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 13

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 7

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 6

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-

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.

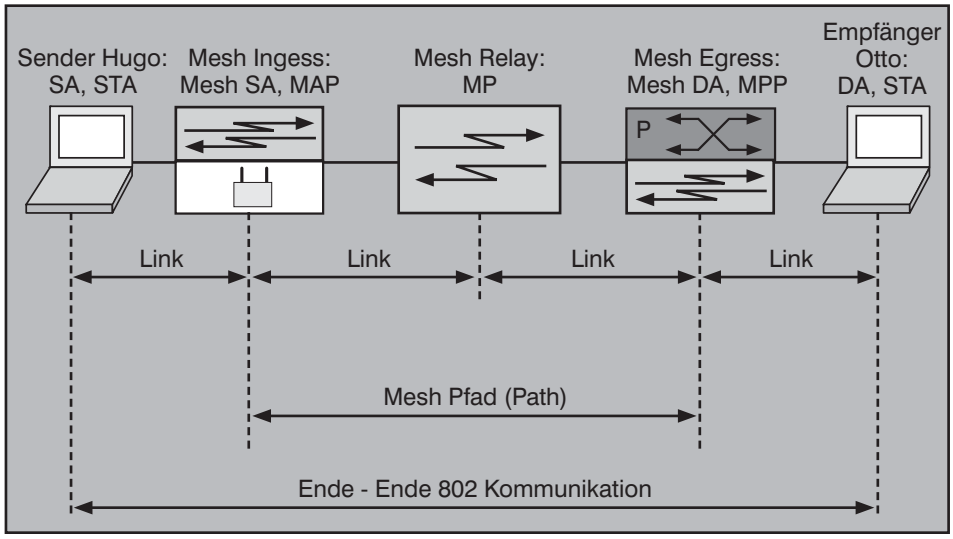

Abbildung 3.7: Mesh WLAN als Layer-2 Dienst nach außen

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

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

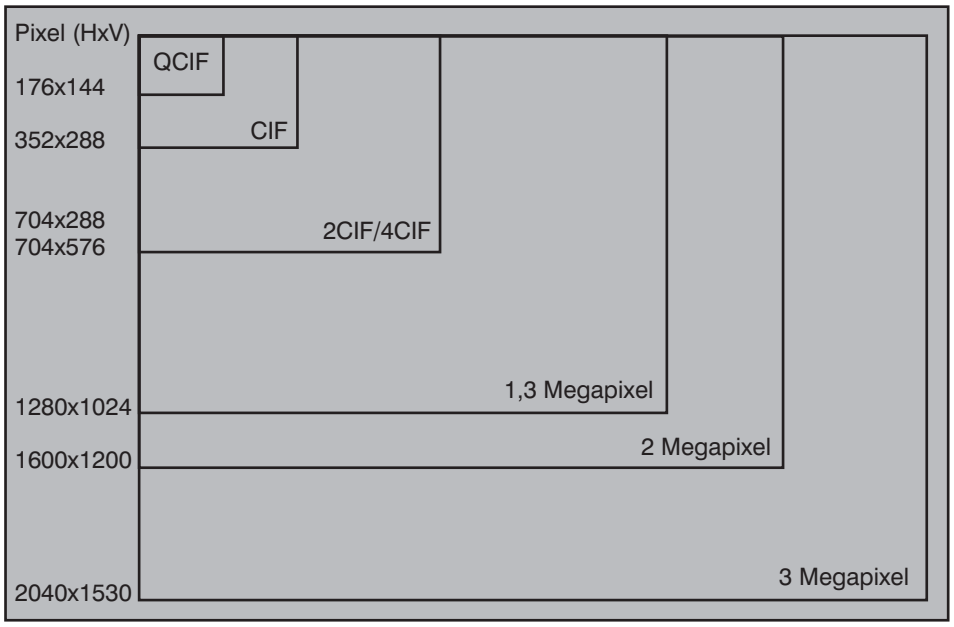

Abbildung 1: Typische Bildformate – PAL und Megapixel

Digitale Kameras im Netzwerk

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 in Mitten 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**