind zwar grundsätzlich standardisiert, sie unterscheiden sich bei verschiedenen Herstellern aber in Details, die zu Inkompatibilitäten führen können. Viele Anbieter halten in ihren Kameras beide Verfahren vor, der Hersteller Axis arbeitet sogar mit einer Kombination aus beiden: Die Permanent-Aufzeichnung erfolgt mit variabler bzw. dynamischer Bildrate mit hoher Auflösung über das M-JPEG-Verfahren; eine Aufschaltung des Live-Bildes auf den oder die Beobachtungsplätze wird dann mit dem parallel laufenden MPEG4-Verfahren in niedrigerer Auflösung durchgeführt. Mobotix geht einen völlig eigenen Weg mit dem proprietären MxPEG-Verfahren, dieses erlaubt eine weitere zusätzliche Komprimierung um 80% im Vergleich zum MJPEG unter Nutzung einiger der Vorteile des MPEG-Verfahrens (wie z.B. Audio-Übertragung).

Signalübertragung

Wie beschrieben stellt das M-JPEG-Verfahren bei der Betrachtung der benötigten Datenrate den Worst-Case dar, dieses soll nachfolgend als Basis zur Herleitung der zu erwartenden Datenraten herangezogen werden. Zunächst einmal ist zu ermitteln, welches Datenvolumen das einzelne Bild erwarten lässt. Jeder digitale Hobby-Fotograf kann selbst einmal mit eigenen Fotos experimentieren um festzustellen, wie die Qualität durch Komprimierung der Bilder sinkt. Die Komprimierung eines Bildes mit einer Größe von 640x480 (entspricht z.B. einer VGA-Qualität) um 80% führt nach Aussage eines Kameraherstellers zu einer „geringen Qualität", eine Komprimierung um 50% wird noch als gut empfunden und die Bildqualität bei einer Komprimierung um 20% als hoch bezeichnet.

Unter der Annahme einer mittleren Bildqualität ist mit einer durchschnittlichen Bildgröße von 35 kByte zu rechnen, die daraus resultierende Nettodatenrate (also ohne Netzwerk-Overhead) ist leicht selbst zu ermitteln, wenn man die geforderte Bildrate entsprechend multipliziert. Beispielsweise erfordert ein M-JPEG-Strom mit 12 Bildern/s eine Nettodatenrate von 3,36 Mbit/s, dies ist zu ergänzen um einen pauschalen Overhead für IP-Über-

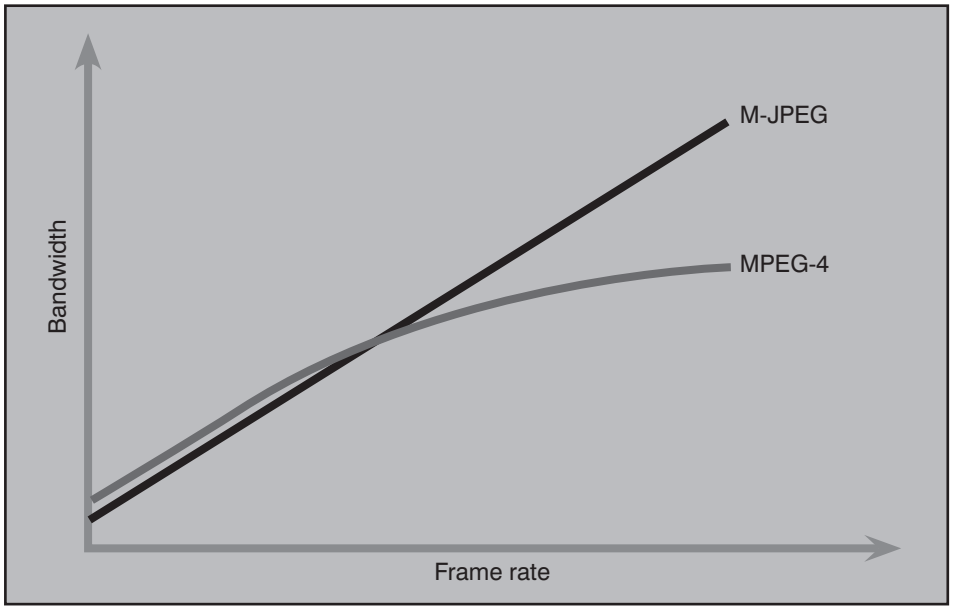


Abbildung 2: Zusammenhang Bildrate und Netzwerklast (Quelle: AXIS)

tragung von ca. 20%. Damit belegt eine Videokamera im Netzwerk mit einem M-JPEG-basierenden Komprimierungsverfahren für 12 Bilder/s ca. 4 Mbit/s. Zum Vergleich: Das MxPEG-Verfahren der Firma Mobotix kommt mit ca. 1 Mbit/s aus, ein MPEG4-Verfahren benötigt ca. 2 bis 3 Mbit/s, und das noch selten vorzufindende H.264 (MPEG4 Part 10) reduziert die MPEG4-Rate nochmals um weitere 40%. Selbst „ältere“ Netzwerk-Anschlüsse mit „nur“ 10 Mbit/s sollten also kein Problem damit haben. Steigert man die Datenrate auf Videofilm-Qualität mit 25 Bildern/s, reichen diese 10 Mbit/s für das MJPEG-Verfahren ebenfalls knapp aus.

Betrachtet man das gesamte Netzwerk mit den in der Regel verteilten Kameras, so belasten diese das Netzwerk nur gering, selbst unter der Worst-Case-Annahme eines MJPEG-Verfahrens. Spannend wird es jedoch, wenn über die „Zusammenschaltung“ von mehreren Kameras bzw. mehreren Videokanälen nachgedacht werden muss. Diese Einzelströme addieren sich letztendlich im Netzwerk in Richtung des Aufzeichnungssystems (also dem Videoserver). So werden 7 Kanäle noch mit 100 Mbit/s auskommen, 70 Kanäle benötigen aber bereits 1 Gbit/s. Eine Verwendung von anderen Komprimierungsverfahren erhöht die Anzahl der möglichen Kanäle (bei Mobotix z.B um das 3-fache).

Auch die Datenrate am Aufzeichnungssystem selber stellt mit 1 oder gar 10 Gigabit/s als Serveranschluss kein Problem dar. Aber das alleine reicht nicht, denn die Leistungsfähigkeit des Aufzeichnungssystems bezüglich seiner Fähigkeit die Bilder abzuspeichern ist gleichermaßen zu betrachten. Im Allgemeinen liegt hier die Herausforderung, und in Abhängigkeit der geplanten Bildrate und Bildauflösung, die gespeichert werden müssen, ist damit zu rechnen, dass sich mehrere Speicherstationen die Funktion des Aufzeichnens teilen, ein entsprechendes Konzept hat das zu berücksichtigen.

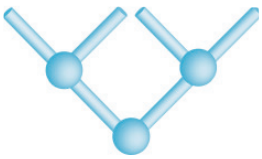
Überlegungen zur benötigten Datenrate sind nur ein Teil der Planung bezüglich des Netzwerkes.Von weiterer Bedeutung ist die Thematik, in welcher Form der komprimierte Videostrom über das Netzwerk übertragen werden kann. Diesbezügliche Überlegungen gibt es bereits für die „normale“ IP-basierende Videoübertragung im TV-Bereich, es wird differenziert zwischen einer dateibasierenden und einer streaming-basierenden Übertragung. Kann Erstere im TV-Bereich noch sinnvoll sein (z.B. Video on Demand), so ist dies für die Videoüberwachung völlig unakzeptabel. Man stelle sich vor, dass sowohl von der Kamera als auch dem Aufzeichnungssystem die auszuwertende Datei mit Hilfe des TCP-Protokolls erst komplett übertragen werden muss, um sie analysieren zu können. Dies würde zum einen viel zu lange dauern und zum anderen die Gefahr deutlich erhöhen, dass bei Fehlern in der Übertragung der Pakete die gesamte Datei beschädigt wird und nochmals übertragen werden müsste, im Extremfall fällt sie als Mittel zur Beweisvorlage vollkommen aus. Es ist nachvollziehbar, dass mit dieser Technik eine Live-Bildübertragung nicht möglich ist, sie könnte - wenn überhaupt - nur für eine deutlich verzögerte nachträgliche Betrachtung sinnvoll sein. Deshalb spielt die Streaming-Technik, die jedem vom Prinzip durch WEB-Anwendungen wie YouTube bekannt ist, auch bei CCTV eine bedeutende Rolle.

Wie bereits mehrfach erläutert, stellt die Übertragungsmenge in einem Lokalen Netzwerk kein Problem dar; anders verhält es sich mit der Latenzzeit bzw. dem Jitter. Zur „sauberen“ Erzeugung eines Live-Videos müssen die ankommenden Einzelbilder zunächst in einen Puffer gepackt werden, der anschließend für einen gleichmäßigen Ausgang der Bildinformation sorgt. Jeder Puffer verursacht Verzögerungen, die sich bei zu großer Ausprägung auch in der Wahrnehmung des Betrachters manifestieren, was jedoch zunächst nicht störend ist (zumindest bei den Videoanwendungen im TV-Bereich). Der Nutzer der Kamera steht aber nicht nur in einer reinen „empfangenden Beziehung“ zum Kommunikationspartner „Kamera“. Er kann diese, z.B. bei PTZ-Kameras (PTZ: Pan, Tilt, Zoom Cameras), auch über horizontale / vertikale Bewegungen oder die Brennweite über Zoom-Objektive steuern. Man stelle sich ein Schwenken oder Zoomen einer Kamera mit dem Ziel, das beobachtete Objekt weiter zu verfolgen, vor, wenn diese Verfolgung dann nur mit einer spürbaren Verzögerung erfolgen könnte. Es ist davon auszugehen, dass immer eine minimale Zeit vergeht, bis das „echte“ Bild auf dem Betrachtungsgerät angezeigt wird, diese beträgt auch bei analogen Kameras bis zu 20 ms, bei digitalen Systemen ist diese noch höher (im Extremfall Faktor 10 - 15). Im Extremfall müsste der Nutzer die Kamera „vorausschauend“ steuern und dies gelingt nur bis zu etwa 100 ms, darüber hinweg leidet die Bedienung von Joystick-Kameras erheblich.

Dieses Problem besteht aber nicht nur bei Live-Bildern, auch eine ereignisgesteuerte Aufzeichnung wird möglicherweise damit Schwierigkeiten haben. Fällt ein zentrales Überwachungssystem oder auch der menschliche Betrachter durch ein erfasstes Ereignis wie z.B. eine Bewegung in einem spezifizierten Bereich die (verzögerte) Entscheidung, die Bildrate zu steigern, so besteht die Gefahr, dass die ersten, in vielen Fällen zur Beweislastermittlung wichtigen Bildsequenzen zu spät aufgenommen werden. Das, was man eigentlich sehen möchte, ist nicht oder nur in einer unzureichenden Qualität aufgenommen worden.

Deshalb ist eine Kombination von großem Puffer, der die Zwischenspeicherung einer hohen Anzahl von gesendeten Einzel-

Seminar



Ethernet-Netzwerke: Techniken, Einsatzgebiete und Betrieb
27.10. - 29.10.08 in Bonn

Dieses Seminar stellt die aktuellen Ethernet-Themen vor und zeigt, wie etablierte und neue Techniken in bereits wohlbekannten und zukünftigen Anwendungsgebieten eingesetzt werden können. Zu den analysierten Sonderanwendungsgebieten gehören insbesondere VoIP, Gefahrenmeldetechniken, Industrienetze und Rechenzentrumsbereiche. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, Planungsregeln vorgestellt, Möglichkeiten und Grenzen von Quality of Service und Risiken durch Fehlentscheidungen bei der Technikauswahl aufgezeigt.

Referenten: Dipl.-Inform. Oliver Flüs, Dipl.-Ing. Hartmut Kell
Preis: € 1.690,- zzgl. MwSt.

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

bildern möglich macht (was z.B. bei einer hohen Qualität gefordert werden würde), und Bewegungssteuerung von Kameras nur schwer sicherzustellen. Eine Abhilfe zur Vermeidung der Notwendigkeit von großen Puffern liefert z.B. die Reduzierung der Bildanzahl bei Live-Übertragungen, selbst unter Akzeptanz einer schlechteren Qualität.

Die Technik zur Erzeugung von Streaming-Daten in einem Videonetzwerk wird weiter unterteilt in Push- oder Pull-Verfahren. Auch hier kann zur Erklärung wieder auf Bekanntes zurückgegriffen werden, denn die Push-Technik ist den meisten Videokonsumenten ein Begriff: Ein Client (also der Betrachter) fordert von der Videoquelle - dies kann die Kamera selbst oder ein Videodatenbankserver sein - das Video an. Als Ergebnis erzeugt die Quelle einen kontinuierlichen Videostrom, der unbestätigt und ungesichert vom Client angenommen wird. Der Betrachter wird demzufolge als rein passiver Nutzer der Videoübertragung angesehen, er greift nicht ein und kann es auch nicht. Diese Technik eignet sich im Falle von hohen Echtzeitanforderungen oder auch bei gleichzeitiger Übertragung des gleichen Videos an mehrere Teilnehmer, dann unter Zuhilfenahme von IP-Multicasting; RTP (Real Time Protocol) ist ein solches Push-Verfahren. Soll das Video jedoch während der Betrachtung angehalten, gegebenenfalls einzelne Elemente bzw. Sequenzen z.B. in Zeitlupe nochmals angesehen oder gar mit Hilfe der Metadaten spezielle Teile des Videos gezielt geladen und betrachtet werden, so wird der Zuschauer wieder zu einem aktiven Teilnehmer an der Videosession. Er muss mit der Videoquelle interagieren. Für diesen Fall wird das Pull-Verfahren bevorzugt eingesetzt. Hier fordert der Client gezielte Bilder oder Bildsequenzen von der Quelle an und diese sorgt dann über entsprechende Quittierungsmechanismen für eine gesicherte Übertragung, die insbesondere bei Nutzung von Videos für die Beweisaufnahme von hoher Bedeutung ist.

Protokolle

Bei den Protokollen stellt sich die Frage, welche der bekannten und neuen Standard-Versionen in einem CCTV-Netz zu erwarten bzw. zu berücksichtigen sind. Beschränkt sich die klassische bzw. kommerzielle Videoübertragung im Wesentlichen auf eine Nutzung von UDP (user datagram protocol), häufig kombiniert mit RTP, so reicht dies für die völlig andere Nutzungsform der CCTV, insbesondere bedingt durch die „aktive“ Rolle des Betrachters, nicht mehr aus. Multimedia-Echtzeit wird wie fast alle Echtzeitanwendungen ohne UDP nicht zu realisieren sein, doch auch TCP hat im Bereich der Videoüberwachung seine Existenzberechtigung. Sind Beweisbilder, möglicherweise noch in Kombination mit wichtigen Metadaten zu übertragen, so kann dies nur mit einem gesicherten Protokoll wie TCP erfolgen. Zum Transfer der eigentlichen Video-, gegebenenfalls kombiniert mit Audiodaten, die durch zusätzliche Mikrofone aufgenommen wurden, wird unter „Echtzeitbedingungen“ neben proprietären Protokollen RTP eingesetzt. RTP lässt nicht die Möglichkeit zu, auf den Stream oder auch auf die Erzeugung des Streams Einfluss zu nehmen; es ist ausschließlich für die Übertragung der „Echtzeitnutzungsdaten“ vorgesehen.

Zur Steuerung des Streams sind zwei ergänzende Protokolle zu betrachten, RTCP (Real Time Control Protocol) und RSTP (Real Time Streaming Protocol). Mit dem u.a. auch bei VoIP eingesetzten RTCP kann das empfangende Netzwerkelement auf das sendende Netzwerkelement Einfluss nehmen. Es liefert Rückinformationen, die zu Maßnahmen auf der Senderseite führen. Beispielsweise kann dieser Videoserver bei einer dynamischen Reduzierung der nutzbaren Bandbreite, die dem Videosender über RTCP mitgeteilt wird, den Kompressionsfaktor erhöhen und damit die Netzlast seinerseits reduzieren. Da RTCP aber vergleichsweise langsam die Sendung regelt, ist es eher für Videokonferenzen geeignet als für CCTV-Anwendungen. RTCP bietet keine Mechanismen, die bei einer Videoaufzeichnung zur Steuerung der Wiedergabe notwendig sind (z.B. Rückspulen); dazu wurde ein weiteres Protokoll entwickelt, das RSTP.

Hiermit lassen sich durch den Betrachter z.B. gespeicherte oder Live-Videoströme starten und beenden. Dabei werden die eigentlichen Nutzdaten nicht von RSTP übertragen. Wie herkömmlich erfolgt dies mit Hilfe von RTP. Aber auch dieses Protokoll wurde primär für andere Zwecke, beispielsweise die kommerzielle Videofilm-Übertragung, entwickelt. Die im CCTV-Bereich notwendigen Funktionen, wie z.B. Recherchen nach bildabhängigen Metadaten, lassen sich auch damit nicht realisieren. Folglich gibt es im Prinzip keine Standard-Protokolle, die ergänzend zu RTP für die CCTV-Anwendung von Bedeutung wären. An proprietären Protokollen und Software-Lösungen zur Abfrage der Video-Datenbanken führt zumeist kein Weg vorbei.

Da im TV-Bereich dem IP-Multicast eine größere Bedeutung zukommt, soll nochmals kurz erläutert werden, warum diese Technik im CCTV-Umfeld nicht die gleiche Rolle spielen kann. Wie mehrfach erläutert nimmt der Betrachter bei CCTV eine aktiv steuernde Rolle ein; er greift auf die Kamera bzw. das Videostrom-erzeugende Gerät zu. Eine permanente ununterbrochene bzw. nicht beeinflussbare Generierung und Verteilung von Videos per Multicast macht dann nur wenig Sinn. Natürlich wäre eine Erzeugung und Verteilung von Videobildern auf viele, rein passive Videoempfänger vorstellbar, und dann wäre mit IP-Multicast eine Optimierung der Bandbreite im Netzwerk möglich. Doch eine derartige Nutzungsform kann nicht das Ziel einer modernen Videoüberwachungslösung sein, was offensichtlich dazu führt, dass bei vielen Kameraherstellern IP-Multicast keine besondere Bedeutung hat.

Ereignisgesteuerte Videoübertragung

Eine wichtige technische Funktion kann erheblich zur Reduzierung der Netzlast(en) und der Minimierung der zentralen Speicherelemente beitragen: die ereignisgesteuerte Videoübertragung. Eine analoge Kamera besitzt nicht die Intelligenz, Bewegung zu erkennen und dann erst mit der Bildübertragung zu beginnen. Sie erzeugt einen kontinuierlichen analogen Bildstrom. In einer hybriden Videoüberwachungsanlage „landet“ das analoge Signal auf einem oder mehreren Videoservern mit Netzwerkanschluss. Dieser besitzt dann die Fähigkeit, gezielt nur die Bilder über das Netzwerk zur zentralen Videodatenbank weiterzugeben, die von Bedeutung sind bzw. bei denen eine Bewegung erkannt wurde, eine ereignisgesteuerte Videoübertragung ist auch in hybriden Netzen möglich.

Bei Einsatz von Kameras, die IP-basierend die Videoinformation über ein lokales Netzwerk übertragen, ist die Analyse-Intelligenz derselben von erheblicher Bedeutung für das Netzwerk. Zur Reduzierung der zu übertragenden binären Videoinformationen erfolgt, wie gezeigt, eine mehr oder weniger starke Komprimierung. Je stärker diese ist, umso mehr Videoinformationen gehen verloren; eine Komprimierung um jeden Preis kann demnach nicht sinnvoll sein. Die Analyse des Videobildes und die Beeinflussung der Bildrate oder Bildauflösung reduziert den Komprimierungsaufwand bzw. -grad und schont das Netzwerk. Dazu muss die Bildanalyse im Idealfall bereits in der Kamera erfolgen. Selbst wenn ein Netzwerk mehr als ausreichende Bandbreite bereitstellt, optimiert diese Intelligenz in der Kamera / Videoserver ein weiteres, kostenrelevantes Element: die Hardware der zentralen Videoauswertung und Speicherung. Ein Zentralsystem, welches mehrere, noch nicht optimierte Videokanäle aufnimmt und diese

erst bewerten muss, um die Daten gezielt abzuspeichern, erfordert entsprechende Leistungseigenschaften bezüglich Hard- und Software.

Hinter dieser als Video Motion Detection bezeichneten Technik steht ein einfaches Prinzip. Ergibt die Bildanalyse auf der Kamera / Videoserver beim Vergleich von zwei aufeinander folgenden Bildern eine Abweichung, so kann schlussfolgernd von einer Veränderung der überwachten Situation ausgegangen werden. Beim Vergleich können sowohl Farb- als auch Kontrast- bzw. Helligkeitsveränderung bewertet werden. In der Praxis hat sich gezeigt, dass der Vergleich der Helligkeitsveränderung die besseren Ergebnisse bringt. Nun wird es wenig Sinn machen, eine Bewertung im gesamten Bild vorzunehmen, wenn die Überwachungsaufgabe z.B. den Eingangsbereich einer Außentür vorsieht. Ereignisse wie Schneefall, sich bewegende Bäume oder ändernde Lichtverhältnisse würden zu Fehlinterpretationen führen. Deshalb lassen digitale Kameras die Definition von mehreren Prüfbereichen bzw. Alarmfeldern zu, die zur Analyse herangezogen werden. (siehe Abbildung 3)

Die Nutzung von Alarmfeldern erfordert von den Kameras in der Regel weitere Mechanismen, um Fehlinterpretationen zu vermeiden. Helligkeitsunterschiede durch Wolkenverdunklungen, Zitterbewegungen eines Kameramastes oder auch Bewegungen von Tieren müssen erkannt werden und sollten nicht zur Auslösung von Übertragungen oder Aufzeichnungen führen. Dazu werden z.B. die Felder bei der Bewertung miteinander verknüpft, erfolgt eine Helligkeitsänderung in allen definierten Alarmfeldern, so kann dies ein Indiz für eine wolkenbedingte Lichtänderung sein, das System zeichnet diese Bilder nicht auf oder überträgt sie nicht. Eine weitere Anforderung an die Leistungsfähigkeit der Bewegungserkennung besteht je nach gestellter Überwachungsaufgabe darin, auch sehr schnelle Bewegungen zu erkennen, Erkennungsmechanismen müssen gegebenenfalls im Millisekunden-Bereich und damit in Echtzeit arbeiten.

Eine Erkennung von Bewegung, die gemäß den Anforderungen zu einer Übertragung bzw. Aufzeichnung des Videos genutzt wird kann auch regelnd auf die Netzlast einwirken. Folgendes Szenario ist denkbar: Eine Kamera erzeugt mit niedriger Bildauflösung (z.B. einer VHS-adäquaten CIF-Qualität) und geringer Bildwiederholrate (z.B. 5 Bilder/s) einen Videostream, der über das Netzwerk permanent zu einem zentralen Archivierungssystem übertragen wird. Im Alarmfeld tritt ein Ereignis ein, welches zum einen

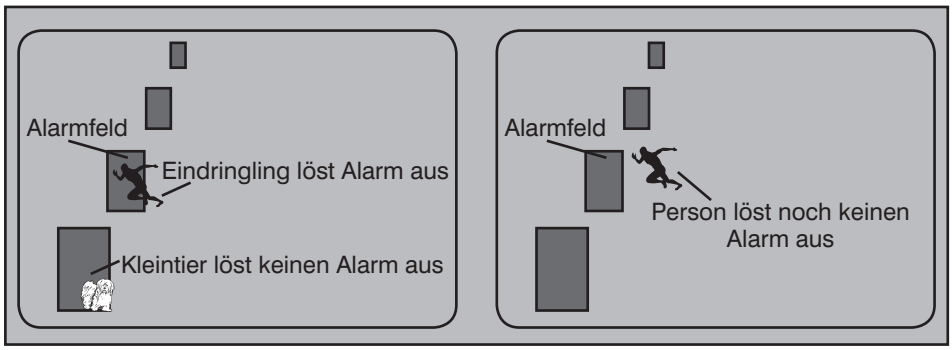


Abbildung 3: Definition von Alarmfeldern

z.B. die Aufschaltung des Videos auf einen Überwachungsbildschirm zur Folge hat und zum anderen zu einer besseren Videoqualität bei der Aufzeichnung wie auch beim Monitoring führen soll (z.B. Wechsel der Bildauflösung zu 4CIF und Bildrate zu 25 Bilder/s). Dazu sind moderne Kameras mit variabler Bitrate (VBR variable bitrate) und / oder mit eine variablen Bildratensteuerung (VFR variable framrate) ausgestattet; bei Kameras, die das nicht unterstützen, spricht man von CBR (constant bitrate) bzw. CFR (constant framerate). Diese schwankende Bild- und Bitrate hat natürlich Schwankungen bei der Netzlast und bei den benötigten Speicherkapazitäten zur Folge. Ein passend dimensioniertes Netzwerk sollte ohne Zusatzmaßnahmen dieses verkraften, bei den Speichermedien sind passende Worst Case- oder Mittelwert-Analysen notwendig und die Decoder-Technik muss mit diesen Wechseln innerhalb des Streams umgehen können.

In Kombination mit der Video Motion Detection zur gezielten Speicherung von Bildern lässt sich der Erkennungsmechanismus auch benutzen, um initiiert durch das zentrale Videoanalysesystem weitere Ereignisse zu starten, denkbar sind Benachrichtigung von Feuerwehr, Starten eines Alarmsignals, Stoppen eines Produktionsvorgangs o.ä.. Doch die Verwendung dieser Funktion ist wohl zu überlegen und entsprechend zu konzipieren, denn verursacht bei einer Fehlinterpretation des Ereignisses die irrtümliche reine Abspeicherung nur eine unnötige Speicherung von weiteren Bildern, so würden bei der getriggerten Ereignisauslösung größeren Ausmaßes wie z.B. die Anfahrt des Wachdienstes eventuell weitere erhebliche Folgekosten entstehen. Bei häufigen Fehlalarmen ist auch denkbar, dass der „echte“ Alarm irgendwann von dem Wachpersonal nicht mehr ernst genommen wird.

Zentral-Systeme

Zur Überwachung einer oder weniger Netzwerkkameras reicht bereits ein einfacher Internet-Browser aus, dieser bietet die Möglichkeit zur Darstellung des Videobildes, zur Konfiguration der Kamera oder auch Steuerung der Kamera. Die Auswertung der Videos erfolgt dann häufig über das direkte Betrachten des Live-Bildes. Wird die Anzahl von Videokanälen erhöht, so liegt es sehr nahe, dass diese Mehrfach-Bilder nicht mehr durch Menschen überwacht werden können bzw. die Gefahr von „übersehenen“ Details steigt. Deshalb wird es unerlässlich werden, die Videos statt durch einen Menschen durch eine Software auswerten zu lassen, um nur das anzuzeigen, was tatsächlich von Relevanz ist. Häufig wird einem perfekt arbeitenden Videoüberwachungssystem ein zumeist schwarzer Bildschirm zugewiesen, nur im „Ereignisfall“ werden Bilder auf den Monitor wiedergegeben. Wie wir gesehen haben, kann diese Bewertung bereits durch die Kamera erfolgen, zentrale Software-Module bieten hier aber in der Regel mehr Möglichkeiten.

Eine Videoüberwachung ohne Speicherung der Videokanäle wird es nicht zulassen, rückblickend die aufgetretenen Ereignisse zu bewerten oder gar Beweismaterial zusammenzustellen. Das einfachste Aufzeichnungsgerät auf dem Niveau eines Standard-Videorekorders speichert zwar auch das aufgezeichnete Video ab, es lässt aber eine nachträgliche Analyse nur durch „manuelles“ Betrachten zu. Genau hier liegt aber die Stärke von digitalen CCTV-Systemen, die Bilder bzw. das Video wird beim Abspeichern mit Zusatzinformationen versehen, sei es nur ein Zeitstempel, der bei der Bilderanalyse zu wesentlich schnelleren Ergebnissen führen wird. Die Speicherung digitaler, komprimierter Videobilder und die Möglichkeit zu komfortablen Recherchen und Auswertungen sind die Kernfunktionen von CCTV, die Wichtigkeit von Live-Beobachtungen nimmt deutlich ab. Ein Zentral-System für größere CCTV-Anlagen besteht aus

- einer Administrationssoftware zur Einstellung des Aufzeichnungsverhaltens und anderer Parameter des CCTV-Sys-

tems mit Diagnose und Wartungsfunktionalität,

- einem Software-Modul zur Kommunikation mit einer oder mehrere Videodatenbanken zur Wiedergabe von gespeicherten Bildern und zur direkten Kommunikation mit den IP-Kameras,

- und natürlich einem Speicher bzw. einer Videodatenbank, die eine Nachanalyse möglich macht.

Die größten technischen Herausforderungen liegen dabei in der Leistungsfähigkeit der CCTV-Videodatenbank. Dieses Werkzeug muss es erlauben, sämtliche Videokanäle abzuspeichern, die Begleitinformationen herauszulesen und in eine Datenbank einzutragen und gleichzeitig vom CCTV-Nutzer z.B. für Bildsuchfunktionen oder Wiedergabefunktionen genutzt werden zu können. Bei der Betrachtung von Videos aus einer Datenbank wird z.B. mit einer speziellen Software dafür gesorgt, dass die Videos angesehen werden können, ohne gleich die ganze Datei laden zu müssen. Diese Software arbeitet mit Hilfe eines Datenbank-Cursors, welcher den passenden Satz an abgespeicherten Ergebnissen zum Client lädt. Mit so genannten SELECT-Funktionen können dann in diesem beim Client befindlichen Datensatz Videofunktionen wie Stop, Rewind, Pause etc. genutzt werden. Ein anderes Beispiel für diese hohen Anforderungen besteht in der Bild-Synchronität: Leistungsfähige Videozentralen-Lösungen lassen ein absolut zeitsynchrones Abspielen von mehreren Kanälen zu, die z.B. gemeinsam eine Überwachung eines identischen Bereiches durchführen, diese Synchronität wird bis hin zu Zeitlupenvergleichen gewährleistet. Da in der Regel mehrere Personen derartige Funktionen und Inhalte der Videodatenbank gleichzeitig nutzen sollen, steigert dies die Anforderung an die Videozentralen-Lösung erheblich. (siehe Tabelle 2)

Besonderheiten IP-Kameras

Netzwerk-Kameras unterscheiden sich von klassischen Kameras wie beschrieben in den Möglichkeiten, die sie durch ihre Intelligenz bieten. Darüber hinaus verzichten sie durch die Funktion Power over Ethernet auf separate Leitungen zur Stromversorgung. Häufig reicht bei nicht bewegbaren Kameras eine Leistungsklasse 2 nach IEEE 802.3af. Die Möglichkeit von PoE darf aber erfahrungsgemäß nicht grundsätzlich überbewertet werden. Sehr häufig befinden sich Kameras nicht in 90m-Reichweite eines Verteilers und es ist Glasfaser einzusetzen. Folge: Ein Betriebsstrom kann darüber nicht übertragen werden. In Anbetracht dessen, dass Videokameras mit Glasfaseranschluss kaum im Markt vorhanden sind, muss neben dem Stromanschluss der Kamera in der Regel auch ein Medien-Konverter eingeplant werden, der entsprechend wetterfest zu montieren ist.

Eine weitere Besonderheit im Unterschied zu klassischen Systemen stellen WLAN-Kameras dar, diese lassen den völligen Verzicht auf Datenleitungen zu. Nicht vergessen werden darf dann aber, dass eine entsprechende Stromverkabelung notwendig ist, damit reduzieren sich die Vorteile der drahtlosen Kamera. In Fachkreisen wird der Einsatz von WLAN-basierenden Videokameras sehr skeptisch bewertet, insbesondere wenn eine hohe Verfügbarkeit der Videoübertragung gefordert ist. Selbst wenn die Zugangssicherheit und die Vertraulichkeit der übertragenen Daten gewährt sind, führt die Charakteristik des Funkkanals zu einer Anfälligkeit gegen beabsichtigte oder unbeabsichtigte Störungen der Übertragung. Welchen Wert besitzt eine Videoüberwachung, die keine Vollständigkeit garantieren kann.

Wie im klassischen Bereich bietet der Markt auch ein reiches Angebot an IP-Kameras mit PTZ-Funktionen. Die im Zusammenhang mit der Latenzzeit angesprochenen Probleme der Steuerungen müssen berücksichtigt werden, reine Zoom-Funktionen lassen sich durch den Einsatz von Megapixel-Systemen gegebenenfalls vermeiden. Mit dem Einsatz von Megapixel-Kameras steigern sich die Möglichkeit zu Detailbetrachtungen erheblich, zum Vergleich: Die maximale Bildauflösung von Analogkameras nach der Digitalisierung des Videosignals beträgt 0,4 Megapixel (704 x 576 = 405504), IP-Kameras liefern mehr als 2 Megapixel, das bedeutet eine mehr als 5-fache Auflösung. Natürlich ist in Abhängigkeit der Anforderungen zu bewerten, ob diese Auflösung notwendig ist. Soll beispielsweise in einem Industriepark mit Hilfe der Kamera ein Brandherd erkannt werden können, so wird auch eine kleinere Auflösung ausreichen, weil Nachanalysen des Bildmaterials mit hoher Auflösung nicht gefordert sind. Die Verwendung von hochauflösenden Kameras hat neben den höheren Anschaffungskosten sehr häufig einen weiteren Nachteil, die Kameras weisen eine verminderte Lichtempfindlichkeit vor. Gerade in Zusammenhang mit nur spärlicher Beleuchtung ist dies zu prüfen. Aufgrund der größeren Sensibilität von PTZ-Kameras bezüglich Latenzzeiten empfehlen einige Hersteller die Einführung von QoS in Datennetze, um die PTZ-Kommandos bevorzugt durch das Netzwerk vermitteln zu können.

Neben den „normalen“ IP-PTZ-Kameras gibt es auch nichtmechanische PTZ-Netzwerk-Kameras, bei denen ein Megapixel-Sensor den Kamerabereich zwischen 140°

		MJPEG-Komprimierung		MPEG4-Komprimierung*	
Kameraanzahl	Bildrate (fps)	GByte/Stunde	GByte/Tag	GByte/Stunde	GByte/Tag
10	2	2,5	20,2	0,50	4,03
30	2	7,6	60,5	1,51	12,10
60	2	15,1	121,0	3,02	24,19
90	2	22,7	181,4	4,54	36,29
10	15	18,9	151,2	3,78	30,24
30	15	56,7	453,6	11,34	90,72
60	15	113,4	907,2	22,68	181,44
90	15	170,1	1.360,8	34,02	272,16
10	25	31,5	252,0	6,30	50,40
30	25	94,5	756,0	18,90	151,20
60	25	189,0	1.512,0	37,80	302,40
90	25	283,5	2.268,0	56,70	453,60

Rahmenbedingungen:
Angenommene Bildgröße für 4CIF-Format MJPEG (kByte): 35
Angenommene Bildgröße für 4CIF-Format MPEG4 (kByte): 7,0
Angenommene Betriebszeit (Stunden pro Tag): 8
*Hinweis: Sehr niedrige Bildraten bei MPEG4 nicht sinnvoll (Standard: 25 fps)

Tabelle 2: Speicherbedarf digitale Bildaufzeichnung

und 360° abdecken kann. Der Bediener kann die Kamera ohne mechanischen Positionswechsel in jede Richtung schwenken, neigen oder zoomen. Dadurch entfällt der Verschleiß von beweglichen Teilen.

Ein Vergleich von vielen Datenblättern der IP-Kameras bringt erstaunlicherweise zutage, dass der Temperaturbereich auch von Außenkameras nicht für strenge Winter gedacht ist. Erstreckt sich dieser zwar von Minus-Temperaturen bis hin zu hohen Sommertemperaturen, so enthalten die Informationen aber häufig eine empfohlene Temperatur erst ab 0 Grad Celsius. Deshalb sind Zusatzheizungen in den Gehäusen gegebenenfalls vorzusehen. Welches Fehlverhalten eine Kamera bei längeren Zeiträumen mit Negativ-Temperaturen ohne Zusatzheizung hat, ist beim Hersteller nachzufragen.

Analoge Kameras jedweder Art können mit Hilfe von Videoservern bzw. Encoder in ein digitales Netzwerk eingebunden werden. Der Encoder digitalisiert und komprimiert das Video und überträgt es über ein lokales Netzwerk, selbst die Steuerung der Kamera erfolgt mit Hilfe der am Encoder vorhandenen Schnittstelle (z.B. RS485) über das Netzwerk. Die meisten Encoder besitzen Treiber für unterschiedliche anzuschließende Kamerasysteme, zu beachten ist dabei die verzögerungsfreie Umschaltung bei Anschluss von mehreren Kameras an einen Encoder. Für den Fall, dass an eine digitale CCTV-Anlage weiterhin klassische Überwachungsmonitore angeschlossen werden müssen, stehen Decoder zur Verfügung.

Projektierung von CCTV-Lösungen

Die Einfachheit der Nutzung einer einzelnen Netzwerkkamera, man schließt sie an ein „normales“ Netzwerk an, benutzt einen Browser und schon kann man überwachen, täuscht über die Komplexität einer Einführung von größeren CCTV-Anlagen. Selbst im Umfeld von Firmen, die bereits eine klassische Videoüberwachung in mittlerem bis größeren Stil nutzen, gestaltet sich die Migration erfahrungsgemäß als schwierig. Einige dieser, gerade in einem konkreten, durch den Autor des Artikels begleiteten Migrationsprojekt gewonnenen Erfahrungen bzw. Planungsschwierigkeiten werden nachfolgend beschrieben.

Die Aufgabe sieht zunächst sehr einfach aus: in einem kleineren überschaubaren Bereich, in dem noch keine Videoüberwachung durchgeführt wird, sollen in Zukunft neue Netzwerk-Kameras positioniert werden (Charakter eines Pilotprojektes). Darüber hinaus betreibt der Kunde bereits ein Videonetzwerk mit fast 50 im Gelände montierten analogen Kameras, deren überwiegende Aufgabe es ist, Brände, Explosionen oder ähnliches zu detektieren und adäquate Folgemaßnahmen wie Evakuierung der Bereiche oder Leiten der Feuerwehr einzuleiten. Es geht weniger um das klassische Gebiet der Videoüberwachung, der Kontrolle von Personen. Aus Sicht des aktuellen Betreibers der Videoanlage ist man sich im Klaren, dass die Zukunft der digitalen CCTV-Technik gehört, demzufolge möchte man ein Dutzend der veralteten Kameras durch neue Netzwerk-Kameras ersetzen und die restlichen analogen Kameras mit Hilfe von Encoder-Techniken ebenfalls digitalisieren.

Die Aufgabe ist also aus Sicht des Betreibers sehr einfach: Sukzessiver Austausch der alten analogen Kameras gegen neue digitale, Hinzufügen von neuen Netzwerkkameras, Austausch des Zentral-Systems und Integration der alten analogen Kameras in das IP-basierende System (ein passendes Lokales Netzwerk steht zur Verfügung).

Bereits in einer frühen Phase der Anforderungsdefinition musste jedoch die erste Hürde überwunden werden, die darin bestand, dem Nutzer klar zu machen, dass der Grundansatz der digitalen Videotechnik völlig anders ist als die aktuell genutzte Verfahrensweise. Heute erfolgt die Analyse und Bewertung von Gefahrenereignissen in erster Linie durch direkte Beobachtung von Live-Bildern, dies hat eine entsprechende Anzahl von Monitoren und Personal zur Folge. Die erste Idee des Nutzers war es, einfach die gesamte analoge Technik durch eine digitale zu ersetzen, am Nutzungsprinzip aber nichts zu ändern. Hieraus leitete sich zunächst die Aufgabe ab, das neue Grundprinzip zu erläutern und dabei insbesondere deutlich zu machen, dass eine optimale und wirtschaftliche Nutzung der vorhandenen Ressource „Netzwerk“ und der neu aufzubauenden Ressource „Zentralentechnik“ nur dann gelingt, wenn u.a.

- Klarheit darüber gewonnen wird, was wer genau in welcher Qualität wann sehen können muss (ist die gewohnte „TV-Qualität“ der analogen Anlage tatsächlich zu jeder Sekunde und an jedem Tag notwendig),
- für jede neue IP-Kamera festgelegt worden ist, welche Grundfunktionen diese besitzen muss (muss eine Zoom-Funktion gefordert werden, wenn die Mega-

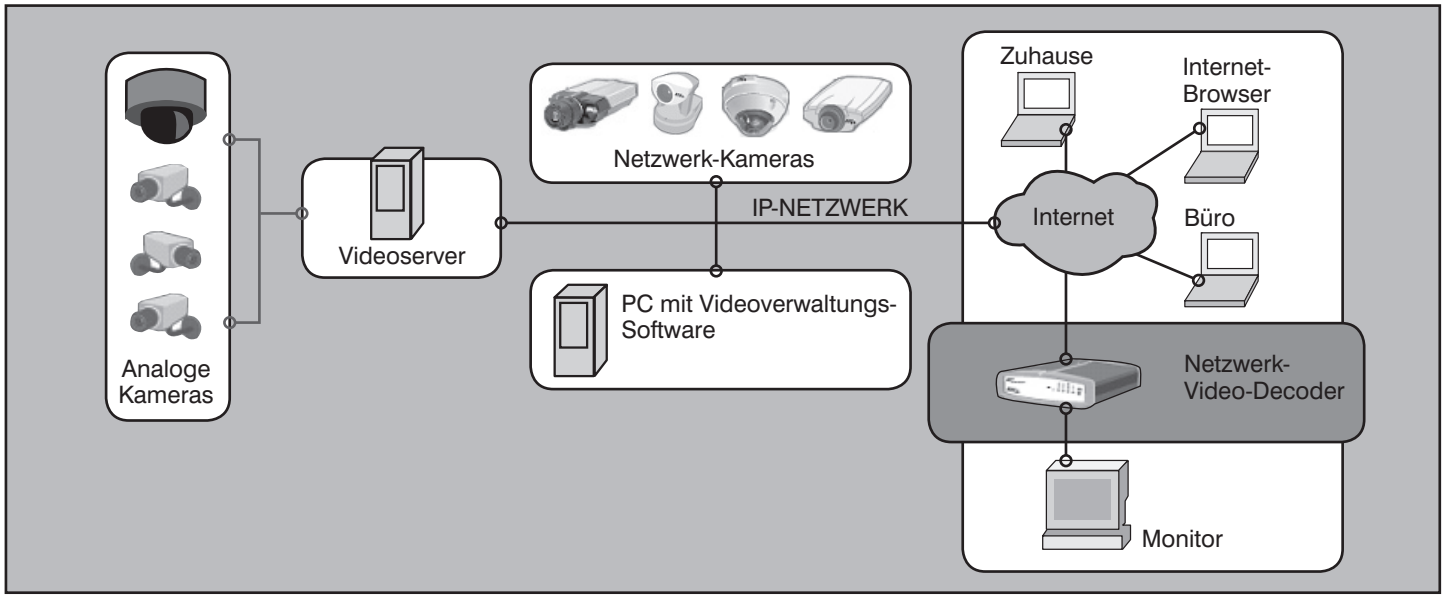


Abbildung 4: Elemente eines CCTV-Netzes

pixeltechnik ein wesentlich leistungsfähigeres digitales Zoomen zulässt),

- bisher nicht zur Verfügung gestandene Zusatzfeatures wie z.B. Video Motion Detection oder kameragesteuerte Events genutzt werden sollen und bekannt sein müssen.

Das Ergebnis dieser „Befragung" bildete ein komplexer Anforderungskatalog, der jedoch noch nicht die ausreichende Detailtiefe oder Klarheit in technischen Fragen hatte, um daraus direkt eine Angebotseinholung in Form einer Leistungsbeschreibung einzuleiten. Im Rahmen der Planung für das Pilotprojekt wurde festgestellt, dass eine Abschätzung der benötigten Videoqualität schwierig war. Deshalb beauftragte man externe Spezialfirmen, eine Videoanalyse durchzuführen und eine - nach Möglichkeit herstellerunabhängige - Lösung auszuarbeiten, deren Inhalt mindestens bestehen sollte aus:

- eine messtechnische Expertise zur Positionierung der Videokameras (inklusive Beistellung von Kameras im Rahmen der Analyse),
- Vorgaben der notwendigen Eigenschaften der vorzusehenden Kameras, inklusive der Ausarbeitung eines Anforderungskataloges mit Wichtung der Anforderungen/Eigenschaften (insbesondere Lieferung von Beispielen zu den unterschiedlichen Bildqualitäten zur Ermittlung der Nutzeranforderungen),
- Vorgaben zum Montageort der vorzusehenden Kameras,
- Vorgaben zur Stromversorgung der vorzusehenden Kameras,
- Vorlage einer Kostenschätzung für die entwickelte, herstellerunabhängige Lösung.

Die Ergebnisse waren nicht zufrieden stellend:

1. Es wurde in einigen Expertisen überhaupt nicht oder nur zum Teil auf die geforderten Lösungsinhalte eingegangen.
2. Es fand keinerlei Befragung des Kunden statt zur gewünschten Nutzung der neuen Anlage. Dabei erlaubt gerade die digitale CCTV-Technik wie im Artikel dargestellt, eine Vielfalt von Möglichkeiten, die als Minimal- oder Wunschforderung in einer Leistungsbeschreibung definiert werden kann.
3. Einige Lösungen beinhalteten sehr rudimentäre, gerade für den Einsteiger im CCTV-Bereich kaum nachvollziehbare Konzepte und vorgeschlagene Produkttypen. Es wurden Standard-Datenblätter beigelegt, die in keinerlei Kontext zu der gestellten Aufgabe gesetzt wurden. Andere Lösungen ließen die zu erwartenden Kosten offen, Alternativkonzepte wurden nicht erstellt.

Prinzipiell war der Informationsstand der Planung nicht wesentlich besser als vor der Analyse und es wurde entschieden, die Erstellung des Anforderungskataloges in Zusammenarbeit mit der ComConsult Beratung und Planung in einem größeren Umfang selbstständig vorzunehmen und mit Hilfe einer funktionalen Ausschreibung die Angebotseinholung fortzusetzen. Dies ist der derzeitige Stand des Projektes, und es wird deutlich, dass ohne entsprechendes Know-How auf der Nutzerseite zu den Möglichkeiten der CCTV-Technik weder ein brauchbares Anforderungsprofil noch die Einholung von mehreren, vergleichbaren Angeboten erfolgreich sein wird. Ohne Anforderungsprofil kann zwar davon ausgegangen werden, dass vielfältige, durchaus funktionierende Lösungen mit unterschiedlichen Produkten möglich sind, aber der Vergleich scheitern wird.

Fazit

Die Nachfrage nach Sicherheitssystemen, die dem Nutzer die Möglichkeit geben, visuelle oder auch auditive Überwachungen mit Hilfe von Lokalen Netzwerken zu realisieren (neben CCTV wird der Begriff der „IP-Surveillance" verwendet) steigt in den letzten Jahren rapide an, das Ende der klassischen Videoüberwachung wird für Anfang der nächsten Dekade prognostiziert. Worin liegen die Vorteile? Vereinfacht gesagt sorgt ein gutes CCTV-System in Kombination mit einer guten Planung dafür, dass der oder die Überwachungsmonitore möglichst häufig bzw. möglichst lange „schwarz" bleiben und damit kein von irgendjemand zu analysierendes Bild liefern. Erst in dem Fall, wenn das definierte „wichtige" Ereignis eintritt und visualisiert wird, muss ein Bild dort erscheinen, wo es ausgewertet werden kann. Damit ist auf der einen Seite nach Möglichkeit ein Kamerasystem einzusetzen, welches die Videobilder nur dann überträgt, wenn das Ereignis eingetreten ist. Dies wird die Grundlast des Netzwerkes niedrig halten. Wenn es ausgehend von der Kamera in Kombination mit dem Möglichkeiten des Netzwerkes einen Mechanismus gibt, der den Videostrom gezielt zu den auswertenden Systemen sendet, so wird auch das dazu beitragen, die im Netzwerk zu fordernde Performance gering zu halten. Im Artikel wurden einige Möglichkeiten beschrieben, die Kameras bzw. auch das Netzwerk zur Optimierung der Netzwerkauslastung bereitstellen. Darüber hinaus konnte dargelegt werden, dass die Ermittlung einer CCTV-Lösung weit über den einfachen Kameraanschluss und die Vorbereitung des Netzwerkes hinausgeht. Die damit verbundene Technik ist als äußerst vielfältig und komplex einzustufen und mit der Schaffung eines Anforderungsprofils muss begonnen werden. Die selbstständige Ausschreibung mit Hilfe von selbst erstellten Einzelpositionen und detaillierten Mengengerüsten muss sorgfältig überlegt werden, sie erfordert ein extremes Detailwissen. Eine möglicherweise bessere Alternative stellt die Funktionalausschreibung auf Basis des Anforderungsprofils dar, sie bietet die Möglichkeit, einen großen Teil der Verantwortung für das komplexe Detailwissen an die Bieter bzw. Auftragnehmer weiterzugeben.

Kongress

Rechenzentrum Infrastruktur-Redesign Forum 2008
24. - 26.11.08 in Königswinter

Das ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2008 analysiert folgende Themenschwerpunkte:

- Zukunftsfähige RZ-Netzwerke: was bedeutet das?
- Speicher-Konsolidierung; wohin fährt der Zug?
- RZ-Verkabelung 2008: wo stehen wir?
- Infrastruktur-Sicherheit im RZ: eine echte Herausforderung
- Integration mobiler Mitarbeiter / Fixed-Mobile-Konvergenz

Moderation: Dr. Jürgen Suppan
Preis: € 2.090,- zzgl. MwSt.* (*gültig bis 30.09.08 - dann regulär € 2.290,- zzgl. MwSt.)

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

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Sicherheit im LAN mit IEEE 802.1X, 08.09. - 09.09.08 in Bonn

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes. Preis: € 1.390,- zzgl. MwSt.

Trouble Shooting in vernetzten Infrastrukturen, 09.09. - 12.09.08 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege. Preis: € 2.190,- zzgl. MwSt.

Projekt-Erfahrungsbericht: Cisco CallManager Rollout und Migration CUCM Version 6, 15.09. - 16.09.08 in Aachen

Dieses 2-tägige Seminar beschreibt Planung, Installation und den Betrieb einer großen verteilten IP-Telefonie-Lösung auf der Basis des Cisco CallManagers. Es macht deutlich, in welchem Umfang die Standard-Installation angepasst und erweitert werden musste, um den Anforderungen der Teilnehmer zu entsprechen. Auch die Umstellung traditioneller Betriebsabläufe im Änderungs-Management und deren Auswirkung auf die Konfiguration des CallManagers wird beschrieben. In diesem Zusammenhang werden insbesondere auf die Akzeptanz der Benutzer und die damit notwendigen Änderungen in der Bedienung der Telefone eingegangen.

Preis: € 1.390,- zzgl. MwSt.

SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie, 15.09. - 17.09.08 in Frankfurt a.M.

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert.

Preis: € 1.690,- zzgl. MwSt.

Lokale Netze für Einsteiger, 15.09. - 19.09.08 in Aachen

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt. Preis: € 2.290,- zzgl. MwSt.

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit, 22.09. - 26.09.08 in Bonn

Bedrohungen der IT-Sicherheit bestehen für praktisch alle Elemente einer vernetzten IT-Infrastruktur. Die Quelle der Bedrohung kann sowohl von außen auf das Netz wirken als auch von innen stammen. Sicherheit entsteht erst, wenn alle signifikanten Gefahrenbereiche systematisch verriegelt werden. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Dabei wird jeder einzelne Baustein detailliert erklärt und anhand typischer Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt. Preis: € 2.290,- zzgl. MwSt.

IP-Telefonie: Vorbereitung, Migration, Management, 13.10. - 15.10.08 in Bonn

Die Vorbereitung der Netze auf IP-Telefonie, die Migration von der klassischen Telekommunikation zu Voice over IP sowie der Betrieb der dadurch entstehenden komplexen Netz- und Anwendungsarchitektur konfrontieren alle Unternehmen mit neuen Herausforderungen. Das Wissen aus verschiedenen Bereichen, von der Netzinfrastruktur bis hin zu neuen und etablierten Kommunikationsapplikationen, muss zu einem interdisziplinären Know-how verdichtet und neu geordnet werden. Diesem Ziel dient das Seminar.

Preis: € 1.690,- zzgl. MwSt.

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 13.10. - 17.10.08 in Aachen

Dieses 5-Tages-Intensiv-Seminar vermittelt dem Einsteiger Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Fallstudien und Gruppenübungen mit Planungsbeispiel vermitteln Informationen, die in der Praxis sofort umgesetzt werden können. Preis: € 2.290,- zzgl. MwSt.

Trouble Shooting für Netzwerk-Anwendungen, 14.10. - 17.10.08 in Aachen

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzte Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.190,- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
24.11. - 28.11.08 in Aachen
02.03. - 06.03.09 in Aachen
11.05. - 15.05.09 in Aachen
31.08. - 04.09.09 in Frankfurt
23.11. - 27.11.09 in Hamburg

TCP/IP und SNMP
20.10. - 24.10.08 in Berlin
16.02. - 20.02.09 in Bonn
25.05. - 29.05.09 in Aachen
21.09. - 25.09.09 in Bonn

Internetworking
13.10. - 17.10.08 in Aachen
09.02. - 13.02.09 in Aachen
11.05. - 15.05.09 in Aachen
05.10. - 09.10.09 in Frankfurt

Paketpreis für alle drei Seminare € 6.183,-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
03.02. - 06.02.09 in Aachen
05.05. - 08.05.09 in Aachen
06.10. - 09.10.09 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
14.10. - 17.10.08 in Aachen
17.03. - 20.03.09 in Aachen
16.06. - 19.06.09 in Aachen
03.11. - 06.11.09 in Aachen

Paketpreis für beide Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 3.940.-- zzgl. MwSt.
(Einzelpreise: je € 2.190.--)

ComConsult Certified Security Expert

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
22.09. - 26.09.08 in Bonn
09.02. - 13.02.09 in Hamburg
14.09. - 18.09.09 in Köln

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten
03.11. - 07.11.08 in Bonn
30.03. - 03.04.09 in Berlin
26.10. - 30.10.09 in Aachen

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs
01.12. - 05.12.08 in Aachen
22.06. - 26.06.09 in Aachen
23.11. - 27.11.09 in Aachen

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ und „Sicherheit in Wireless LANs“. € 6.183.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

ComConsult Certified Voice Engineer

Basis-Seminar: Session Initiation Protocol-Basis-Technologie der IP-Telefonie
17.11. - 19.11.08 in Frankfurt
30.03. - 01.04.09 in Berlin
15.06. - 17.06.09 in Stuttgart
28.09. - 30.09.09 in Bad Neuenahr
23.11. - 25.11.09 in Hamburg

Basis-Seminar: Sicherheitsmechanismen für Voice over IP
03.11. - 04.11.08 in Bonn
09.02. - 10.02.09 in Hamburg
14.05. - 15.05.09 in Bonn
05.10. - 06.10.09 in Frankfurt

Alternative 1: IP-Telefonie evaluieren, planen, betreiben
27.10. - 29.10.08 in Bonn
02.03. - 04.03.09 in Stuttgart
25.05. - 27.05.09 in Hamburg
14.09. - 16.09.09 in Köln
02.11. - 04.11.09 in Frankfurt

Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management
13.10. - 15.10.08 in Bonn
16.02. - 18.02.09 in Bonn
15.06. - 17.06.09 in Stuttgart
26.10. - 28.10.09 in Berlin

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
17.11. - 18.11.08 in Frankfurt
02.02. - 03.02.09 in Bonn
04.05. - 05.05.09 in Königswinter
07.09. - 08.09.09 in Aachen
09.11. - 10.11.09 in Königswinter

Basis-Paket Alternative 1: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 1“
Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Basis-Paket Alternative 2: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 2“
Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,-- zzgl. MwSt. statt € 1.390,-- zzgl. MwSt.

Impressum

Verlag:
ComConsult Technology Information Ltd.
ComConsult Research
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline 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
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research