ComConsult Technologie Information

Der Netzwerk Insider

April 1999

Technologie Information für die Ausbildung zum CCNE

Schwerpunktthema

Quality of Service im LAN: Leistung kontra Komplexität

von Dipl.-Inform. Petra Borowka

Neue Applikationen mit Video, Sprache und multimedialen Anteilen führen zu veränderten Anforderungen an Unternehmensnetzwerke, die nur durch Dienstgüte-Implementierung erfüllt werden können. In den letzten 3 Jahren war der Hoffnungsträger für Quality of Service allein ATM. Inzwischen sind jedoch Quality of Service-Ansätze mit etablierter LAN-Technologie soweit gereift, daß sie als zukünftige Alternative zu ATM beachtet werden müssen.

Wandel im Netzdesign und der Protokolltechnik

Die klassische LAN-Technik hat mit Quality of Service nicht viel gemein: Betrieben werden Token Ring, FDDI und insbesondere Ethernet mit der aktuell größten Marktdominanz als Techniken, die zwar dafür sorgen, daß die MAC-Pakete (Frames) verschiedener angeschlossener Stationen einigermaßen geordnet über dasselbe Kabel übertragen werden, darüber hinaus jedoch gilt das Ellenbogenprinzip: Die Station mit den längsten Paketen und dem leistungsfähigsten Netzwerkadapter nimmt sich den Löwenanteil der Kapazität in Shared LANs. Von Bandbreiten- oder Antwortzeit-Garantie keine Spur. Schlechte Zeiten für Applikationen mit engen Zeitrestriktionen wie Video und noch mehr Sprache. In den letzten eineinhalb Jahren hat sich allerdings das LAN Design verstärkt vom Hub-Einsatz hin zum Switch-Einsatz gewandelt: Zuerst im Backbone, dann zunehmend auch zur Endgeräteanbindung auf den Etagen werden sternförmige Netze mit Punkt-zu-Punkt-Verbindungen bis zum Endgerät aufgebaut. Nachdem nun das Design eines modernen Ethernet- oder Token Ring-LANs (wenn der 100 Mbit Token Ring denn endlich verfügbar wäre...) eins zu eins dem eines ATM-Netzes ähnelt, sollte es dann nicht möglich sein, auch noch den letzten fehlenden Baustein Dienstgüte in der Frame-Technologie zu integrieren?

Zusammenspiel für Dienstgüte

Neue Ansätze für Quality of Service mit Frame-Technologien

Mit einer für Internetworking-Hersteller sehr unüblichen Diskretion wurden in den letzten zwei Jahren eine Reihe Verfahren spezifiziert, die in ihrer Gesamtheit Quality of Service auf Basis reiner Frametechnologie ermöglichen. Nun stehen die ersten Implementierungen an, gefolgt vom Beweis der praktischen Einsatzfähigkeit. Ähnlich wie bei ATM handelt es sich um ein Zusammenspiel mehrerer Protokoll-Spezifikationen, die insgesamt eine Ende-zu-Ende Dienstgüte ermöglichen sollen:

- Dienstklassen CL und GS der ISSLL
- DS
- RSVP
- COPS
- IEEE 802.1D/p
- 802.1Q
- 802.3x&y

weiter auf Seite 5

Thema

Sicherheitsrisiken nehmen zu

von Dr. Jürgen Suppan

Spätestens der Virus "Melissa" hat es uns wieder gezeigt. Unsere modernen DV-Technologien haben erschreckende Sicherheitsmängel.

Mit relativ wenig Aufwand können mehr oder weniger agressive Viren entwickelt werden, die man mit den bestehenden Hilfsmitteln in kürzester Zeit weltweit verteilen kann. Von diesen Risiken ist auch das Netzwerk betroffen. Und die bisher eher seltenen Angriffe spielen uns eine Sicherheit vor, die in der Realität nicht vorhanden ist. Dabei verläuft die Entwicklung der Kommunikations-Technologie in einer Richtung, in deren Umfeld man eher die Forderung nach absoluter Sicherheit erwarten würde. Zur Zeit binden wir unsere großen "mission critical" Datenbank-Anwendungen in Netzwerke ein, demnächst machen wir uns mit Sprach- und Video-Integration vollständig von der Verfügbarkeit der Netzwerke abhängig.

Im Bereich der Ausfallsicherheit zollen wir dieser Entwicklung erfreulicherweise Tribut (siehe Leitartikel: Quality of Service). Doch wo ist das gleich große Engagement in Richtung Sicherheit gegen Sabotage und Datenbeeinflussung? Wie können wir weiterhin tatenlos den immensen Sicherheitslöchern unserer Netzwerke zusehen und uns an ihrer Tiefe erfreuen? Nur wenige Beispiele reichen aus, um das hohe Bedrohungspotential aufzuzeigen, dem wir ausgesetzt sind. Allen bekannt sind die mit dem Netzwerk-Management-Standard SNMP verbundenen Sicherheitsrisiken. Jedes Kind kann zur Zeit eine Vire schreiben, die die meisten der auf dem Markt angebotenen Netzwerk-Komponenten beliebig umkonfigurieren kann (man nehme die 10 am häufigsten verkauften Produkte und ...). Weitere Beispiele? Was ist mit den hochgelobten neuen Redundanz-Mechanismen unserer Layer3-Switches. Wie sicher sind HSRP und VRRP? In welchem Umfang lassen sie beispielsweise eine unternehmensinterne Umlenkung aller relevanten Datenströme zu?

weiter auf Seite 2

Zum Geleit

Wer ist schneller, der Markt oder der Mensch ?

Liebe Leserinnen und Leser,

die letzten Wochen haben wieder eine unvorstellbare Flut von neuen Normungsansätzen, neuen Technologien, Produktankündigungen, Preissenkungen, Firmenübernahmen und neuen Erfahrungen gebracht. Es mag an der CeBit gelegen haben, aber trotzdem stellt sich die Frage: wer kann das noch verarbeiten ? Selbst Profis wie ComConsult, bei denen ganze Abteilungen vollzeitmäßig Markt- und Technologie-Entwicklungen beobachten und bewerten und die dabei den direkten Zugriff auf die Labors der Hersteller haben, kommen an ihre Kapazitätsgrenze.

Man nehme einen x-beliebigen Webserver eines großen Herstellers von Netzwerk-Komponenten und schaue sich die Änderungsgeschwindigkeit der Inhalte des Servers an. Welche Chance hat der normale Anwender, neben seiner 100%tigen Arbeitsbelastung dieser Entwicklung zu folgen ? Die Konsequenz: vermehrt treten signifikante Störungen in Netzen durch Fehlkonfigurationen von Geräten auf.

Welche Chance haben Hersteller und Vertreiber, dieser Entwicklung logistisch zu folgen. Man sehe sich ihre zunehmenden Probleme in der Konfiguration ihrer eigenen Produkte an und erkennt, daß auch hier die Grenze der Belastbarkeit längst überschritten ist. Man sehe sich die Bilanzen der führenden Hersteller an und erkennt, daß auch die Wirtschaftlichkeit dieser Entwicklung längst einem hemmungslosen Verdrängungswettbewerb gewichen ist.

Aber machen wir uns nichts vor. Natürlich macht diese Situationen einen großen Teil des Reizes unseres Berufs aus. Es wird eben nie langweilig, auch wenn wir in regelmäßigen Abständen unseren Kopf für irgendeine Störung hinhalten müssen.

Umsomehr sehen wir uns motiviert, Ihnen mit unserem "Netzwerk Insider" und unseren Seminaren und Kongressen aktuelles und praxisorientiertes Wissen direkt von der Quelle anzubieten. Wir denken, daß wir mit der Internet-Basis des "Netzwerk Insiders" genau den richtigen Weg zur schnellen und umfassenden Information unserer Kunden gewählt haben.

In diesem Sinne
Ihr Dr. Jürgen Suppan

Impressum

Verlag:
ComConsult
Technologie Information GmbH
Pascalstraße 25
D-52076 Aachen
Telefon 02408/14907
Telefax 02408/149233

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

Erscheinungsweise:
Monatlich
12 Ausgaben im Jahr

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

Für unverlangt
eingesandte Manuskripte
wird keine Haftung
übernommen

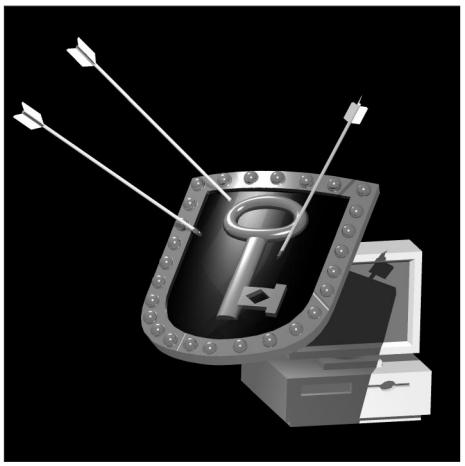
Sicherheitsrisiken nehmen zu - Fortsetzung von Seite 1

HSRP überträgt ein unverschlüsseltes Passwort, VRRP zwar als Option (nicht als Regel) ein verschlüsseltes, verhindert aber nicht eine Manipulation der Daten. Andere Sicherheitsrisiken liegen in der Veränderung der IP-Konfiguration von Endgeräten, die zu Störungen von Servern und zu Netzüberlastungen durch Route-Zyklen führen können.Es gibt weitere Beispiele (Sync-Angriffe, Blokade von Ports), aber die aufgeführten reichen sicher aus. Was kann dagegen getan werden? Natürlich sind interne und externe Firewalls eine interessante technische Antwort. Aber wer so argumentiert, macht aus einem organisatorischen Problem ein nur scheinbar leicht zu lösendes technisches Problem. Firewall-Betrieb bedeutet die Entwicklung eines Unternehmensweiten Grundverständnisses zu Sicherheitsrisiken. Wie erkläre ich den Mitarbeitern, daß ich Java oder PDF sperre, wenn selbst die Netzbetreiber monieren, daß sie durch diesen Filter den Online-Zugriff auf die CISCO oder 3Com-Handbücher verlieren. Dies ist nicht die Frage eines sicher möglichen hexadezimalen Filters, sondern der Bedarf nach einem zu begründenden, abzusichernden und zu pflegenden Sicherheitsstandard. Wer glaubt, dieses Problem mit Technik lösen zu können, wird spätestens am Personalbedarf des Betriebs einer wirklich funktionsfähigen Firewall scheitern. Die Schaffung eines gemeinsamen Grundverständnisses zum Thema Sicherheit und die Bereitschaft, es wirklich zu Leben, nur darin kann die Lösung liegen. Dazu gehört auch die Frage, wie Mitarbeiter bestraft werden, die gegen Sicherheitsrisiken verstoßen. Sicher nicht dadurch, daß der Betriebsrat als erstes die Sozialverträglichkeit der Bestrafung als Gegenstand einer mittelfristig angelegten Kommission zur Schaffung einer geeigneten Betriebsvereinbarung macht.Was kann und muß noch getan werden? Nun, natürlich müssen wir den marktdominierenden Herstellern wie 3Com, Bay, CISCO wesentlich mehr Feuer unter dem Hintern machen. Nur wenn diese Hersteller das Gefühl haben, daß der Kunde auf der Basis von Sicherheitsfragen Kaufentscheidungen trifft, wird sich etwas ändern. Auch dies ist genau die Frage nach einem in den Unternehmen gelebten Sicherheitsverständnisses. Dazu gehört natürlich auch ein Prozeßverantwortlicher mit den ausreichenden Kompetenzen (heißt: Weisungsbefugnis in Sicherheitsfragen gegenüber wesentlich ranghöreren Entscheidungsträgern). Wer sich für diese Fragen, seien sie technisch oder organisatorisch, interessiert, der sei auf unser hochaktuelles Sicherheitsforum vom 7. bis 9. Juni zu diesem Thema verwiesen. Erfahrungsberichte, viele Tips aus der Praxis und natürlich Informationen über die neuesten Bedrohungen und die zugehörigen Abwehrmaßnahmen machten auch schon in den Vorjahren diese Veranstaltung zum Treffpunkt aller sicherheitsbewußten Netzwerk-Betreiber.

Mit aktuellen Infos

Netzwerk Sicherheits-Forum 1999

Lange Zeit nur mit mäßiger Aufmerksamkeit bedacht, sind die wichtigsten Problembereiche der Netzwerk-Sicherheit bei den meisten Unternehmen nunmehr erkannt und thematisiert worden.
Erste Schutzmaßnahmen wie der Einsatz von Firewallsystemen oder die Verwendung von starken Verschlüsselungs- und Authentisierungsverfahren sind zumeist eingeführt worden, aber immer noch verbleiben eine Vielzahl offener Punkte. So fehlt häufig die Basis eines fortschreibungsfähigen Sicherheitskonzeptes, die Schutzmaßnahmen werden nicht an neueste Bedrohungen angepaßt oder sind durch das Fehlen weiterer wichtiger Sicherheitskomponenten leicht zu unterlaufen. Dies ist um so gefährlicher, wenn man die ständig zunehmenden Möglichkeiten potentieller Eindringlinge betrachtet.Auch der diesjährige Kongreß wird sich nicht auf die Darstellung vorhandener Sicherheitsprobleme beschränken, sondern insbesondere hierzu Lösungsmöglichkeiten aufzeigen. Diese Veranstaltung ist für jeden



Erhebliche Bedrohung

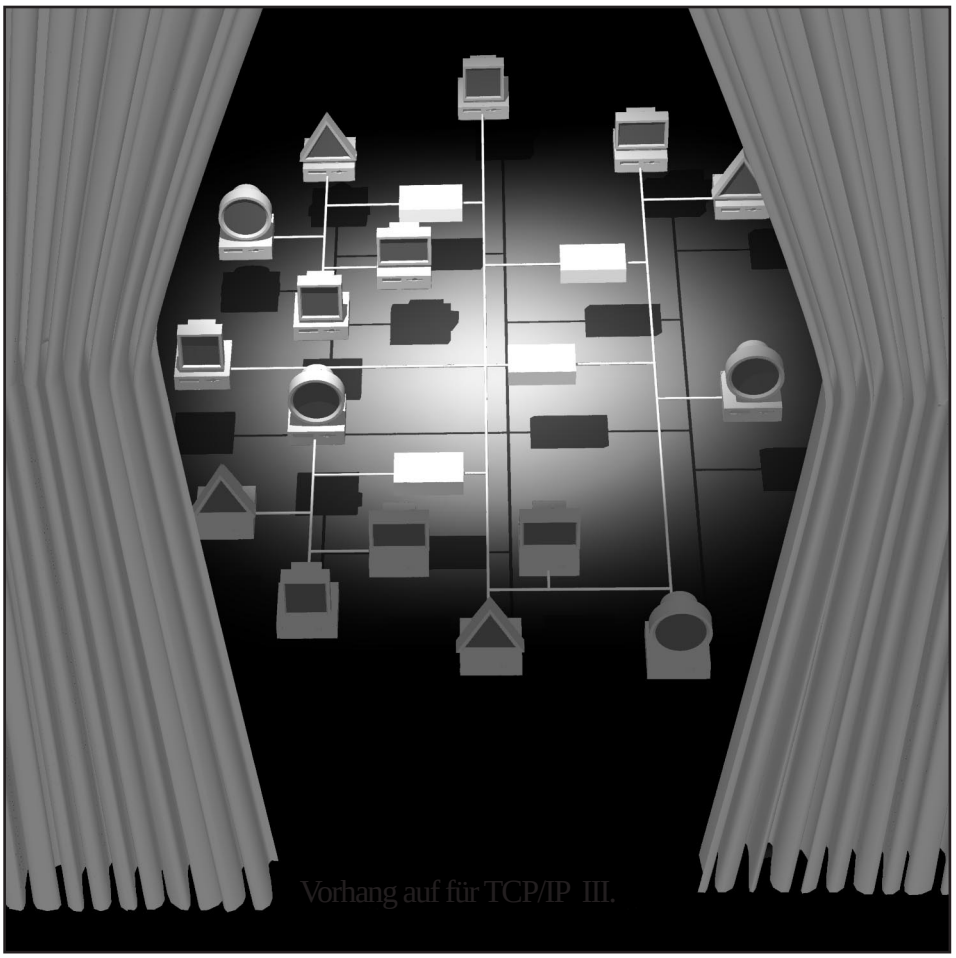
Sicherheitsverantwortlichen, Netzwerk-Administrator und auch allgemein an Sicherheitsfragen Interessierten zu einer unverzichtbaren Plattform für aktuelle Informationen, Produktvergleiche und anregenden Fachdiskussionen geworden. Bekannte Experten geben Einblick in den aktuellen Stand der Netzwerk-Sicherheit, wobei größter Wert auf Praxisnähe gelegt wird. Die Teilnehmer werden damit in die Lage versetzt, Ihre Sicherheitsprobleme selbst besser einzuschätzen und die notwendigen organisatorischen und technischen Gegenmaßnahmen zu treffen. Unter anderem sollen folgende Fragestellungen beantwortet werden:
Wie sind Sicherheitsanalyse und Sicherheitskonzept effizient zu erstellen? Welche Sicherheitsprobleme werden bei "Remote Access" unterschätzt? Ein Firewall ist installiert, was fehlt jetzt noch? Wie lassen sich sichere E-Mail Lösungen aufbauen? Sind die Betriebsrisiken einer Webpräsenz zu beherrschen? Wie sicher sind meine Daten beim Internet-Provider? Sind Verschlüsselung und Key-Management schon heute zu beherrschen? Unterläuft "Malicious Code" meine vorhandenen Sicherheitsmaßnahmen?

Tips + Tricks

Dipl.-Inform. Detlef Weidenhammer informiert mit "Netzwerk-Sicherheit: Konzepte - Produkte - Realisierungen" praxisnah über die erfolgreiche Umsetzung von Sicherheits-Lösungen für Netzwerke und liefert damit die ideale Basis für die Durchführung entsprechender Projekte.
Der Report basiert auf einer Reihe von erfolgreichen Sicherheitsprojekten, für die der Autor vom Konzept bis zur Realisierung verantwortlich war. Man findet in diesem Report neben Gefahrenbeschreibungen, Konzeptdarstellungen und Produktübersichten viele nützliche und erfolgsrelevante Tips aus der Praxis.
Der Leser erfährt wo die Sicherheit im Netzwerk-Betrieb gefährdet ist und wie eine Sicherheits-Planung erarbeitet wird. Welches die erfolgs-versprechendsten Sicherheitsmaßnahmen sind und wie Zugriffsschutz, Prüfung der Authentität, Vertraulichkeit sensibler Daten im Netzwerk umgesetzt werden können. Wie man Angriffsversuche erkennt und wie sie berichtet werden. Welche Produkte es gibt und wie die Projekt-realisierung aussieht, welche Betriebsaufwände entstehen, und inwieweit sie den Erfolg gefährden. Auch die Produktsituation im Bereich Firewall-und Remote-Access-Server wird ausgiebig behandelt. Der Report gibt eine breite Produktübersicht und ist die ideale Basis für die Auswahl des geeigneten Produkts.

Neues CCNE-Seminar

Heterogene Netze mit TCP/IP



Vorhang auf für TCP/IP III

Zum Thema

Mit TCP/IP steht bereits seit längerer Zeit eine erprobte Protokollfamilie zur Kommunikation in heterogenen Netzen zur Verfügung.
Ihre Leistungsfähigkeit und insbesondere die Möglichkeit, auch größte Netzwerke mit nur einem geringen Maß an zentraler Organisation aufzubauen und effektiv zu betreiben, trug wesentlich zum Erfolg des weltumspannenden Internets bei.
Aber auch in Lokalen Netzen hat sich TCP/IP weitgehend durchgesetzt, da es bei der Vernetzung über Hersteller- und Betriebssystemgrenzen hinweg deutliche Vorteile gegenüber anderen Lösungen bietet.
Da die Unterstützung durch alle namhaften Hersteller gegeben ist, entwickelt sich TCP/IP zunehmend zur alleinigen Basis der Kommunikation in lokalen und globalen Netzen.
Bei sorgfältiger Beachtung aller Empfehlungen zu Adressierung, Routing, Sicherheit und Systemkonfiguration sind auch stark heterogene Netze mit einem überschaubaren Betreuungsaufwand erfolgreich zu betreiben.

Neben den Seminaren "TCP/IP und SNMP" und "Betrieb von TCP/IP" bietet die ComConsult Akademie jetzt ein drittes Seminar zur TCP/IP-Thematik an. Der Titel des dreitägigen Seminars, das 1999 viermal stattfindet, lautet: "Heterogene Netze mit TCP/IP: Von den Grundlagen zum erfolgreichen Einsatz".
Anders als "TCP/IP und SNMP", das wegen seiner inhaltlichen Überschneidung im SNMP-Bereich mit dem dritten Seminar der Ausbildung zum "ComConsult Certified Network Engineer","Neue Ethernet-Technologien" seit geraumer Zeit nicht mehr zum CCNE-Zyklus gehört, soll "Heterogene Netze mit TCP/IP" genau wie "Betrieb von TCP/IP" schon von der Konzeption her in den CCNE-Zyklus eingebunden werden.
Referenten sind der Geschäftsführer der GAI-NetConsult, Dipl.-Inform. Detlef Weidenhammer und Dipl.-Phys. Frank Breitschaft, die schon zusammen das Seminar "TCP/IP und SNMP" leiten.
Dipl.-Phys. Frank Breitschaft besitzt langjährige Erfahrung im Betrieb heterogener Netze. Im Bereich Netzwerkentwicklung und Netzwerkberatung bei der GAI NetConsult GmbH tätig, liegt sein Schwerpunkt im Bereich der Beratung und Planung von Netzen - insbesondere unter Sicherheits-aspekten - und in der Projektbetreuung bei der Einführung von Netzwerkdokumentationen.Dipl.-Inform. Detlef Weidenhammer ist als Geschäftsführer der GAI NetConsult GmbH vorwiegend auf den Gebieten Internet/Intranet und Netzwerk-Sicherheit tätig. Basierend auf langjähriger praktischer Tätigkeit bringt er seine Erfahrungen als Fachberater und auch als Referent bei Seminaren und Kongressen ein. Dieses Seminar vermittelt die wesentlichen Kenntnisse, die zum Aufbau und störungsfreien Betrieb eines TCP/IP-basierenden Netzwerkes benötigt werden. Für Ein- und Umsteiger in diese Thematik werden zu Beginn auch Grundkenntnisse vermittelt, bevor in Fallstudien und konkreten Beispielen tiefer in die Problematik eingestiegen wird.
Die Teilnehmer lernen im Seminar, wie sie den Betrieb von IP-Netzen automatisieren und verbessern können, die zentralen Protokolle IP, TCP und UDP im Detail kennen; wo sich Optimierungsmöglichkeiten bieten und wie sich Fehlkonfigurationen vermeiden lassen, wie ein lokaler IP-Adreßbereich durch Subnetzbildung strukturiert werden kann und welche Fehler dabei unbedingt zu vermeiden sind, wie sie durch automatische Adreßvergabe mit DHCP den Konfigurationsaufwand reduzieren und Fehlersituationen verhindern können, wie sie den DNS-Dienst betreiben und in Ihr Netzwerk integrieren können, die wichtigsten Routingprotokolle gegeneinander abzuwägen und eines für Ihren Bedarf auszuwählen, wie sie auch die Windows-Welt effizient in einem IP-Umfeld betreiben können und wie sie weltweite Konnektivität durch den Anschluß an das Internet erhalten. Außerdem die Sicherheitsschwächen von IP genauso wie die entsprechenden Schutzmaßnahmen kennen.

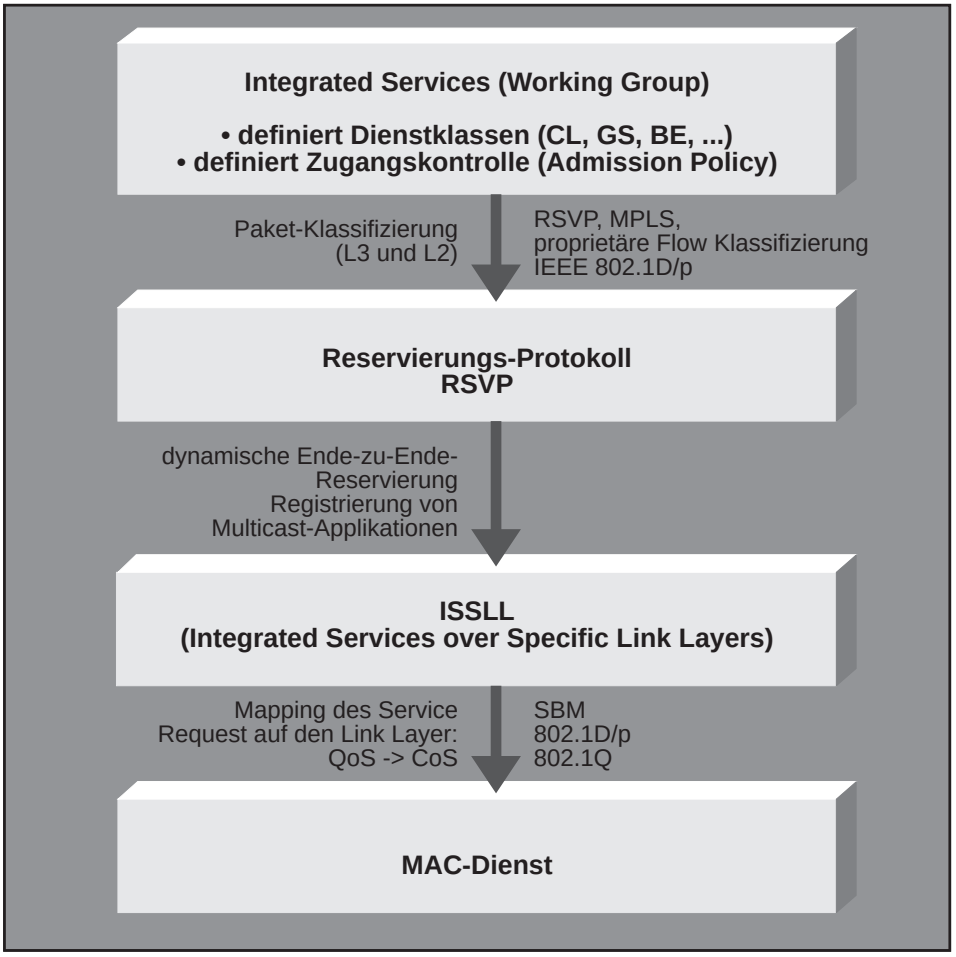
Quality of Service im LAN: Leistung kontra Komplexität

In WAN-Umgebungen kommen Ansätze wie DS, MPLS oder auch das proprietäre Tag Switching (Cisco) zum tragen, auf die in einer nachfolgenden Ausgabe einzugehen sein wird. Für eine QoS-Implementierung sind zwei Kriterien zu erfüllen:

• Einzelne Netzelemente (Verbindungen, Subnetze und Router) müssen entlang eines Gesamtweges (Path) den QoS kontrollieren können.
• Die Anforderungen einer Applikation müssen den Netzelementen auf dem Gesamtweg mitgeteilt werden können.

Die Arbeitsgruppe "Integrated Services" der IETF hat bislang zwei Grund-Dienstklassen spezifiziert: Controlled Load (CL) und Guaranteed Service (GS). Darüber hinaus erarbeitet sie eine Basis-Definition für Zugangskontrolle (Admission Policy). Um eine Kommunikationssitzung beziehungsweise einen "Flow" einer bestimmten Dienstgüte zuzuordnen, müssen die Pakete entsprechend klassifiziert werden können, z.B. über RSVP, DS und MPLS auf Ebene 3 oder über IEEE 802.1D/p und IEEE 802.1Q auf Ebene 2. Diese Flow-Klassifizierung muß zu einer Ende-zu-Ende durchgeschalteten Reservierung oder Priorisierung führen, die auf klassischen Data Link Ebenen wie Ethernet oder Token Ring abläuft. Hier kommt die IETF-Arbeitsgruppe ISSLL (Integrated Services over Specific Link Layers) ins Spiel, die Protokolle spezifiziert, um eine bestimmte reservierte Dienstgüte (QoS) auf eine Dienstklasse (Class of Service CoS) abzubilden. Ebene-2-Dienstklassen sind in den Standards IEEE 802.1D/p und 802.1Q über Prioritätsklassen vordefiniert. Das Zusammenspiel verschiedenen Protokollebenen ist in Bild 1 dargestellt. Eine einzige Annahme liegt dabei allen Ansätzen zugrunde: Die Netze sind "Switch-rich", d.h. zwischen Sender und Empfänger ist mindestens ein Layer-2-Switch ("Bridge", MAC-Kopplung) oder Layer-3-Switch ("Router", geroutete Kopplung) positioniert, in dem die Bearbeitung von Serviceklassen stattfinden kann. Nach wie vor verwendet die Standardisierung hier konservativ die Begriffe Bridge und Router anstelle von Layer-2- und Layer-3-Switch! Nachfolgend werden die einzelnen QoS-Verfahren von den unteren zu den höheren Ebenen betrachtet.

Bild 1 DS, RSVP, 802.1D/p und 802.1Q



Erweiterter MAC-Dienst: Priorisierung und Multicast-Registrierung mit IEEE 802.1D-1998

Die ursprüngliche Standard-Erweiterung 802.1p wurde als so wichtig eingestuft, daß sie in eine neue Version 802.1D-1998 des Basisstandards 802.1D für Brückentechnik eingearbeitet wurde. Als erweiterte Filterfunktionalität von Brücken (d.h. Layer-2-Switches) wird hier ein Konzept mit Priorisierungen definiert, die Ende-zu-Ende signalisiert werden. Die optionalen erweiterten Filter beinhalten:

- Filter für bevorzugten Verkehr (Expedited Traffic)
- Multicast-Filter
- Dynamische Registrierung von Gruppen, insbesondere Multicast-Gruppen

Aktuell ist eine statische Priorisierung mit den Werten 0..7 definiert. Vorgeschlagen wird mindestens eine zweistufige Dienstklassen-Implementierung von 0..3 für unkritische Applikationen und 4..7 für Realzeit-Applikationen. Darüber hinaus ist eine beliebige Verfeinerung denkbar, da jeder Switch eine eigene Implementierung von 802.1D haben kann. Dies erlaubt ihm, mit eigenen spezifischen Warteschlangen (Queues) und Bearbeitungsverfahren zu arbeiten wie

- Zwei Queues und statische Priorisierung (802.1D Default)
- Zwei bis acht Queues pro Port und statische Priorisierung (802.1D Option)
- Acht Queues pro Port und relative Priorisierung (WFQ, WRR)
- Mehrere Queues pro Port, Flow Klassifizierung nach Layer-3-Header, separate komplexe Policy je Flow, Reshaping an jedem Switch

Für die acht Prioritäts-Werte wird eine Abbildung auf verschiedene Verkehrsstypen (CoS, siehe auch Bild 2) vorgeschlagen, die in etwa auch dem Vorschlag der Integrate Services Arbeitsgruppe der IETF entspricht: 1=BK, Hintergrund-Verkehr und Rückstufungsklasse für Applikationen, die die zugebilligte Dienstgüte überlasten, 0=BE, Best Effort als Default entsprechend des klassischen LAN-Verhaltens, 3=EE Excellent Effort als erste bevorzugte Dienstklasse, 4=CL als erste Priorität im Rahmen typischer "mission-critical-Applikationen", 5=VI für Video-Applikationen mit der typischen Zeitgrenze von 100 Millisekunden Delay, 6=VO für Sprach-Applikationen mit der erheblich stär-

keren Restriktion von 10 Millisekunden Delay, 7=NC für Netzwerksteuerung und -management.

Die Wahl von (nur) acht Prioritätsstufen stellt z.B. verglichen mit ATM eine radikale Vereinfachung dar, um die "High Speed - Low Cost"-Philosophie der Brückentechnik beizubehalten. Die Zielsetzungen dabei waren in erster Linie Delay-Management für neue Realzeit-Applikationen, in zweiter Linie Durchsatz-Management in Form von Service-Level Agreements für wichtige bereits etablierte Applikationen. Ein Einsatz-Beispiel könnte wie folgt aussehen: Die betriebenen Switches unterstützen fünf Queues, somit sind maximal fünf Classes of Service realisierbar. 802.1D schlägt folgende Zusammenfassung vor: Queue1=Background, Queue2=Best Effort und Excellent Effort, Queue3=Controlled Load, Queue4=Video, Queue5=Voice und Network Control. Die Zuordnung von Applikationen könnte sein: BK=Mail, BE/EE=Office-Applikationen, CL=SNA-Host, Unix-Datenbank und RMONv2, VI=Videokonferencing, VO/NC=Telefonie über IP, und SNMP-Polling, Traps.

Die drei Prioritäts-Bits können auf die drei Precedence-Bits des IPv4 TOS Feldes oder auf Class Selector Codepoints des DS Byte (siehe unter Differentiated Services) gemappt werden. Somit ist eine Basis-Kompatibilität erreichbar und die Möglichkeit gegeben, auf Layer 2 und Layer 3 eine durchgängige Class-of-Service-Strategie zu fahren.

Multicast-Applikationen werden über ihre MAC-Multicast-Adresse identifiziert und können über GARP und GMRP mit bestimmten Filtervoreinstellungen und spezieller Priorisierung je Multicast-Applikation dynamisch an Switchports registriert werden. Mit GARP werden die Gruppen-Attribute und Dienstgüte-Parameter von sogenannten GARP-Applikationen, z.B. Multicast-Applikation bekanntgegeben (und auch wieder gelöscht). Jede GARP Applikation arbeitet mit einem sogenannten Context, dessen Semantik die zugehörigen Ports festlegt. der Standard-Kontext (default) ist die aktive Spanning Tree Konfiguration, in einer VLAN-Umgebung sind auch andere Contexts möglich (VLAN-bezogen). GMRP ist eine GARP-Applikation, die für Multicast-Gruppen zu einem aktuellen Zeitpunkt die dynamische Registrierung / Deregistrierung an einem Switch oder Switchport veranlaßt und über GARP zwei Attribut-Typen registrieren läßt: die benutzte MAC-Multicast-Adresse und die Dienstanforderung mit den Parametern "All" und "All Unregistered" (All = Forward all Groups d.h. nur die registrierten Multicast-Applikationen werden weitergeleitet; All Unregistered = Forward all Unregistered Groups d.h. die nicht registrierten Multicast-Applikationen werden auch weitergeleitet, und zwar an alle Ports). Ist eine Multicast-Gruppe registriert, so werden die entsprechenden Frames nur an die Ports weitergeleitet, für die die Registrierung gilt.

Da IP Multicasts auf MAC-Multicasts gemappt werden, sind konsistente Multicast-Strategien mit separater Multicast-Priorisierung und Behandlung in Layer-2/3 Mischkonfigurationen möglich. Die getrennte Handhabung von Multicast- und Unicast-Applikationen wird beim DS-Konzept auch für große Verbundnetzwerke vorgeschlagen. Ein konsistenter LAN/WAN-Betrieb ist somit auf Basis der neuen 802.1D-1998 Version möglich.

Bild 2 Beispiel für Prioritätswerte und Verkehrstypen (CoS)

user priority	Abkürzung	Verkehrs-Typen
1	BK	Background (Hintergrund)
2	-	Frei
0 (Default)	BE	Best Effort
3	EE	Excellent Effort
4	CL	Controlled Load
5	VI	"Video", <100 Millisec. Latenz und Jitter
6	VO	"Video", <10 Millisec. Latenz und Jitter
7	NC	Network Control

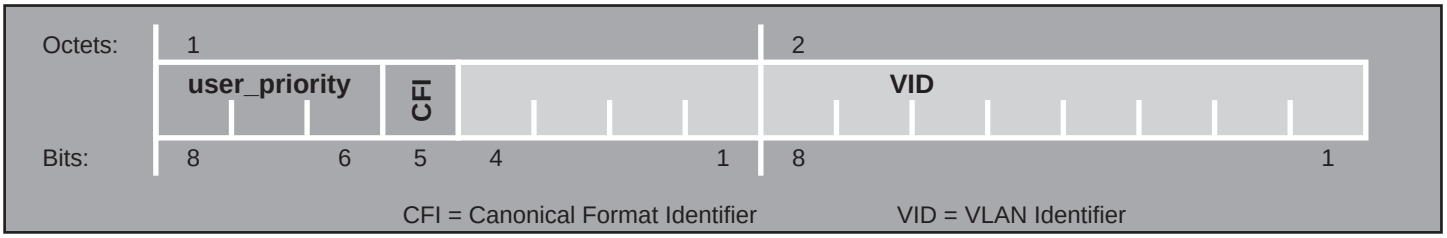
Erweiterung der Priorisierung auf Organisations-Einheiten: IEEE 802.1Q

Das Grundkonzept benutzt die Definition von VLANs je Port. Frames werden durch einen sogenannten Tag (2 Byte Kennung im Anschluß an die MAC-Adressen) einem bestimmten VLAN zugeordnet. MAC-Adressen werden je VLAN gelernt; somit können doppelte MAC-Adressen in unterschiedlichen VLANs unterstützt werden. Die VLAN-Technik nach IEEE 802.1Q erlaubt einige Verbesserungen:

- Tuning durch eine organisationsgerechte Verbindung von Layer-2- und Layer-3-Strukturen, insbesondere bei einer Konfiguration mit Microsegmentierung / dediziertem LAN und zentralen Server-Pools
- Benutzergruppenbezogene Priorisierung bestimmter Applikationen bzw. Verkehrstypen durch die Erweiterung von 802.1D auf separate Benutzergruppen
- Dynamische Einbindung von Multicast-Applikationen je Benutzergruppe. Je Port und je VLAN kann für einzelne Multicast-Gruppen das Default-Filtern konfiguriert werden

Der eigentliche Tag besteht aus 2 Byte, wobei die ersten 3 Bit die Prioritäts-Bits aus

Bild 3 IEEE 802.1Q Tag Format



Quality of Service im LAN: Leistung kontra Komplexität

802.1D-1998 sind, gefolgt von einem Token Ring Encapsulation Flag; Bit 5 bis Bit 16 enthalten die VLAN-Kennung (VID) als Integer Wert (siehe Bild 3). Das CFI-Bit wird auf 1 gesetzt, wenn ein Token Ring Frame in ein Ethernet Frame enkapsuliert über einen High Speed Backbone (Gbit, 100Base-FX) übertragen wird. Damit erhalten Token Ring Segmente die wenn auch weniger performante Chance, auch bei der Migration zu Hochgeschwindigkeiten weiterhin mit durchgeschleppt zu werden.

Über ein spezielles Protokoll, GVRP (GARP VLAN Registration Protocol) können dynamische VLAN-Zugehörigkeiten am Switch registriert werden, z.B. wenn ein Switch über Abhören von IGMP erkennt, daß Endgeräte an einer bestimmten Multicast-Applikation teilnehmen wollen. Die entsprechende Multicast-Applikation wird dann einem dynamischen VLAN zugeordnet, das an allen Ports aktiviert wird, an denen teilnahmewillige Endgeräte angebunden sind. Oder aber eine bestimmte Multicast-Applikation wird nur einer einzigen Gruppe von Benutzern zugänglich gemacht, die über dann einem gemeinsamen VLAN zugeordnet werden. Beliebige Kombinationen sind dabei denkbar.

Ein Beispiel: Die Finanzabteilung eines Unternehmens nutzt die Multicast-Applikationen "Börseninformations-Dienste", "Videokonferenz" und darüber hinaus Hostzugriff mit SNA/DLSw, Datenbank-Zugriff mit TCP, Office-Anwendungen. Der Vertrieb nutzt die Multicast-Applikation "Internet-Werbung" sowie Hostzugriff mit SNA/DLSw und Office-Anwendungen. Die Entwicklung nutzt als Multicast-Applikation "Internet-Trainings" und "Kundenschulung", außerdem Datenbank-Zugriff mit TCP und Office-Anwendungen. Lösung: Jede Abteilung wird einem separaten VLAN zugeordnet. Die jeweilige Multicast-Applikation wird nur für diese Abteilung zugelassen, für alle anderen gesperrt. Server mit Applikationen, die von mehreren Abteilungen genutzt werden, werden mehreren VLANs zugeordnet. Die Multicast-Applikationen werden mit höchster Priorität

Tabelle QoS Ansätze für LANs

Protokoll	Bedeutung	Arbeitsgruppe	Zielsetzung	Informationen
DS	Differentiated Services	IETF / DIFFSERV	Class of Service, SLA's	http://ietf.org/ids.by.wg/diffserv.html;RFC's 2474, 2475
RSVP	Resource ReSerVation Setup Protocol	IETF / RSVP	QoS Signalisierung: Schaltung einer Ende-zu-Ende Reservierung zwischen Netzknoten (Client, Server)	http://ietf.org/ids.by.wg/rsvp.html; RFC's 2205, 2207, 2208, 2210
COPS	Common Open Policy Service Protocol	IETF / RSVP Admission Policy (RAP)	Client-Server Modell um Policy Kontrolleüber DS/CoS und QoS Signalisierungs-Protokolle, z. B. RSVP, zu unterstützen	http://ietf.org/ids.by.wg/rap.html
ISSLL Framework	Integrateted Services over Specific Link Layer Architektur	IETF / ISSLL	Realisierung von Dienstgüte in Form von Dienstklassen (CoS) auf Link Protokolle mit reinen Frame-Technologien	http://ietf.org/ids.by.wg/issll.html
CL	Controlled Load	IETF / ISSLL	Bevorzugte Bearbeitung	RFC 2211
GS	Guaranteed Service	IETF / ISSLL	Reservierung/Garantie einer maximalen Antwortzeit (Delay)	RFC 2212
802.1D/p	MAC Bridges	IEEE LMSC	Integration neuer Funktionen in den Basis-Brückenstandard: Priorisierung und dynamische Multicast-Registrierung	ftp://p8021:-go_wildcats @p8021.hep.net/8021/d-drafts/
802.1Q	Virtual Bridge Local Area Networks	IEEE LMSC	Erweiterung der 802.1D/p-Funktionalität auf Virtuelle LANs	ftp://p8021:-go_wildcats @p8021.hep.net/8021/d-drafts/
GARP	Generic Attribute Registration Protocol	IEEE LMSC	Protokoll, um Gruppen-Attribute für Applikationen dynamisch an einem oder mehreren Switches bzw. Switchports zu registrieren	ftp://p8021:-go_wildcats @p8021.hep.net/8021/q-drafts/
GMRP	GARP Multicast Registration Protocol	IEEE LMSC	Protokoll, um eine Multicast-Applikation oder Multicast-Gruppe dynamisch zu registrieren	ftp://p8021:-go_wildcats @p8021.hep.net/8021/d-drafts/
802.3x	802.3x&y-1997 Supplements to ISO/IEC 8802-3: 1996	IEEE LMSC	Flußkontrolle und Full-Duplex Operation für Punkt-zu-Punkt Verbindungen, 100 Mbit/s Ethernet	http://standards.ieee.org/catalog/IEEE802.3.html

belegt (VI/VO/NC), SNA und Datenbank als mission-critical eingestuft (CL oder SNA=CL und Datenbank=EE), Office-Anwendungen erhalten die niedrigste Priorität (BE).

Im wesentlichen sollten VLANs einfach und überschaubar eingerichtet werden: Nur ein VLAN pro Switchport und nur in wenigen Ausnahmefällen gebäudeübregreifende VLANs. Somit reduziert sich die VLAN-Technik auf die Bildung von Portgruppen bei einem Layer-3 Switch.

Flow-basierte Reservierung: RSVP

Für begrenzte Netzumgebungen wie z. B. LANs muß nicht immer eine Beschränkung auf eine Basis-Priorisierung mittels Class of Service erfolgen. Hier kann auch eine Priorisierungs- und Reservierungs-Technik für einzelne Kommunikationsbeziehungen erfolgen, sogenannte Flows. Das Resource Reservation Setup Protocol war ursprünglich zur Realisierung von Multimedia-Applikationen gedacht, beschreibt jedoch inzwischen die Signalisierung zur dynamischen Ressourcen-Reservierung sowohl für Unicast- als auch für Multicast-Applikationen. Von der Applikation werden "irgendwie" die Reservierungs-Parameter besorgt und an den RSVP-Prozeß weitergegeben wie in Bild 4 dargestellt. Dieser fragt eine lokale oder zentrale Policy Kontrolle, ob die Reservierung überhaupt berechtigt ist. Falls ja, wird die Admission-Kontrolle angefragt, ob die Reservierung aktuell technisch machbar ist (CPU-Kapazität, Speicherplatz für die Reservierung, Interface-Auslastung etc.). Ist die technische Machbarkeit gegeben, wird das Paket klassifiziert, an den Scheduler weitergegeben und in die entsprechend hoch oder niedrig priorisierte Bearbeitungs-Warteschlange eingereiht.

Über getätigte Reservierungen wird in den beteiligten Routern (Layer-3-Switches) eine Zustandsprotokollierung mitgeführt, was für die beteiligten Geräte hohen CPU- und Speicheraufwand bedeutet und mit heutiger Gerätetechnik nur eine mittlere Skalierbarkeit erlaubt. Die eigentliche Zugangs-Kontrolle sowie die tatsächlichen Dienstgüte-Parameter sind für RSVP transparent, da RSVP lediglich für den Reservierungsvorgang, nicht jedoch für die Inhalte zuständig ist. RSVP kann Sender- oder Client-getriggert ablaufen.

Im Sender-Modell registriert sich z.B. eine Multicast-Applikation bei RSVP und teilt dabei ihre Verkehrscharakteristik in Form von Dienstgüte-Parametern mit. Danach werden sogenannte Path Messages "downstream" zu allen potentiellen Empfängern weitergeleitet. Ein Client, der an dieser Multicast-Applikation teilnehmen will, leitet eine Path-Nachricht über das RSVP API an seine Applikation weiter. Diese wählt entsprechende Parameter aus (Path_MTU, PackSize, Controlled Load oder Guaranteed Service, min. Durchsatz, max. Delay, ...) und übergibt sie der lokalen RSVP-Schnittstelle. RSVP startet daraufhin die Reservierungs-Anfrage von der Empfängerstation in Richtung Sender, also "upstream". Ein wichtiger Aspekt für Multicast-Applikationen ist dabei, daß gleichartige Reservierungen auf dem Weg zum Multicast-Sender mittels MERGE zusammengefaßt werden, da die Pakete ja nur insgesamt einmal für alle Empfänger auf diesem Weg generiert werden und Bearbeitungsleistung erfordern. Kopiert werden müssen Pakete erst dort, wo sich ein Sender-Empfänger-Pfad endgültig verzweigt.

Beim Host-Modell registriert sich ein Client in einer Multicast-Gruppe (z.B. mit IGMP). Der Server dieser Multicast-Gruppe sendet intervallmäßig Path-Nachrichten, die den registrierten Client downstream erreichen. Der Client generiert daraufhin eine Reservierungs-Anfrage wie beim Server-Modell beschrieben. Router verhalten sich wie Hosts und geben Reservierungs-Anfragen upstream weiter. Zukünftig ist denkbar, daß

Bild 4 RSVP Implementierung im Endgerät und Koppelgerät

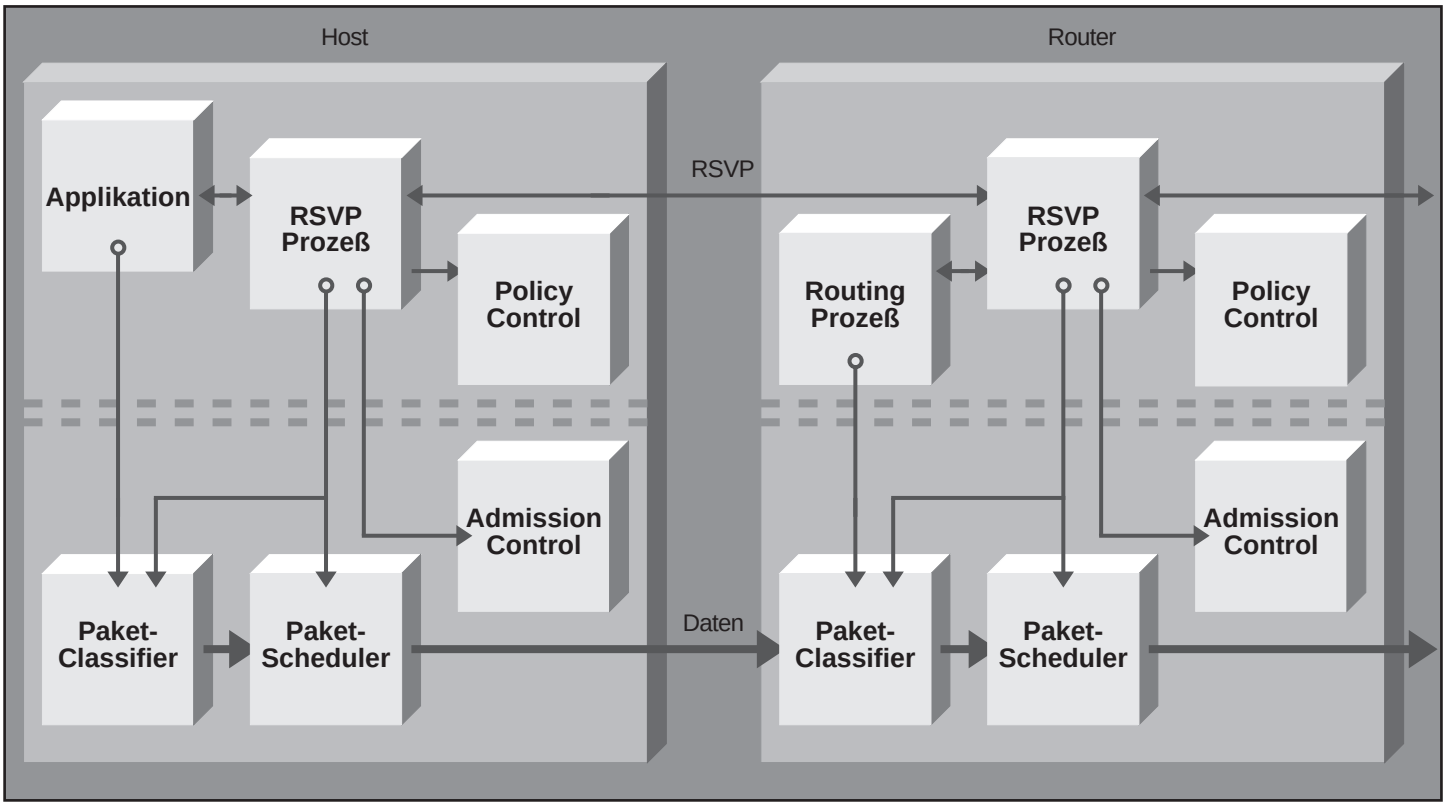
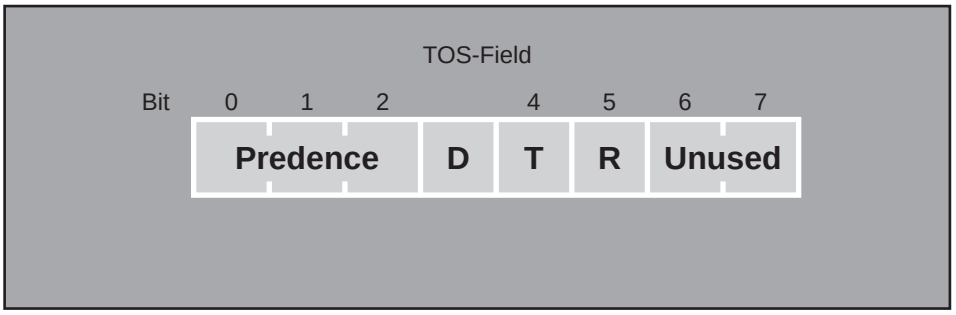


Bild 5 TOS Byte bei IP Version 4



Path Messages in Routing Protokolle integriert werden, jedoch erst wenn die Router das sogenannte Reverse Path Forwarding unterstützen (Aufbau von Multipunkt-zu-Punkt Baumstrukturen, d.h. Zusammenfassen mehrerer Path Nachrichten zu einer einzigen Path Nachricht, die dann noch den Server erreicht, um den Overhead für Path Nachrichten zu optimieren).

Applikationen, die über RSVP mit QoS-Reservierung versehen werden können, sind z.B. Online-Dienste (Wetter, Börse, Werbung, Touristik), Video-Dienste mit ggf. mehreren Kanälen zur Auswahl als Multicast-Applikation, aber auch SNA/DLSw, wichtige Intranet-Applikationen oder Telefonie über Internet. Da RSVP Reservierungen durch Flow Klassifizierung je Client separat schaltet und verwaltet, entsteht relativ hoher Overhead und es ist eher als Zugangstechnik ("Edge-Technik") denn als Backbonetechnik einzustufen. Im Backbone sollten stattdessen weniger CPU- und Speicher-intensive Verfahren eingesetzt werden, z.B. DS auf der Basis von Dienstgüte-Klassen (CoS), wie z.B. IEEE 802.1D-1998 / 802.1Q und DS sie vorschlagen.

Class of Service Konzept: Differentiated Services (DS)

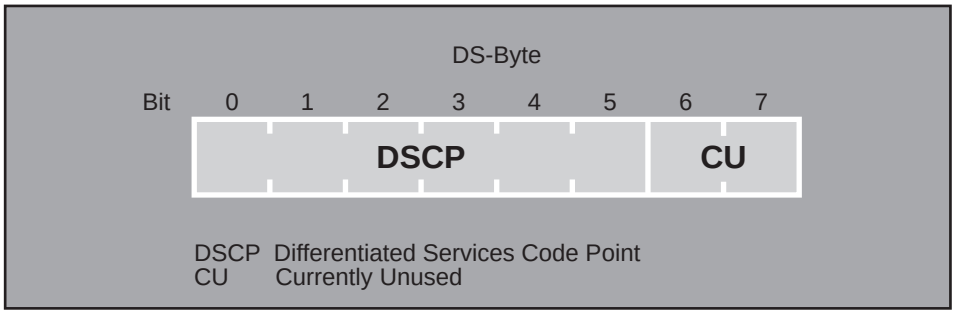
Für große Internetzwerke ist eine rein endgerätebezogene Flow-Behandlung zu aufwendig. Gleichartige Sessions werden daher zu sogenannten Dienstklassen (Class of Service) zusammengefaßt und nach demselben Service Level bearbeitet: Dienstgüte wird nicht mehr auf einer Per-Micro-Flow Basis gehandhabt sondern für gleichartige Kommunikationsbeziehungen und Applikationen aggregiert. Diese Reduzierung führt zu einer erheblich besseren Skalierbarkeit, da die Bearbeitungs-Komplexität so weit wie möglich aus dem Kernbereich (Core) des Netzes herausgenommen und von den Zugangsgeräten geleistet wird, die ein niedrigeres Verkehrsaufkommen und weniger Flows handhaben müssen.

Mit dem Differentiated Services Konzept hat ein Carrier/Internet Provider die Möglichkeit, den Kunden eine Reihe von Netzdiensten anzubieten, die sich nicht nur nach Preisgruppen sondern auch tatsächlich kontrollierbar nach Performance unterscheiden. Der Kunde schließt vertraglich einen bestimmten Performance Level ab, der auf IP-Paketbasis durch entsprechende Werte in einem sogenannten DS-Feld eingetragen wird und zur entsprechend bevorzugten oder benachteiligten Behandlung innerhalb des Providernetzes führt. Typischerweise gehört zum Service-Profil, das zwischen Provider und Kunde vertraglich abgeschlossen wird, die Festlegung der Zugangsrate und in wenigen Fällen des Delays. Überschreitet der Kunde die vertraglich zugesicherten Raten, ist die vereinbarte Dienstgüte für den Mehranteil nicht mehr garantiert (Rückstufung auf einen Default Level). Zusammenfassend gilt:

- DS Dienste sind immer ausschließlich für unidirektionale Verkehrsströme definiert
- DS Dienste sind immer für aggregierten Verkehr definiert, nicht für individuelle Micro-Flows

Zur Implementierung des Differentiated Services Konzepts wird ein Byte im IP-Header benutzt, das in den IP Protokollversionen vorhanden ist: Das TOS Byte bei IPv4 (siehe Bild 5) und das Traffic Class Byte bei IPv6.

Bild 6 DS Byte



Dieses Byte erhält eine neue Aufteilung und wird DS Byte genannt: Bit 0 bis 5 ist der DSCP-Wert (Differentiated Services Code Point), Bit 7 und 8 sind reserviert (CU, Currently Unused) wie in Bild 6 dargestellt. Ein eingetragener Wert entspricht einer Service-Klasse und heißt Codepunkt (Codepoint). Codepunkte, die in etwa rückwärtskompatibel zu IPv4 TOS sind, heißen Class Selector Codepoint, wobei ein Class Selector den Wert 'xxx000' hat und somit jeweils eine Gruppe von Codepoints definiert. Gleichzeitig läßt sich der Wert der Precedence Bits aus IPv4 auf den Class Selector mappen, was die Kompatibilität ermöglicht. Kompatibilität des DS Byte zu etwa gesetzten DTR-Bits im TOS Byte ist jedoch in keinem Fall mehr gegeben oder angestrebt.

Der im DS Byte eingetragene Wert spezifiziert ein sogenanntes Per-Hop Behavior (PHB), d.h. einen Service Level für die Bearbeitung an einem einzelnen Switch/Router. Der Provider stimmt die PHB-Implementierung mit Verkehrsflußsteuerung (Traffic Conditioners), Verfügbarkeits-Strategie (Provisioning Strategies) und Abrechnungsmodellen ab, die es erst im Zusammenspiel einem Provider ermöglichen, mit vielen/allen Kunden anforderungsgerechte Service Level Agreements (SLA's) abzuschließen. Durch Konkatenierung desselben Per-Hop Behaviors über alle zwischengeschalteten Hops einer Verbindung hinweg entsteht ein Ende-zu-Ende Dienstgüte. Während ein SLA Ende-zu-Ende Dienstgüte und Funktionalität beschreibt, werden die detaillierten Dienstgüte-Parameter für jeden Service Level in sogenannten Traffic Conditioning Agreements (TCA's) spezifiziert. Dazu gehören

1. Detaillierte Performance Parameter wie erwarteter Durchsatz, wahrscheinliche Verlustrate und Latenzzeit (Delay)
2. Verkehrsprofile, die erfüllt werden müssen, z.B. Token Bucket Parameter
3. Festlegung, wie Verkehr behandelt wird, der das spezifizierte Profil überbucht
4. unterstützte Markierungs-Funktionen
5. unterstützte Shaping-Funktionen

Quality of Service im LAN: Leistung kontra Komplexität

DS kennt vier Komponenten zur Verkehrssteuerung: Meßpunkt (Meter), Markierung (Marker), Anpassung (Shaper) und Paketvernichtung (Dropper). Ein Meter überprüft den gesendeten Datenstrom auf Übereinstimmung mit dem zugehörigen Profil und generiert Kontroll-Input für die anderen Komponenten, die die Zugangs-Kontrolle umsetzen: Shaper fügen dem gesendeten Verkehrsaufkommen bei Bedarf Delay hinzu, so daß die spezifizierte Übertragungsrate nicht überschritten wird. Dropper entscheiden, welche und wieviele Pakete bei Überschreiten der Senderate bis hin zum Pufferüberlauf vernichtet werden. Marker setzen den Wert im DS Byte neu

- um Out-Of-Profile Verkehr herunterzustufen
- falls das SLA an einem bestimmten Netzpunkt eine DS-Änderung spezifiziert
- um sicherzustellen, daß nur DS-Werte genutzt werden, die in der entsprechenden Netzdomäne gültig sind.

Zusätzlich zu den genannten vier Komponenten sind sogenannte Traffic Classifier erforderlich, die genau wie bei RSVP ermöglichen, einzelne Pakete den unterschiedlichen Verkehrsklassen zuzuordnen. Hier gibt es BA-Classifier (Behavior Aggregate), die nur das DS Byte auswerten und MF-Classifier (Multiple Field), die mehrere Protokollfelder des Headers und sogar des Datenteils auswerten können. Im Regelfall sind MF-Classifier für einen Einsatz an den Grenzpunkten des Providernetzes gedacht, um einige Per-Micro-Flow Dienste am Übergang zum Endkunden-Netz zu implementieren. Typischerweise wird ein Datenstrom vormarkiert und vor-angepaßt am Grenzübergang einer DS Domäne anliegen. An den Schnittstellen zu non-DS Kunden muß der Provider die Erstmarkierung und entsprechendes Shaping vornehmen.

Im ersten Ansatz sind TCA's statisch, nicht dynamisch. Entsprechend kann die notwendige Konfiguration mit einem simplen "Push" mittels SNMP oder CLI auf die beteiligten Switches / Router herungergeladen werden. Natürlich muß dies für alle Komponenten konsistent und koordiniert erfolgen, um Fehler oder Nichterfüllung von TCA's zu vermeiden. Zur Unterstützung des Netzadministrators ist eine logisch zentralisierte Datenbank mit Toplogie-Information und allen aktuellen TCA-Daten hilfreich. Die Idee ist, hierfür Policy Server und LDAP als Verzeichnis Zugriff zu nutzen. Policy Server und Directory Schema spielen in diesem Fall die Rolle eines Bandwidth Brokers (BB). Alternativ kann die Konfigurations-Information auch mittels Signalisierungs-Paketen zwischen Boundary Knoten derselben DS Service Domäne ausgetauscht werden (Intra-Domain Signalling). Für die Signalisierung kann dann beispielsweise ein leicht modifiziertes genutzt werden. Statische Konfiguration ist besser geeignet für quantitative Service Level (absolute Festlegung von Übertrgungsrate, Verlustrate, Latenzzeit), Signalisierung besser für qualitative Service Level (relative Festlegung, Paketbearbeitung besser oder schlechter im Vergleich zu anderen Sevice Klassen).

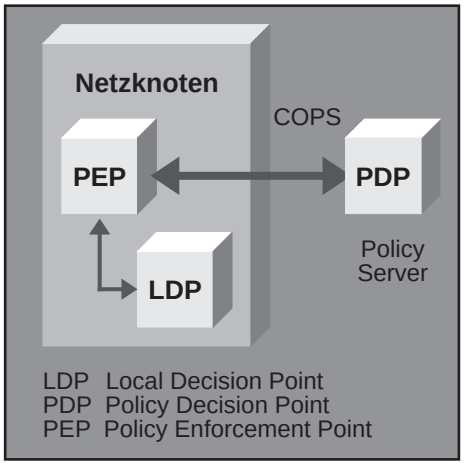
Zur Autorin
Dipl. Inform. Petra Borowka, Studium Universität Dortmund. Langjährige Projekterfahrung mit verschiedensten Industrie- und Dienstleistungsunternehmen im Bereich Beratungsprojekte, standardbasierte Netzwerk-Planungen, Schulungen, Veröffentlichungen. Unternehmensberatung Netzwerke UBN

petra.borowka@ubn.de

Übergang zur zentralen QoS-Kontrolle: COPS

Für die Implementierung einer Zugangskontrolle (Policy Service) gibt es einen Draft-Vorschlag vom August 1998 (Expiry Date Februar 1999), entwickelt von Firmen wie Level3, Intel, IPHighway, IBM und Cisco. COPS (Common Open Policy Service) definiert ein einfaches Query-Response-Modell, um Policy-Informationen zwischen einem Policy Server und den ihm zugeordneten Clients auszutauschen (siehe Bild 7). Ein solcher Client kann z.B. ein Router sein, der angefragte DS-Priorisierungen und RSVP-Reservierungen zulassen oder ablehnen muß. Netze sind aufgeteilt in Administrations-Domänen, wobei jede Domäne mindestens mit einem Policy Server ausgestattet ist. Clients stellen Reservierungs-Anfragen an den Policy Server, senden ihm aber auch Updates und Löschungswünsche. Der Server bearbeitet Updates und Löschungen und entscheidet über Reservierungs-Wünsche. COPS benutzt als Basis-Protokoll TCP, für die Durchführung von Reservierungen wird RSVP als Signalisierungs-Protokoll angenommen.

Bild 7
COPS Konfiguration
für zentrale Policy-Kontrolle



Vorteile für Netzbetreiber

Was sind die Vorteile solcher Ansätze, die einen Anwender dazu bringen könnten, von der lange und mit hohem Marketingeinsatz der Hersteller gehegten Vision vom ATM-Netz Abschied zu nehmen?

- Möglichkeit, neue Applikationen wie Multicast und verteilte Bearbeitung, Telefonie- und Konferenz-Applikationen einzurichten und effizient zu betreiben
- Investitionsschutz für vorhandenes Frame-technologie-Equipment
- Leistungs-Verbesserungen durch Umgehen der Frame-Cell-Konvertierung, die bei ATM-Backbone stets erforderlich ist
- kurze Ende-zu-Ende Bearbeitungszeiten aufgrund hoher LAN-Übertragungskapazität (Pufferzeit von 1500 Byte bei 1 Gbit Ethernet: nur noch 12 Mikrosekunden);
- einfache und somit schnell umsetzbare Priorisierungs-Strategien, die jedoch zu hohen Effizienzsteigerungen beitragen
- Erreichung eines Basis-QoS, der Realzeit-Applikationen mit mittlerer bis guter Qualität ermöglicht
- Netzbetrieb auf der Basis eines über 20jährigen Know How Aufbaus
- Pluspunkte bei der Kostenfrage

um nur einige wichtige Argumente zu nennen.

Quality of Service im LAN: Leistung kontra Komplexität

Fazit

In der klassischen Internetworking Welt ist mit der Etablierung von Switching bis zum Endgerät ein deutlicher Trend erkennbar, QoS-Funktionalität mit Frame-Technologie auf 802.x LANs zu ermöglichen. Insbesondere wird an der Interaktion von Layer-3- und Layer-2-Geräten gearbeitet, die eine durchgehende Dienstgüte in Form von Priorisierung, Delay-Garantie und Durchsatz-Garantie ermöglicht. Der Fokus liegt dabei auf Einfachheit und Beschränkung auf wesentliche Dienstklassen bzw. elementare Paket-Klassifizierung. Damit hat ATM ein wichtiges Alleinstellungsmerkmal verloren. Die erreichte Funktionalität ist zwar sicher nicht mit den hochkomplexen Möglichkeiten eines ATM-Netzes vergleichbar, kann jedoch eine praktikable Grundqualität herstellen, die den Dienstgüte-Anforderungen in den nächsten zwei Jahren von etwa 85% bis 95% der heutigen Netze gerecht werden dürfte. Aktuell ist hierfür noch ein Zusammenspiel verschiedener Protokolle erforderlich: Paketklassifizierung (COPS, DS, RSVP, MPLS, 802.1D-1998), Abbildung von Dienstklassen auf MAC-Dienste (ISSLL, 802.1D-1998, 802.1Q) sowie dynamische Handhabung von Multicast-Applikationen und -Gruppen (GARP, GMRP, GVRP, IGMP). Dabei wird allerdings eines klar: Die Realisierung von Dienstgüte in LANs führt zu einer deutlichen Steigerung der Konfigurations-Komplexität. Deshalb ist in jedem Fall zu überprüfen, wieweit in einem gegebenen Netz tatsächlich Steuermechanismen in Form von QoS erforderlich sind.

Literatur

Vom Best Effort zum Quality of Service LAN: Netzwerk Redesign Forum der ComConsult Akademie, Bonn, 1998

Borowka, P.: Internetworking - Konzepte, Komponenten, Protokolle, Einsatzszenarios; mitp Verlag, Bonn 2. erw. Aufl. 1998

QoS Links

http://www.
ietf.org/html.charters/diffserv-charter.htm

http://www.ieee.org

http://www.
data.com/issue/981121/quality.html

http://www.
data.com/issue/981107/boxes.html

Seminare

Aufbau und Design hochverfügbarer Netzwerke (QoS-LANs)

Voice und Video über IP

Abkürzungen

A	API	Application Programming Interface
	ATM	Asynchronous Transfer Mode
B	BA	Behavior Aggregate
	BB	Bandwidth Broker
C	CL	Controlled Load
	CLI	Command Line Interface
	CU	Currently Unused
D	DLSw	Data Link Switching
	DS	DiffServ, Differentiated Services
	DSCP	Differentiated Services Code Point
G	GARP	Generic Attribute Registration Protocol
	GMRP	GARP Multicast Registration Protocol
	GS	Guaranteed Service
	GVRP	GARP VLAN Registration Protocol
I	IEEE	Institute for Electrical and Electronic Engineers
	IETF	Internet Engineering Task Force
	IGMP	Internet Group Management Protocol
	ISSLL	Integrated Services over Specific Link Layers
L	LDAP	Lightweight Directory Access Protocol
	LMSC	LAN-MAN Standards Comittee der IEEE
M	MF	Multiple Field
	MPLS	Multi-Protocol Label Switching
Q	QoS	Quality of Service
R	RR	Round Robin
	RSVP	Resource ReSerVation Setup Protocol
S	SBM	Subnet Bandwidth Manager
	SLA	Service Level Agreement
	SNMP	Simple Network Management Protocol
T	TCA	Traffic Conditioning Agreement
VW	VID	VLAN ID
	VLAN	Virtuelles LAN
	WFQ	Weighted Fair Queueing

Anzeige

Ausbildung zum CCNE
Nutzen Sie unsere Paketpreise!

Zwei 5-tägige Seminare und das 3-tägige Seminar zum Paketpreis von DM 9.150,-- oder EUR 4.678,32 (statt mind. DM 9.950,--) zzgl. MwSt.

Drei 5-tägige Seminare zum Paketpreis von DM 9.600,-- oder EUR 4.908,40 (statt mind. DM 10.500,--) zzgl. MwSt.

Drei 5-tägige Seminare und das 3-tägige Seminar zum Paketpreis von DM 11.900,-- oder EUR 6.084,37 (statt mind. DM 13.490,--) zzgl. MwSt.

Lokale Netze für Einsteiger

Einzelpreis: DM 3.500,-- (EUR 1.789,52) zzgl. MwSt.

- **14.06. - 18.06.99 Mannheim**
- **21.06. - 25.06.99 Aachen**
- **20.09. - 24.09.99 Aachen**
- **25.10. - 29.10.99 Aachen**
- **22.11. - 26.11.99 Köln**
- **06.12. - 10.12.99 Aachen**

Internetworking

Einzelpreis: DM 3.790,-- (EUR 1.937,80) zzgl. MwSt.
* Einzelpreis: DM 3.690,-- (EUR 1.886,67) zzgl. MwSt.

- **03.05. - 07.05.99 Aachen***
- **21.06. - 25.06.99 Aachen***
- **18.10. - 22.10.99 Aachen**
- **13.12. - 17.12.99 Aachen**

Neue Ethernet Technologien und Management

Einzelpreis: DM 3.690,-- (EUR 1.886,67) zzgl. MwSt.
* Einzelpreis: DM 3.500,-- (EUR 1.789,52)zzgl. MwSt.

- **07.06. - 11.06.99 Aachen***
- **27.09. - 01.10.99 Aachen**
- **29.11. - 03.12.99 Aachen**

Betrieb von TCP/IP-Netzen

Einzelpreis: DM 2.990,-- (EUR 1528,76) zzgl. MwSt.

- **21.06. - 23.06.99 München**
- **22.11. - 24.11.99 Hamburg**

Heterogene Netze mit TCP/IP

Einzelpreis: DM 2.990,-- (EUR 1528,76) zzgl. MwSt.

- **03.05. - 05.05.99 Berlin**
- **05.07. - 07.07.99 Darmstadt**
- **18.10. - 20.10.99 Berlin**
- **29.11. - 01.12.99 Bonn**

ComConsult Akademie