

FAQs

Als kleine Hilfe haben wir die wichtigsten Fachwörter aus der Welt des Ethernet für sie zusammengetragen:

RMON

RMON (Remote Monitoring) ist ein Standard, um in netzwerkfähigen Geräten statistische Daten zu erheben, sie in Datenbanken zu speichern, sowie über Zugriffe Daten abzufragen (Netzwerkmanagement).

RMON ist eine Erweiterung der Simple Network Management Protocol MIB (Management Information Base). Details wurden von der IETF in RFC 2819 und RFC 2021 festgelegt.

RMON definiert eine RMON-MIB, welche die MIB II ergänzt und dem Netzmanager wesentliche Informationen zum Netzwerk liefert. Das Bemerkenswerteste an RMON ist die Tatsache, dass es, obwohl es einfach nur die Spezifikation einer MIB ist keine Änderungen am zugrunde liegenden SNMP Protokoll vornimmt, die SNMP Funktionalität erheblich erweitert.

DER RMON Standard war ursprünglich in RFC 1271 definiert (heute RFC 1757) Sein Zweck besteht darin, proaktive Überwachungs- und Diagnosefunktionen für verteilte LANs bereitzustellen.

SNMP

Das **Simple Network Management Protocol** (englisch für „einfaches Netzwerkverwaltungsprotokoll“, kurz **SNMP**), ist ein Netzwerkprotokoll das entwickelt wurde um Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwachen und steuern zu können. Das Protokoll regelt hierbei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. Hierzu beschreibt SNMP den Aufbau der Datenpakete, die gesendet werden können, und den Kommunikationsablauf. SNMP wurde dabei so ausgelegt, dass jedes netzwerkfähige Gerät mit in die Überwachung aufgenommen werden kann. Zu den Aufgaben des Netzwerkmanagement, die mit SNMP möglich sind, zählen:

- Überwachung von Netzwerkkomponenten.
- Fernsteuerung und Fernkonfiguration von Netzwerkkomponenten.
- Fehlererkennung und Fehlerbenachrichtigung.

Durch seine Einfachheit hat sich SNMP zum Standard entwickelt, der von den meisten Managementprogrammen unterstützt wird.

LACP - Trunking

Das **Link Aggregation Control Protocol (LACP)** ist ein Netzwerkprotokoll nach IEEE 802.3ad zur dynamischen Bündelung von physikalischen Netzwerkverbindungen.

Mit Hilfe von LACP können redundante physikalische Verbindungen zwischen zwei Switches zu einer logischen Verbindung zusammengefasst werden. Hierdurch wird eine Lastverteilung auf alle an der logischen Verbindung beteiligten physikalischen Verbindungen erreicht, sowie außerdem die Ausfallsicherheit der Verbindung gesteigert.

Das LACP stellt den offiziellen IEEE-Standard für die Link Aggregation Technik dar. Link Aggregation bezeichnet die dynamische Bündelung von mehreren physikalischen Verbindungen zwischen zwei Netzwerk-Komponenten zu einer logischen Verbindung. Neben LACP bestehen noch proprietäre Lösungen zur dynamischen Bündelung, zum Beispiel das PAgP von Cisco. Weiterhin existieren noch unzählige statische Link Aggregation-Verfahren, die alle mehr oder weniger proprietär sind und somit nicht herstellerübergreifend eingesetzt werden können.

Früher wurde statt des Begriffs Link Aggregation auch der Begriff Trunking verwendet.

Port Mirroring

Ein Nachteil von Switches ist, dass ein Netz nicht mehr so einfach zu debuggen ist, da Pakete nicht mehr auf allen Strängen im Netz sichtbar sind, sondern im Idealfall nur auf denjenigen, die tatsächlich zum Ziel führen. Um dem Administrator trotzdem die Beobachtung von Traffic zu ermöglichen, beherrschen bessere Switches *Port Mirroring*. Der Administrator loggt sich dazu auf dem (verwaltbaren) Switch ein und teilt diesem mit, welche Ports er beobachten möchte. Der Switch schickt dann Kopien von Paketen der beobachteten Ports an den Rechner des Beobachters, wo sie z. B. von einem Sniffer aufgezeichnet werden können.

Network Time Protocol – NTP, SNTP

Das **Network Time Protocol (NTP)** ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze. Obwohl es meistens über UDP abgewickelt wird, kann es durchaus auch über andere Layer-4-Protokolle wie z. B. TCP transportiert werden. Es wurde speziell dafür entwickelt, eine zuverlässige Zeitgabe über Netzwerke mit variabler Paketlaufzeit (Ping) zu ermöglichen.

ASIC

Eine **Anwendungsspezifische Integrierte Schaltung** oder **Application Specific Integrated Circuit (ASIC)**, auch **Custom-Chip**, ist eine elektronische Schaltung, die als integrierter Schaltkreis realisiert wurde. ASICs werden weltweit von vielen Herstellern nach Kundenanforderung gefertigt und normalerweise nur an diese geliefert. Darin unterscheidet sich das ASIC deutlicher von anderen Mikrochips als durch Unterschiede in Fabrikation und Entwurf. Wird ein wie ein ASIC entwickelter Baustein am Markt verkauft, spricht man häufig von einem anwendungsspezifischen Standardprodukt (ASSP).

ASICs finden Verwendung in nahezu allen möglichen elektronischen Geräten, vom Radiowecker bis zum Hochleistungsrechner. Der Grund für die Entwicklung solcher ICs, welche oft sogar nur für eine einzige bestimmte Modellreihe entworfen werden, ist vor allem bei hohen Fertigungstückzahlen die Kostenersparnis gegenüber dem diskreten Aufbau von Schaltkreisen aus einzelnen Transistoren oder TTL-Bausteinen.

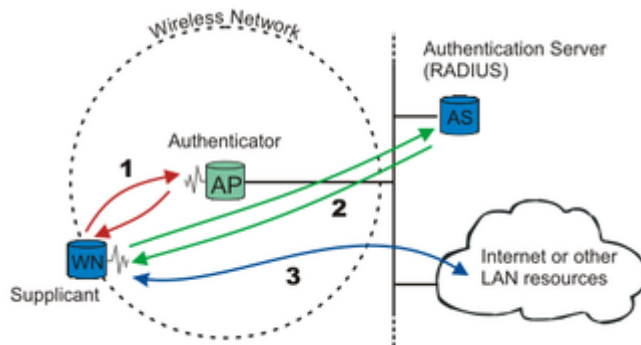
Rein digitale ASICs integrieren eine große Zahl von Logik-Funktionen, für die sonst aus diversen Standardbausteinen wie Prozessor, Logikfamilien (z.B. 74xx) oder ähnlichen Bausteinen zusammengestellt werden müssten. Mixed-signal ASICs enthalten zusätzlich zu den digitalen Schaltkreisen auch analoge Schaltungen wie z.B. Analog-Digital-Wandler, PLLs, etc.

ASICs werden vor allem für in Großserien gebaute Geräte zur Kostensenkung verwendet. Ein Großteil der heutzutage hergestellten Chips sind applikationsspezifisch, wie zum Beispiel die Prozessoren in Mobiltelefonen zur Kodierung von Signalen oder zur Aufbereitung von Daten. Der Unterschied zu PLDs und FPGAs besteht darin, dass die Funktionalität des anwendungsspezifischen ICs vom Hersteller eindeutig festgelegt werden muss und somit fest vorgegeben ist. Die interne Schaltung kann vom Anwender nicht mehr verändert werden. Es gibt auch ASIC-Varianten, auf denen Mikroprozessoren oder Signalprozessoren integriert sind (System on Chip), wodurch eine gewisse Flexibilität für den Anwender durch die darauf ablaufende Software erreicht werden kann.

Die bekannten CPUs (Intel Pentium, AMD Athlon, etc.) sind hingegen universelle integrierte Schaltungen, die eine Vielzahl verschiedener Aufgaben bewältigen können. Das hat jedoch den Nachteil, dass diese Aufgaben nicht optimal abgearbeitet werden: Leistungsverbrauch, Datendurchsatz, Chip-Fläche, Taktfrequenz und andere Zielparameter sind in bestimmten Anwendungen höher als mit einem spezialisierten Baustein.

Wegen der Anpassung ihrer Architektur auf ein spezifisches Problem, arbeiten ASICs sehr effizient und um einiges schneller als eine funktionsgleiche Umsetzung per Software in einem Mikrocontroller. In einem Mobiltelefon hat das zum Beispiel den Vorteil, dass der Akku länger hält und das Gerät kompakt ist.

IEEE 802.1x - Radius



Ein WLAN-Client muss authentifiziert werden, bevor er auf weitere LAN-Ressourcen zugreifen darf

IEEE 802.1x ist ein Standard zur Authentifizierung in Rechnernetzen.

Der Standard IEEE 802.1x stellt eine generelle Methode für die Authentifizierung und Autorisierung in IEEE 802-Netzen zur Verfügung. Am Netzwerkzugang, einem physikalischen Port im LAN, einem logischen IEEE 802.1q VLAN oder einem WLAN, erfolgt die Authentifizierung durch den Authenticator, der mittels eines Authentifizierungsservers (RADIUS-Server) die durch den Supplicant übermittelten Authentifizierungsinformationen prüft und gegebenenfalls den Zugriff auf die durch den Authenticator angebotenen Dienste (LAN-, VLAN oder WLAN) zulässt oder abweist.

Der Standard empfiehlt das Extensible Authentication Protocol (EAP) oder das PPP-EAP-TLS Authentication Protocol zur Authentifizierung, da keine eigenen Authentisierungsprotokolle definiert werden.

Spanning Tree Protocol – STP, RSTP

Das **Spanning Tree Protocol (STP)** dient zur Vermeidung redundanter Netzwerkpfade (Schleifen) im LAN, speziell in geschichteten Umgebungen. Es wurde von Radia Perlman entwickelt und ist in der IEEE-Norm 802.1D standardisiert.

Netzwerke sollten zu jedem möglichen Ziel immer nur einen Pfad haben, um zu vermeiden, dass Datenpakete (Frames) dupliziert werden und mehrfach am Ziel eintreffen, was zu Fehlfunktionen in darüber liegenden Netzwerkschichten führen könnte und die Leistung des Netzwerks vermindern kann. Andererseits möchte man mitunter redundante Netzwerkpfade als Backup für den Fehlerfall zur Verfügung haben. Der Spanning Tree-Algorithmus wird beiden Bedürfnissen gerecht.

Zur Kommunikation zwischen den Switches wird das Bridge Protokoll genutzt. Die Bezeichnung Bridge stammt aus der Annahme, dass ein Switch eine Multiport-Bridge ist. Die Pakete dieses Protokolls werden Bridge Protocol Data Unit (BPDU) genannt.

Zunächst wird unter den Spanning-Tree-fähigen Bridges im Netzwerk eine sog. *Root Bridge* gewählt, die die Wurzel des aufzuspannenden Baumes wird und „Chef“ des Netzwerks ist. Dies geschieht, indem alle Bridges ihre Bridge-ID (die jede Bridge besitzt) an eine bestimmte Multicast-Gruppe mitteilen. Die Bridge ID ist 8 Byte lang (2 Bytes Bridge Priority und 6 Bytes MAC Adresse). Die Bridge mit der niedrigsten ID wird zur Root Bridge. Sollte die Bridge Priority identisch sein, wird als ergänzendes Kriterium die MAC Adresse der Komponenten benutzt (und zwar die Bridge mit der niedrigeren MAC Adresse). Von der Root Bridge aus werden nun Pfade festgelegt, über die die anderen Bridges im Netzwerk erreichbar sind. Sind redundante Pfade vorhanden, so müssen die dortigen Bridges den entsprechenden Port deaktivieren. Die Pfade, über die kommuniziert werden darf, werden anhand von Pfadkosten bestimmt, die die dortige Bridge übermittelt. Die Kosten sind abhängig vom Abstand zur Root Bridge und dem zur Verfügung stehenden Uplink zum Ziel. Ein 10 Mbit/s-Uplink hat beispielsweise höhere Pfadkosten als ein 100 Mbit/s-Uplink zum gleichen Ziel und würde dabei unter den Tisch fallen. Auf diese Weise ist jedes Teilnetz im geschichteten LAN nur noch über eine einzige, die *Designated Bridge* erreichbar. In der grafischen Darstellung ergibt sich ein Baum aus Netzwerkpfeilen, der dem Algorithmus seinen Namen gab.

Die Root Bridge teilt den in der Hierarchie eine Stufe unterhalb liegenden Designated Bridges im Abstand von 2 Sekunden mit, dass sie noch da ist, woraufhin die empfangende Designated Bridge ebenfalls an nachfolgende Bridges die entsprechende Information senden darf. Wenn diese *Hello-Pakete* ausbleiben, hat sich folglich an der Topologie des Netzwerks etwas geändert, und das Netzwerk muss sich reorganisieren. Diese Neuberechnung des Baumes dauert im schlimmsten Fall bis zu 30 Sekunden. Während dieser Zeit dürfen die Spanning-Tree-fähigen Bridges außer Spanning-Tree-Informationen keine Pakete im Netzwerk weiterleiten. Dies ist einer der größten Kritikpunkte am Spanning Tree-Algorithmus, da es möglich ist, mit gefälschten Spanning-Tree-Paketen eine Topologieänderung zu signalisieren und das gesamte Netzwerk für bis zu 30 Sekunden lahmzulegen. Um diesen potenziellen Sicherheitsmangel zu beheben, aber auch, um bei echten Topologieänderungen das Netzwerk schnell wieder in einen benutzbarem Zustand zu bringen, wurden schon früh von verschiedenen Herstellern Verbesserungen am Spanning-Tree-Algorithmus und dem dazugehörigen Protokoll erdacht. Eine davon, das *Rapid Spanning Tree Protocol (RSTP)* ist inzwischen zum offiziellen *IEEE-Standard 802.1w* geworden. Die Idee hinter RSTP ist, dass bei signalisierten Topologieänderungen nicht sofort die Netzwerkstruktur gelöscht wird, sondern erst einmal wie gehabt weiter gearbeitet wird und Alternativpfade berechnet werden. Erst anschließend wird ein neuer Baum zusammengestellt. Die Ausfallzeit des Netzwerks lässt sich so von 30 Sekunden auf unter 1 Sekunde drücken. In der 2003 zu verabschiedenden Revision des 1998 letztmalig überarbeiteten 802.1D-Standards soll das alte STP zugunsten von RSTP komplett entfallen.

TDR - Messverfahren

Längenmessung

Eine der ersten Anwendungen der Zeitbereichsreflektometrie war die Längenmessung von Kabeln in der Elektroindustrie. Hierbei wird die Zeit gemessen die ein ausgesandter Impuls bis zu seinem wiedereintreffen nach der Reflexion benötigt. Kennt man die Ausbreitungsgeschwindigkeit im Kabel, die vom Dielektrikum abhängt, so kann man von der gemessenen Zeit direkt auf die Länge des Kabels zurückschließen. Aus diesem Einsatzfeld hat sich der Begriff des Kabelradars entwickelt.

Während man früher für diese Messungen noch das Oszilloskop benötigte, gibt es heute bereits fertige Messgeräte (z.B.: von Fluke), die einem den Längenwert direkt anzeigen. Diese Technik findet eine große Anwendung im Bereich der Telekommunikation und der Netzwerktechnik. Bei Neuverkabelungen in Gebäuden erfolgt hierbei die Abrechnung des verlegten Netzkabels nach den gemessenen Werten der Zeitbereichsreflektometrie. Aufgrund der immer höheren Bandbreite, ist jedoch ein Trend zur optischen Zeitbereichsreflektometrie zu erkennen, in der das verwendete Medium eine Glasfaser darstellt.

Störquellenortung

Das Ziel der Störquellenortung ist es Kabelbrüche oder Kabelquetschungen festzustellen und deren Lage zu orten. Hierbei macht man sich die Eigenschaft der Zeitbereichsreflektometrie zu nutze, nicht nur Totalreflexionen feststellen zu können, sondern jede Änderung im Medium zu erkennen. Nur beim Kabelende, einem Kabelbruch oder einem Kurzschluss zwischen Innen- und Außenleiter kommt es zu einer Totalreflexion.

Breitet sich der Impuls entlang des unveränderten Mediums aus, so ändert sich der Wellenwiderstand im Kabel nicht und die Impedanz bleibt unverändert gleich. Kommt die Impulswelle jedoch auf eine Quetschung, so ändert sich die Impedanz und es erfolgt eine Teilreflexion. Aus dem Zeitpunkt des Eintreffens der Reflexion und deren Natur kann dann auf Ort und Ausmaß der Quetschung geschlossen werden.

Leitfähigkeitsmessung

Leitfähige Medien schließen, je nach Grad der Leitfähigkeit, bestimmte Frequenzen in Teilen kurz und führen zu Dämpfungen der übrigen Frequenzen. Setzt man die Amplitudenwerte des ausgesandten Impulses mit den Amplitudenwerten des reflektierten Impulses in Relation, so lässt dies Rückschlüsse auf die Leitfähigkeit des Mediums zu. Da die maximalen Amplituden der hohen Frequenzen jedoch schwer zu bestimmen sind, ist dies ein schwieriges Verfahren, deren Anwendung in Teilen der Feuchtigkeitsmessung im Boden zu suchen sind. Erwähnenswert sind hierbei die Arbeiten von Dr. M. Stacheder.

Internet Group Management Protocol – IGMP

Das **Internet Group Management Protocol (IGMP)** ist ein Netzwerkprotokoll der Internetprotokollfamilie und dient zur Organisation von Multicast-Gruppen. IGMP benutzt wie ICMP das Internet Protocol (IP) und ist integraler Bestandteil von IP auf allen Hosts, die den Empfang von IP-Multicasts unterstützen.

Verwendung

Das Internet Group Management Protocol basiert auf dem Internet Protocol (IP), das IP-Multicasting (Gruppenkommunikation) im Internet möglich macht. IP-Multicasting ist die Verteilung von IP-Paketen unter einer IP-Adresse an mehrere Stationen gleichzeitig. IGMP bietet die Möglichkeit dynamisch Gruppen zu verwalten. Die Verwaltung findet nicht in der Sende-Station statt, sondern in den Routern, an denen Empfänger einer Multicast-Gruppe direkt angeschlossen sind. IGMP bietet Funktionen, mit denen eine Station einem Router mitteilt, dass sie Multicast-IP-Pakete einer bestimmten Multicast-Gruppe empfangen will. Multicast-Routing-Protokolle (DVMRP, MOSPF, PIM), übernehmen die Koordination der Übertragung zwischen den Routern. Der Sender von Multicast-IP-Paketen weiß dabei nicht, welche und wieviele Stationen seine Pakete empfangen. Denn er verschickt nur ein einziges Datenpaket an seinen übergeordneten Router. Der dupliziert das IP-Paket bei Bedarf, wenn er mehrere ausgehende Schnittstellen mit Empfängern hat.

Transport Layer Security - SSL

Transport Layer Security (TLS) oder **Secure Sockets Layer (SSL)** ist ein Verschlüsselungsprotokoll für Datenübertragungen im Internet. TLS 1.0 und 1.1 sind die standardisierten Weiterentwicklungen von SSL 3.0. Hier wird die Abkürzung SSL für beide Bezeichnungen verwendet.

VLANs – Virtuelle Netzwerke

Ein **VLAN** (Virtual Local Area Network) ist ein virtuelles lokales Netzwerk innerhalb eines physikalischen Netzwerkes. Eine weit verbreitete technische Realisierung von VLANs ist teilweise im Standard IEEE 802.1Q definiert.

Gründe und Vorteile

Lokale Netzwerke werden mit Hilfe von aktiven Komponenten - Hubs und Switches - aufgebaut.

Mit Hubs aufgebaute Netzwerke haben vor allem wegen des CSMA/CD-Zugriffsverfahrens und den daraus resultierenden anwachsenden Traffics eine starke Beschränkung zu erfahren. Der maximale Durchsatz wird nie zu erreichen sein und bei starken Netzwerklasten können bei Datagramm-Protokollen Verbindungsabbrisse entstehen.

Durch die Switching-Technik (OSI-Ebene 2) können sehr große LANs aufgebaut werden, ohne starke Bandbreiteneinbußen zu verursachen. Switches können derzeit bis zu ca 24.000 angeschlossene Stationen gleichzeitig verwalten (MAC-table). Vorteil eines großen geschichteten Netzwerkes ist die einfache Erreichbarkeit aller Stationen, die Einsparung von Routern und deren Verwaltung und eine geringe Latenz der Datenpakete.

Aus folgenden Gründen will man ein solches Netzwerk oft wieder unterteilen:

- die Broadcast-Last wird sehr hoch vor allem in MS-Windows-Netzwerken
- jede Station kann jede andere direkt ansprechen (Sicherheitsproblem)

Eine Lösung für dieses Problem sind VLANs. Mit Hilfe von VLANs können auf einem Switch oder über mehrere Switches hinweg virtuell getrennte Netze betrieben werden. Diese Technik eignet sich auch für die standortübergreifende Vernetzung (z. B. per ATM) mehrerer VLANs über einen Switch bzw. Router.

Nicht immer lässt sich ein Netzwerk über getrennte Switches aufbauen. Physikalisch getrennt verkabelte Netzwerke sind unflexibel, Änderungen nur mit hohem Aufwand möglich. VLAN stellt unabhängig von der physikalischen Struktur eine logische Struktur des Netzwerkes zur Verfügung.

Gigabit Interface Converter - GBICs

Ein **GBIC** (Akronym für **GigaBit Interface Converter**) wird in der Netzwerktechnik zur Flexibilisierung von Schnittstellen verwendet.

Bei einem GBIC handelt es sich um einen streichholzschachtelgroßes Modul, das in eine elektrische Schnittstelle eingefügt wird, um diese zum Beispiel in eine optische Schnittstelle umzuwandeln. Mit Hilfe von GBICs kann die Art des zu übertragenden Signals an die Bedürfnisse der Übertragung angepasst werden.

Häufig zu finden sind GBICs im Bereich von Backbone-Netzwerken oder SANs. Die Schnittstellenkarte des Hosts beziehungsweise der Zentralverteiler (etwa der Switch) stellen ihre Schnittstelle nicht starr, sondern flexibel zur Verfügung.

Im Bereich der Computer-Netzwerke kann so über einen GBIC eine Schnittstelle flexibel als Gigabit Ethernet über Twisted-Pair-Kabel oder Lichtwellenleiter betrieben werden, ohne wie früher üblich die Schnittstellenkarte des Systemes austauschen zu müssen.

[Bearbeiten]

Interface-Typen

- SX (500 m Reichweite bei 50/125er Glasfaser, 220 m bei 62,5/125er Glasfaser)
- LX (10 km Reichweite bei 9/125er Glasfaser)
- LH(X) (40 km Reichweite bei 9/125er Glasfaser)
- ZX (80 km Reichweite bei 9/125er Glasfaser)
- T ("Kupfer" 100 m Reichweite ab Cat.5-UTP-Kabel)
- CWDM
- DWDM
- SONET (als OC48 oder OC192)

[Bearbeiten]

Bauformen

- reguläre Bauform (meist einfach als „GBIC“ bezeichnet)
- SFP (**Small Form-factor Pluggable** auch als Mini-GBIC, SFF GBIC, GLC oder „New GBIC“ beziehungsweise „Next Generation GBIC“ bezeichnet)
- XFP (wie SFP aufgebaut, aber länger)

Die Idee neuer Bauformen entstand aus dem Bedürfnis heraus, auf gleicher Fläche mehr Anschlüsse unterzubringen.

Medium Dependent Interface – MDI (-X)

Ethernet-Verbindungen mit Twisted Pair-Kabeln müssen immer gekreuzt (Crossover) verbunden werden, damit die Tx (Transmit, Sende) und Rx (Receive, Empfangs) - Leitungen beider Seiten so miteinander verbunden sind, dass jeweils die Sendeleitung des einen Geräts an der Empfangsleitung des anderen liegt.

Generell gilt: Sollen zwei gleichartige Anschlüsse (Computer und Computer oder auch Hub und Switch) verbunden werden, muss ein Crossoverkabel verwendet werden. Im weitaus häufigeren Fall der Verbindung von zwei verschiedenen Anschlüssen werden ungekreuzte Kabel verwendet.

MDI

Die Anschlussart **MDI** wird von typischen Ethernet-Netzwerkkarten verwendet. So muss im Fall der direkten Verbindung zweier Computer ein sogenanntes Crossoverkabel verwendet werden, bei dem die Adern so vertauscht sind, dass dies eintritt.

MDI-X

Die Anschlussart **MDI-X** ist üblich bei Verteilergeräten (z. B. Switch, Hub). Hier sind die Belegungen der Buchsen schon gekreuzt, so dass zum Anschluss eines weiteren Computers ein 1:1-Kabel (ungekreuzt) verwendet werden kann.

Auto-MDI(X)

Heutige Switches beherrschen meist Auto-MDI(X). Sie erkennen automatisch, welcher Partner angeschlossen ist und stellen ihren Anschluss entsprechend ein.

QoS – Quality of Service

Die Dienstgüte in IP Netzwerken hat zusätzliche IP-spezifische Parameter. Wird IP über ein Telekommunikationsnetz übertragen, bildet es nach dem OSI-Modell eine höhere Schicht auf diesem Netz. Daher sind in diesem Fall für die Beurteilung der gesamten Dienstgüte eines IP-basierten Dienstes sowohl die Übertragungsgüte als auch die IP-spezifischen Parameter relevant. Qualitätsbeeinträchtigungen addieren sich. Handelt es sich beispielsweise um einen Internetzugang, der auf Einwahl basiert, so bildet sich die gesamte Dienstgüte aus Übertragungsgüte, Verkehrsgüte und der IP-Qualität.

Wird IP nicht über ein Telekommunikationsnetzwerk übertragen, sondern beispielsweise über ein LAN wie Ethernet, so addieren sich Qualitätsbeeinträchtigungen dieses LANs zu denen der IP-Übertragung. Ein besonderer Faktor bei der IP-Qualität besteht darin, daß sie vom Endgerät maßgeblich mitbeeinflusst wird. Übertragungsgüte und Verkehrsgüte beruhen dagegen ausschließlich auf der Qualität des Netzes; die Qualität der Endgeräte geht nicht mit ein.

In IP (Internet Protocol) Netzwerken faßt man unter QoS üblicherweise die folgenden Parameter zusammen:

- Latenz: die Verzögerung der Ende-zu-Ende Übertragung
- Jitter: die Abweichung der Latenzzeit von ihrem Mittelwert
- Verlustrate: die Wahrscheinlichkeit, daß einzelne IP Pakete bei der Übertragung verloren werden
- Durchsatz: die pro Zeiteinheit im Mittel übertragene Datenmenge

Unterschiedliche Dienste haben unterschiedliche Anforderungen an diese Parameter. Für reine Dateitransfers ist üblicherweise der Gesamtdurchsatz der entscheidende Parameter, die individuelle Latenz und Verlustrate hingegen sind hier weniger von Bedeutung. Für Echtzeitkommunikation wie z.B. Voice over IP hingegen spielt die Latenz, der Jitter und die Verlustrate eine weitaus größere Rolle, weil sie maßgeblich die Sprachverständlichkeit beeinflussen. IPTV hat sogar ganz erhebliche Anforderungen an die gesamte Dienstgüte, da bereits kleine Qualitätsmängel in der Übertragung sich sichtbar in der Bilddarstellung am Fernseher auswirken.

QoS bezeichnet allgemein die Dienstgüte von Übertragungskanälen. Die Dienstgüte setzt sich aus einer Reihe von Eigenschaften wie Verlustrate, Verfügbarkeit, Durchsatz und Latenz (Verzögerung) zusammen. Letztere macht sich vor allem bei Anwendungen, die kurze Reaktionszeiten erfordern (beispielsweise Telnet), bemerkbar (z.B. erscheint bei großer Latenz eine Eingabe erst mit einer gewissen Zeitverzögerung auf dem Bildschirm). Der Extremfall „Echtzeitanwendung“ stellt hohe Anforderungen an die Übertragungsgeschwindigkeit, da z.B. im Falle von Echtzeit-Videos die Bilder zu springen anfangen und somit die Dienstgüte nicht gewährleistet ist. Der Durchsatz ist wichtig, da Videos oft eine hohe Datenrate erfordern und bei Nichterbringung dieser Rate das Video einfach gestoppt wird.

Innerhalb eines Übertragungskanal kann es so erforderlich sein, die QoS für bestimmte Datenströme zu Lasten anderer Datenströme zu erhöhen. Dies kann z.B. durch die Priorisierung von IP-Datenpaketen anhand bestimmter Merkmale und Eigenschaften geschehen. Mit diesen Mechanismen ist es möglich, z.B. Voice-over-IP, welches einen verzögerungskonstanten und kontinuierlichen Datenstrom benötigt, stärker zu bevorzugen als das Herunterladen von einem Dateiserver (FTP) oder den Aufruf von Webseiten.

Man stellt durch bestimmte Reservierungsprotokolle im Netz sicher, dass für die gesamte Dauer einer Datenkommunikation die Isochronität von Datenströmen gewährleistet werden kann.

IPv4- und IPv6-Pakete haben standardmäßig ein Flag (DSCP Differentiated Service CodePoint (RFC 2474); früher Precedence (RFC 791)) im IP-Header, das kennzeichnet, welcher Art die Daten in diesem Paket sind ("Traffic Class"). Anhand dieses Flags werden die Datenpakete priorisiert (d.h. bevorzugt) behandelt. Es gibt eine Reihe weiterer Verfahren zum Management von Dienstgüte.

Realisierung in IP-Netzen

Auf der theoretischen Ebene kann QoS durch Priorisierung oder Parametrisierung des Datenverkehrs, Bandbreitenreservierung, Bandbreitenlimitierung und Paketoptimierung realisiert werden.

Power over Ethernet - PoE

Power over Ethernet (PoE) bezeichnet eine Technologie, mit der netzwerkfähige Geräte über das 8-adrige Ethernet-Kabel mit Strom versorgt werden können.

Im engeren Sinne wird heute mit PoE meist der IEEE-Standard 802.3af ("*DTE Power over MDI*") gemeint, der im Juni 2003 in seiner endgültigen Fassung verabschiedet wurde. Vorher gab es bereits einige herstellereigenspezifische Implementierungen, die ebenfalls unter der Bezeichnung Power over Ethernet firmierten.

Hauptvorteil von Power over Ethernet ist, dass man ein Stromversorgungskabel einsparen kann und so auch an schwer zugänglichen Stellen oder in Bereichen, in denen viele Kabel stören würden, Ethernet-angebundene Geräte installieren kann. Somit lassen sich einerseits zum Teil drastisch Installationskosten einsparen, andererseits kann der damit einfache Einsatz einer zentralen unterbrechungsfreien Stromversorgung (USV) die Ausfallsicherheit der angeschlossenen Geräte erhöhen.

PoE wird von Netzwerkgeräten genutzt, die wenig Leistung verbrauchen. Es wird typischerweise in IP-Telefonen, kleinen Hubs, Kameras, kleinen Servern oder in

schnurlosen Übertragungsgeräten (WLAN-Access-Points, FSO-Geräte, Bluetooth-Access-Points) eingesetzt.

802.3af unterteilt die beteiligten Geräte in Energieversorger (*Power Sourcing Equipment, PSE*) und -Verbraucher (*Powered Devices, PD*). Die Versorgungsspannung beträgt 48 V, die maximale Stromaufnahme der Endgeräte 350 mA im Dauerbetrieb (kurzzeitig sind beim Einschalten 400 mA erlaubt). Daraus ergibt sich eine maximale Leistungsaufnahme von 12,95 Watt. Zur Energieübertragung werden normalerweise die freien Adernpaare im Ethernetkabel verwendet, wenn dies nicht möglich ist (weil z. B. ISDN über die Leitung geführt ist), können auch die signalführenden Adern genutzt werden. Diese Betriebsart muss jedoch sowohl vom PSE als auch vom PD explizit unterstützt werden (da die Spannung in diesem Fall durch den Ethernet-Transceiver hindurch muss). Die Stromversorgung über die Signalleitungen wirkt sich bei 10BaseT (10 Mbit/s) und 100BaseTX (100 Mbit/s) nicht allzu störend auf das Ethernet-Signal aus. Auf 1000BaseT Gigabit-Ethernet ist PoE zwar möglich, wird aber nicht empfohlen, da 1000BaseT alle 8 Adern im Kabel belegt und man deshalb in jedem Fall auf das ohnehin empfindliche Gigabit-Ethernet-Signal einwirken würde.

Die Herausforderung für die Hersteller proprietärer PoE-Lösungen bestand früher darin, Schäden an nicht PoE-fähigen Endgeräten nach Möglichkeit zu vermeiden. Obwohl die Adern 4, 5, 7 und 8 gemäß dem Ethernet-Standard eigentlich nicht belegt sind, bedeutet das nicht, dass es nicht doch Netzwerkkarten o. ä. gibt, bei denen die entsprechenden Pins nach irgendwohin durchgeschleift sind. Wenn dort versehentlich Power over Ethernet anliegen sollte, kann dies zu irreparablen Schäden am Gerät führen. 802.3af löst dieses Problem durch ein als *Resistive Power Discovery* bezeichnetes Verfahren. Hierbei legt der Energieversorger zunächst mehrfach einen nur minimalen Strom auf die Adern, mit dem sich im Normalfall kein Gerät beschädigen lässt. Er erkennt dabei, ob und wo der Energieverbraucher einen 25-kOhm-Abschlusswiderstand besitzt und damit PoE-fähig ist. Daraufhin wird der Verbraucher mit einer geringen Leistung versorgt, und muss nun signalisieren, zu welcher von vier im Standard definierten Leistungsklassen er gehört. Erst dann bekommt das PD die volle Leistung und kann den Betrieb aufnehmen.

Die Stromversorgung der Powered Devices kann dabei durch sogenannte Endspan-Devices (z. B. Switches) oder Midspan-Devices (Einheiten zwischen Switch und Endgerät) erfolgen. Strom fließt entweder über die 4 ungenutzten Drähte oder aber über die 4 Drähte, die zur Datenübertragung genutzt werden.

Als Midspan-Devices werden zumeist Hubs eingesetzt, die Strom auf die jeweiligen Drähte liefern. Aufgrund des zusätzlichen Platzbedarfs und der zusätzlich notwendigen Patchkabel in Verteilerschränken sind jetzt auch Patchpanels (Verteilerfelder, POE-Patchpanel) verfügbar, die den Strom liefern. Diese ersetzen die herkömmlichen Patchpanels und belegen somit keinen zusätzlichen Platz in den Verteilerschränken. Durch entsprechende Managementsoftware können bei diesen Verteilerfeldern die einzelnen Ports stromfrei oder stromführend definiert werden.

Quelle: www.wikipedia.org

WLAN Standards nach IEEE:

IEEE 802.11a - 54 MBit pro Sekunde - 5 GHz-Band

WLAN Standard von 1999 welcher im 5 GHz Bereich angesiedelt ist und durch den Frequenzbereich (Frequenzen von 5,725 GHz bis 5,850 GHz) relativ störungsfrei ist. Leider gibt es in dem Frequenzbereich auch Netze des Militärs und zur Flugsicherung. In Europa sind die Geräte daher nur für den Einsatz innerhalb von Gebäuden und mit einer gedrosselten Sendeleistung zugelassen. Die Reichweite ist sehr gering und liegt zwischen 15 und 25 Metern bei einer maximalen Übertragungsrate von 54 MBit pro Sekunde.

IEEE 802.11b - 11 MBit pro Sekunde - 2,4 GHz-Band

Ebenfalls ein Wireless LAN Standard von 1999 welcher im 2,4 GHz Bereich angesiedelt ist. Trotz der im Vergleich zu IEEE 802.11a geringen Übertragungsrate von 11 MBit pro Sekunde ist dieser WLAN-Standard wesentlich verbreiteter und findet sich an vielen Universitäten und auch bei öffentlichen WLAN Hot-Spots wieder. Die Vorteile sind unter anderem die höhere Reichweite von bis zu 300m, die mit externer Antenne im Outdoor-Einsatz erreicht werden kann, und auch die Kompatibilität zum IEEE 802.11g Standard. Ein wesentlicher Nachteil von IEEE 802.11b ist jedoch das Frequenzband. Da bei 2,4 GHz auch andere Geräte arbeiten und unter anderem auch Bluetooth dort angesiedelt ist, kann es zu Störungen kommen.

IEEE 802.11c - Wireless Bridging

IEEE 802.11c ist ein Standard für die drahtlose Koppelung unterschiedlicher Netzwerk-Topologien. IEEE 802.11c wurde entwickelt um mehrere Netzwerke mittels Wireless Lan verbinden zu können. Als Grundlage dieht hierbei die Mac-Adresse als Identifikation der Gegenstelle.

IEEE 802.11d - World Mode

Der IEEE 802.11d Standard wird auch gerne als „World Mode“ bezeichnet und regelt die technischen Unterschiede in unterschiedlichen Ländern und Regionen. Hierzu gehört unter anderem die Anzahl und die Auswahl der Kanäle, die in einem Land für die Nutzung von WLAN freigegeben sind. Ebenfalls geregelt wird die Auswahl der Basistechnologie, also ob IEEE 802.11 a, h, b oder g verwendet werden darf. Der Endbenutzer muss dank IEEE 802.11d lediglich seinen aktuellen Standort über eine Länder bzw. Regionsauswahl spezifizieren, das Gerät arbeitet dann mit der jeweils zugelassenen Standards.

IEEE 802.11e - QoS und Streaming-Erweiterung für a/g/h

Der IEEE 802.11e Standard sieht Neuerungen für IEEE 802.11 a, h und g vor und erweitert diese unter anderem um QOS (Quality Of Service). Mit den Änderungen

sollen die WLAN-Standards besser auf die Nutzung von Multimedia und Voice over IP (VOIP) abgestimmt werden und in der Lage sein eine gewisse Datenrate zu garantieren sowie minimale Schwankungen bei der Paketlaufzeit. QOS erlaubt es z. B. die Datenpakete für Internet-Telefonie bevorzugt zu versenden und dadurch geringere Verzögerungen zu haben.

IEEE 802.11f - Roaming nach dem IAPP für a/g/h

Der IEEE 802.11f Standard sieht Verfahren für das Roaming von Clients zwischen verschiedenen Accesspoints nach dem IAPP (Inter Access Point Protocol) vor. Mittels IEEE 802.11f wird es möglich innerhalb eines großen drahtlosen Netzwerkes seinen Standort über die Reichweite eines einzelnen Accesspoints hinaus zu verändern. Roaming bedeutet, dass die Netzwerk-Verbindung ohne Abbruch von einem Accesspoint auf den anderen übergeht.

IEEE 802.11g - 54 MBit pro Sekunde - 2,4 GHz-Band

WLAN-Standard von 2002/2003 welcher vollkommen abwärtskompatibel mit dem älteren IEEE 802.11b Standard ist und ebenfalls auf Frequenzen von 2,4 GHz bis 2,4835 GHz im 2,4 GHz Frequenzband arbeitet. Die Geschwindigkeit ist wie bei IEEE 802.11a auf maximale 54 MBit pro Sekunde beschränkt, die Sendeleistung und somit auch die Reichweite ist vergleichbar der des IEEE 802.11b Standards. Dank der Kompatibilität lassen sich IEEE 802.11g Router und Accesspoints problemlos in ein bestehendes IEEE 802.11b-Netz integrieren.

IEEE 802.11h - 54 MBit pro Sekunde - 5 GHz-Band

Der IEEE 802.11h WLAN-Standard ergänzt den IEEE 802.11a Standard um DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) und erlaubt somit nach der RegTP-Nutzungsverordnung für Frequenzen eine maximale Sendeleistung von bis zu 200 mW.

IEEE 802.11i - Authentifizierung und Verschlüsselung für a/b/g/h

Mittels IEEE 802.11i wird versucht die Sicherheit von WLANs zu erhöhen. IEEE 802.11i sieht unter anderem die Authentifizierung nach IEEE 802.1x (Extensive Authentication Protocol) vor und auch die Verschlüsselung nach AES (Advanced Encryption Standard).