

Von Backbone bis Speichernetz

Aktuelle Trends für Local Area Networks

Kai-Oliver Detken

IT-Lösungen müssen permanent mit den steigenden Anforderungen mitwachsen können, um nicht schon nach kurzer Zeit von der Entwicklung wieder überholt zu werden. Dabei muß heute gleich in mehreren Bereichen entschieden werden, wie die Zukunft der lokalen Netze aussehen soll. Nachdem sich die Diskussion über vorhandene Technologien in den letzten Jahren stark gelegt hat, stehen jetzt immer mehr Ethernet-Weiterentwicklungen auf der Tagesordnung. Hinzu kommt die Diskussion um die erste Meile, die ebenfalls Ethernet betrifft. Mit 10-Gigabit-Ethernet steht zudem der nächste Geschwindigkeits-sprung bevor.

Die bereits seit Jahren diskutierte Konvergenz von Sprach- und Datennetzen wird immer intensiver. Unternehmen, die Voice-over-IP (VoIP) einführen wollen, benötigen leistungsfähige Netzinfrastrukturen mit Quality-of-Service-Funktionen (QoS). Zudem müssen für immer mehr Mitarbeiter mobile Anbindungsmöglichkeiten an das Firmennetz geschaffen werden. Dabei stellt die Gewährleistung der Sicherheit eine große Herausforderung dar. Hier kommen zunehmend Virtual Private Networks (VPN) zum Einsatz.

Ein weiterer Punkt ist die Garantie der Ausfallsicherheit von Netzinfrastrukturen, die neben einer redundanten Auslegung der Hardwarekomponenten vor allem durch ein geschicktes Netzdesign realisiert werden kann. Zuguterletzt muß den rapide steigenden Datenmengen mit leistungsfähigen Speicherlösungen entgegengekommen werden.

Ethernet steht im Vordergrund

10-Gigabit-Ethernet (10GE) ist seit Mitte 2002 standardisiert. Die LAN-Technik steht nun vor ihrer Einführung in die Bereiche Metropolitan Area Network (MAN) und Wide Area Net-

work (WAN). Dabei wird das nur für optische Schnittstellen spezifizierte Ethernet die vorhandenen SDH-Strukturen ergänzen. Allerdings kann es durch die Möglichkeit, SDH als Transportnetz zu nutzen, zur Ablösung anderer Übertragungsverfahren wie ATM oder Frame Relay kommen.

Auch im Access-Bereich eröffnet Ethernet neue Alternativen. Zahlreiche Hersteller haben sich in der IEEE-Arbeitsgruppe Ethernet-in-the-First-Mile (EFM) mit dem Ziel zusammengeschlossen, die LAN-Technik über herkömmliche Telefonleitungen zum Endkunden zu bringen. Wie bei 10-Gigabit-Ethernet einigten sich die Mitglieder von IEEE 802.3ah darauf, nur eine Vollduplex-Übertragung vorzusehen. Die Gruppe hat sich dafür in vier Untergruppierungen aufgeteilt:

- Punkt-zu-Multipunkt-Übertragung (P2MP);
- Punkt-zu-Punkt-Verbindungen über Lichtwellenleiter (P2P) und P2MP auf der physikalischen Schicht;
- Operation, Administration und Maintenance (OAM);
- Datentransfer über Kupferkabel.

Die 10GE-Technologie steht in Unternehmensnetzen derzeit vor allem für eine leistungsfähige Kopplung von verteilten Campus-Netzen oder die Verbindung von Rechenzentren. Im Backbone-Bereich von LANs dagegen reicht Gigabit-Ethernet in den meisten Fällen bislang aus. Das kann sich allerdings schnell ändern, wenn z.B. Applikationen wie Business-TV mit Multimediaübertragungen zu jedem Arbeitsplatz eingeführt werden (*Bild 1*). Durch Gigabit-Ethernet und 10GE gewinnt die Glasfaser für die Netzverkabelung weiter an Bedeutung. Während im Primärbereich die Kupfer- immer mehr durch Glasfaserkabel abgelöst werden, findet jetzt die Diskussion bei den Etagenverteiltern statt. Den Weg vom Switch zum Desktop-System hat die Glasfaser allerdings

Das Thema in Kürze

Heutige Unternehmen besitzen mit Gigabit-Ethernet im Backbone meistens auch noch für die nächsten Jahre und Aufgaben genügend Kapazität. Dennoch sollten die IT-Manager ihre Infrastruktur und die Aktivitäten im LAN-Bereich gerade auch im Hinblick auf die Aufrüstung der Unternehmensnetze für Voice over IP kontinuierlich verfolgen. Der Beitrag bietet durch die Darstellung der aktuellen Entwicklungen eine gute Hilfestellung.

Kai-Oliver Detken ist Senior IT Consultant der Detken Consultancy & Internet Technologies e.K. sowie Dozent und freier Autor in Grasberg

noch nicht erobert. Folgende Gründe sprechen dafür, daß es auch noch länger so bleiben wird:

- 100-Mbit/s-Ethernet ist heute ausreichend für den Desktop-PC;
- neue Techniken wie VoIP-Telefone oder Laptops besitzen keine LWL-Anschlüsse;
- GE kommt mit der UTP-Verkabelung Kat.5 aus, so daß auch der nächste Performance-Schritt mit Kupfer abgedeckt ist;
- höhere Installationskosten und Preise je Port bei den aktiven LWL-Komponenten.

Allerdings bieten Glasfasern hohe Datenraten und größere Reichweiten, sind abhörsicher und zudem unempfindlich gegen elektromagnetische Störungen.

Neue Merkmale der Ethernet-Technik

Eine weitere Entwicklung im Ethernet-Umfeld ist die Stromversorgung von Systemen über Datenverkabelung. In der IEEE-Arbeitsgruppe 802.2af DTE Power wurden die wesentlichen Teile des Standards fertiggestellt. Zwei Arten der Stromversorgung sind definiert: über Switche, die die Einspeisung vornehmen, sowie mit Hilfe der nachträglichen Einspeisung ins Kabel, der sog. Midspan Insertion (MI). Der Strom läßt sich sowohl über das Signalkabel als auch über das unbenutzte Adernpaar von 10-/100-Mbit/s-Ethernet-Kabeln übertragen. Allerdings ist dabei zu beachten, daß die MI nur das unbenutzte Paar verwenden darf und das Endgerät in der Lage sein muß, über beide Alternativen Strom zu empfangen. Das bedeutet aber auch, daß die GE-Technik nicht mit einbezogen werden kann, da hier alle vier Leiterpaare verwendet werden. Zudem vertragen sich viele schon im Markt befindliche und von ihren Herstellern als proprietär ausgelegte Systeme nicht mit dem Standard.

Zur Verbesserung der Redundanz ist der Spanning-Tree-Algorithmus verbessert worden. Das Protokoll Rapid Reconfiguration nach IEEE802.1w erlaubt eine deutlich schnellere Reaktion auf Fehler als die herkömmliche Spanning-Tree-Methode. Je nach Lei-

stungsfähigkeit des Switch und der Art des Fehlers werden Reaktionszeiten von wenigen Sekunden erreicht. Dabei wird der neue Pfad vorab erkannt und muß nicht erst neu berechnet werden, wenn es zu Ausfällen kommt. Allerdings gibt es keine Ga-

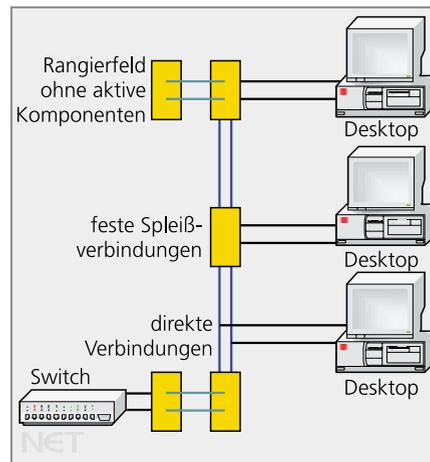


Bild 1: Hierarchischer Stern mit verringertem Administrationsaufwand

stantien für die Umschaltzeiten. Darüber hinaus erlaubt der Standard kurze Schleifen sowie das Überholen der Pakete untereinander beim Transport über ein Netz. Setzt man hingegen das Multiple-Spanning-Tree-Protokoll (IEEE802.1s) ein, an dem zur Zeit gearbeitet wird, muß die Baumstruktur nur noch für ein virtuelles LAN (VLAN) bzw. eine VLAN-Gruppe berücksichtigt werden. Zwischen zwei Switchen im Netz kann es dann mehr als nur einen aktiven Pfad geben.

Ebenfalls wichtig ist das Standard Extensible Authentication Protocol nach IEEE 802.1x zur Kontrolle des Zugangs zu Netzen auf Port-Ebene. Windows XP, Macintosh und Linux unterstützen es ebenso wie neuere Netzkomponenten. Vor allem in WLANs verspricht es eine erhöhte Sicherheit. Der Zugang wird durch die MAC-Adressen sichergestellt und überprüft. Dies kann man auch mit VPN-Szenarien und RADIUS-Datenbank kombinieren.

Netzkonvergenzen

Schnelle und ausfallsichere Netze sind für Applikationen wie VoIP eine wichtige Grundlage. Bei Echtzeitanwendungen muß sichergestellt werden, daß möglichst keine Pakete verloren

gehen und es zu keinen großen Verzögerungen kommt. Ansonsten wird die Wiedergabe verzerrt oder ganze Wortteile gehen verloren. Da die Verzögerung mit jeder aktiven Komponente zunimmt, ist es besonders in größeren Netzen wichtig, daß die Netzkomponenten Sprachpakete priorisieren können. Die Grenze für eine gut verständliche Sprachübertragung liegt bei etwa 150 bis 250 ms.

Immer mehr Unternehmen denken darüber nach, wie sie in ihrem Unternehmen die Daten- und Sprachkommunikation über ein Netz abwickeln können. Dabei müssen die vorhandenen Switche und Router vorhandene Priorisierungsmechanismen wie IEEE 802.1(p)D auf Layer 2 und Differentiated Services (DiffServ) auf Layer 3 unterstützen. Die von den Herstellern implementierten Verfahren weichen jedoch zum Teil beträchtlich voneinander ab.

In Unternehmensnetzen ist QoS bislang kaum im Einsatz. Anders sieht es bei Service Providern aus, die damit ihren Kunden Service Level Agreements (SLA) anbieten können. Allerdings ist es nicht ganz einfach, in größeren Unternehmensnetzen den Datenverkehr mit Hilfe von QoS zu steuern.

Neben der Priorisierung von VoIP-Paketen kann mit QoS auch die im Netz vorhandene Bandbreite effizienter genutzt werden.

Mobilfunknetze

Bei den Wireless LANs (WLAN) hat es Jahre gedauert, bis sich die Industrie auf den einheitlichen Standard IEEE 802.11b einigen konnte, der eine maximale Brutto-Übertragungsrates von 11 Mbit/s bietet. Und die nächste Generation nach 802.11a verspricht schon bis zu 54 Mbit/s, allerdings streiten hier noch unterschiedliche Übertragungstechniken um die Vorherrschaft.

Die ETSI hat darüber hinaus mit Hiperlan/2 einen eigenen Vorschlag für die drahtlose Übertragung mit 54 Mbit/s entwickelt. Daraufhin sah sich die IEEE gezwungen, mit der Radio Regulatory Technical Advisory Group (RRTAG) 802.18 eine Koordinierungsstelle für

die Aktivitäten bei Funknetzen einzurichten. Deren Bemühungen, aus den beiden konkurrierenden Ansätzen einen weltweit einheitlichen Standard zu machen, werden eventuell schon im nächsten Jahr erfolgreich sein.

Die Verzögerungen, die durch die Auseinandersetzungen um 802.11a und Hiperlan/2 entstanden sind, nutzten einige Hersteller, um den Standard 802.11g mit 22 Mbit/s zur Marktreife zu bringen. Er arbeitet wie die b-Variante im 2,4-GHz-Band.

Management

Durch die zunehmende Segmentierung von geschichteten Netzen sind neue Analysysteme notwendig, die nicht nur den störungsfreien Betrieb eines Netzes gewährleisten sollen, sondern auch um eventuell auftretende Störungen schnell finden und beheben zu können. Allerdings ist in heutigen Netzen, wo jeder einzelne Switch-Port ein Segment darstellt, die Flächendeckung schwer zu realisieren. Immer noch liegen viele Fehlerursachen auf den untersten zwei Schichten: defekte Netzkarten, Kabel und Ports, zu hohe Auslastung des Netzes durch Übertragungen usw. Zwar bleibt durch die meist starke Segmentierung der Fehler häufig räumlich beschränkt, trotzdem ist es notwendig, ihn schnell zu lokalisieren und zu beheben. Dafür haben sich in der Praxis zwei Lösungsansätze als brauchbar erwiesen:

- zentrales Management aktiver Komponenten mit SNMP;
- Monitoring mit RMON 1 und 2.

Aktive Komponenten bieten über SNMP ausreichende Statistiken zur Fehlererkennung an, so daß z.B. kritische Port-Zustände, Server, Drucker oder Applikationen überwacht werden können. Zusätzlich lassen sich auch Berichte über beliebige Parameter und Zeiträume erstellen. Von den Herstellern sind heute allerdings Netzmanagementlösungen erhältlich, die nur auf die Parameter der eigenen Geräte abgestimmt sind. Herstellerunabhängige Produkte wie TheGuard! oder OpenView, die umfangreichere Funktionalitäten bieten, sind meist kostspieliger.

Managementlösungen übertragen Daten über SNMP unkomprimiert, ungesichert und unverschlüsselt. Zwar gibt es mit SNMPv3 eine aktualisierte Version, die fast alle Nachteile beseitigt, indem sie eine Verschlüsselung mit MD5, SHA-1 und 3-DES, Traps mit ausführlicher Fehlerbeschreibung und Proxy-Support anbietet, sie ist aber selten in heutigen Komponenten vorhanden.

RMON1 besteht aus neun bzw. zehn Gruppen, von denen meistens nur vier unterstützt werden. Ein komplettes RMON1 bietet neben den Statistikfunktionen wie z.B. Netzlast, ein- und ausgehende Bytes, Pakete oder physikalische Fehler auch detaillierte Informationen auf Layer 2 über sog. Toptalker, Protokollverteilungen und Konversationsbeziehungen. Ebenso lassen sich Daten mitschneiden und mit dem lokalen Protokollanalysator auswerten. RMON2 bietet diese Möglichkeiten zusätzlich auf Layer 3. Für eine volle RMON1/2-Unterstützung sind bei den Anbietern teure Zusatzmodule nötig.

RMON ist eine Untergruppe des SNMP-Protokolls. Es leidet aber unter dem Nachteil der hohen Netzlast und geringen Sicherheit und wird im Gegensatz zu SNMP nicht weiterentwickelt. Trotz der Nachteile beider Ansätze gibt es wenig Alternativen.

Speichernetze

Um große Datenmengen in den Griff zu bekommen, setzen immer mehr Firmen auf vernetzte Speicherlösungen. Dabei kommen hauptsächlich zwei Ansätze zum Einsatz:

- Storage Area Networks (SAN) basierend auf Fibre Channel (FC);
- Network Attached Storage (NAS) basierend auf Ethernet.

NAS-Systeme (*Bild 2*) eignen sich besonders zur schnellen Bereitstellung neuer Speicherkapazitäten für Arbeitsgruppen. Sie werden über eine

integrierte Fast-Ethernet- oder GE-Karte direkt mit dem LAN verbunden. Die meisten Geräte stellen Dateisysteme für Windows-, Unix- bzw. Linux-Umgebungen zur Verfügung. Um das Problem des aufgrund der steigenden Datenmengen nicht mehr ausreichenden

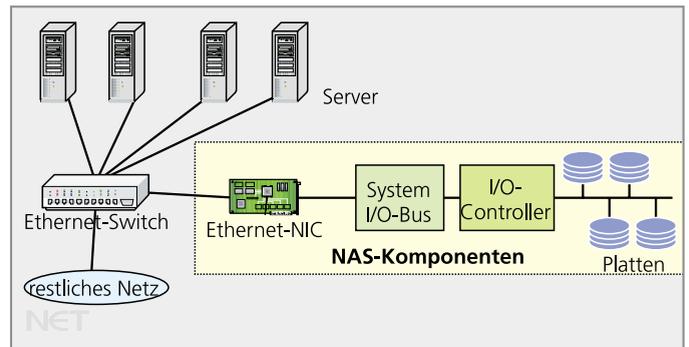


Bild 2: Typische NAS-Struktur

den Zeitfensters für ein Offline-Backup zu beseitigen, werden Images des Datenbestandes erstellt, mit dem sich eine konsistente Kopie der Daten erzeugen läßt. Diese können dann ohne Zeitdruck gesichert werden.

Auch in SAN-Systemen haben sich solche Verfahren etabliert. SAN verwendet FC als Übertragungsprotokoll. FC greift auf dem Block-Level auf die Daten zu und erreicht dadurch eine wesentlich höhere Performance als NAS, das auf File-Level arbeitet. Für den Aufbau von leistungsfähigen Speichernetzen haben sich FC-gestützte SANs inzwischen durchgesetzt. Die FC-Übertragungstechnik ist inzwischen bei einer Datenrate von 2 Gbit/s angekommen. Fortschritte macht auch die Konvergenz von SAN und NAS. Gateways ermöglichen, daß SAN-Festplatten für NAS genutzt werden können oder sich ein NAS nachträglich zu einem SAN umbauen läßt.

Mit iSCSI (Internet-SCSI) entwickelt die IETF einen neuen Standard, der es ermöglichen soll, Block-Level-SCSI-Daten über IP-Netze zu übertragen. Damit lassen sich Speichernetze auf der Basis vorhandener Ethernet-Infrastrukturen aufbauen. Gegenüber FC hat iSCSI den Nachteil, daß die Protokollverarbeitung relativ aufwendig ist. Spezielle TCP/IP-Offload-Karten sollen die Server von dieser Arbeit entlasten. (bk)