LAN (Local Area Network) / Ethernet

Definition:
Ein Local Area Network (LAN) ist ein Netzwerk, das eine begrenzte geografische Fläche abdeckt, wie z. B. ein Bürogebäude, eine Schule oder ein Wohnhaus. LANs ermöglichen die Verbindung von Computern und anderen Geräten, um Daten auszutauschen und Ressourcen wie Drucker und Internetzugang gemeinsam zu nutzen.

Ethernet ist eine weit verbreitete Technologie zur Implementierung von LANs. Es definiert die physikalischen und datentechnischen Standards für die Übertragung von Daten in einem Netzwerk.
Ethernet wurde in den 1970er Jahren von Robert Metcalfe und seinem Team bei Xerox PARC entwickelt. Die erste Spezifikation wurde 1980 veröffentlicht und hat sich seitdem weiterentwickelt.

Funktionsweise:
Das ursprüngliche Ethernet basiert auf einem Koaxialkabel als Übertragungsmedium. Dabei wurden mit einem Kabel mehrere Stationen hintereinander zu einer Kette verbunden. Die Netzwerk-Topologie hat man als Bus bezeichnet.

Später wurden weitere Ethernet-Varianten für Backplanes, Twinax-Kabel, Glasfaser und Twisted-Pair entwickelt.

Der entscheidende Durchbruch von Ethernet im LAN kam durch den Umstieg von Shared- auf Switched-Media (von Bus zu Stern-Topologie) in Verbindung mit einer strukturierten Verkabelung. Gleichzeitig hat die konsequente Rückwärtskompatibilität dazu geführt, dass Investitionen bis zu einem gewissen Grad zukunftsfähig blieben. Alte Komponenten für 10 und 100 MBit/s können mit Komponenten für 1 GBit/s kombiniert werden. Im Zweifelsfall bedarf es nur eines Medienkonverters.

Ethernet transportiert Daten paketweise ohne festes Zugriffsraster. Damit unterscheidet sich Ethernet von anderen paketorientierten Systemen, die mit einem festen Zeitraster jedem Teilnehmer eine Mindestbandbreite garantieren können. Deshalb bereitet Ethernet Probleme bei allen Arten von zeitkritischen Anwendungen. Bei Ethernet gibt es keine Garantie, dass die Daten innerhalb einer bestimmten Zeit den Empfänger erreichen. Das bedeutet, der Erfolg einer Übertragung ist nicht sicher. Er unterliegt nur einer gewissen Wahrscheinlichkeit. So verwerfen Ethernet-Komponenten Datenpakete, wenn nicht genug Bandbreite zur Verfügung steht.

Wegen der unzuverlässigen Übertragungstechnik ist Ethernet auf Fehlerbehandlung höherer Protokolle angewiesen. Das ist auch ein Grund, warum in bestimmten Bereichen heute noch andere Vernetzungstechniken bevorzugt werden. Im Vergleich dazu ist Ethernet eine einfach zu implementierende Vernetzungstechnik, die sich über Jahrzehnte hinweg in lokalen Netzwerken bewährt und durchgesetzt hat.

Die tatsächliche Übertragungsgeschwindigkeit (Netto-Datenrate) von Ethernet hängt von der Geschwindigkeitsstufe und der TCP-Verbindungsqualität ab.

Standards:

Gebräuchliche Ethernet-Varianten

Bezeichnung	Übertragungsmedium	max. Segmentlänge	Datenrate (brutto)
100Base-TX	TP-Kabel (2 Adernpaare)	100 m	100 MBit/s
1000Base-T (1GE)	TP-Kabel (4-Adernpaare)	100 m	1.000 MBit/s
1000Base-SX	2 MMF-Glasfasern	220 - 550 m	1.000 MBit/s
1000Base-LX	2 SMF-Glasfasern	5 km	1.000 MBit/s
1000Base-BX10	1 SMF-Glasfaser	5 k	1.000 MBit/s
2500Base-T (2G5)	TP-Kabel (4-Adernpaare)	100 m	2.500 MBit/s
5000Base-T (5GE)	TP-Kabel (4-Adernpaare)	100 m	5.000 MBit/s
10Base-T (10GE)	TP-Kabel (4-Adernpaare)	(Cat6a) 100 m	10.000 MBit/s
10Base-SR	2 MMF-Glasfasern	25 - 400 m	10.000 MBit/s
10Base-LR	2 SMF-Glasfasern	10 km	10.000 MBit/s
10Base-BX	1 SMF-Glasfasern	40 km	10.000 MBit/s

Auto-Negotiation

Mit Auto-Negotiation können Ethernet-Hosts automatisch die Ethernet-Variante der Gegenstelle am anderen Ende der Leitung erkennen. Häufig wird Auto-Negotiation auch als Auto-Sensing bezeichnet. Dieser Begriff ist allerdings missverständlich und sollte daher nicht verwendet werden.

Auto-Negotiation wurde deshalb notwendig, weil der Umstieg von 10Base-T auf 100Base-TX in der Regel in einem Mischbetrieb endete. Aus diesem Grund beherrschen Fast-Ethernet-Komponenten durchgängig Auto-Negotiation.

Um Probleme mit Auto-Negotiation zu vermeiden, sollte man die Netzwerk-Stationen entweder mit Auto-Negotiation betreiben oder auf eine feste Übertragungsart einstellen. Probleme treten in der Regel nur dann auf, wenn man Vollduplex- und Halbduplex-fähige Komponenten mischt.

Bei den Glasfaser-Varianten ist Auto-Negotiation nicht definiert. Hier muss man Voll- oder Halbduplex manuell einstellen.

Übertragungstechnik:

Fast-Ethernet ist die Weiterentwicklung des Ethernet-Standards 10Base-T, um über Twisted-Pair-Kabel 100 MBit/s zu übertragen. Durch den Leitungscode 4B5B wird die Übertragungsrate von 10 MBit/s auf 100 MBit/s angehoben. Dabei werden 4 Bit binäre Dateninformationen in 5 Bit binäre Übertragungsinformationen codiert. Die Reichweite ist wie bei 10Base-T auf 100 Meter beschränkt.

Die CAT-Kategorie gibt an, welche Frequenz der Datenübertragung erreicht werden kann. Je höher die CAT-Kategorie eines Kabels ist, desto höher sind Frequenz und Übertragungsrate bei Gebrauch dieses Kabels.

Kategorie	Maximale Übertragungsgeschwindigkeit (100 Meter)	Maximale Bandbreite
Cat5	10/100 Mbps	100 MHz
Cat5e	1000 Mbps / 1 Gbps	100 MHz
Cat 6	1000 Mbps / 1 Gbps	250 MHz
Cat6a	10000 Mbps / 10 Gbps	500 MHz
Cat7	10000 Mbps / 10 Gbps	600 MHz
Cat8	25 Gbps oder 40 Gbps	2000 MHz bei 30 Meter

Internet Protokolle:

Im wesentlichen gibt es zwei Übertragungsprotokolle – IPV4 und IPV6. IPv4 war die erste stabile Version des Internet-Protokolls. IPv6 ist die neueste Version und soll IPv4 ersetzen.

IPv4- und IPv6-Pakete sind unterschiedlich zusammengesetzt, wobei IPv6 unterschiedliche Header und insgesamt einen kürzeren Header-Speicherplatz besitzt. IPv6 bietet auch separate Header-Pakete als Feature zur Erweiterung der Routing-Optionen.

Die vollständige Adressumgebung von IPv4 beträgt 2^{32} oder 4.294.967.296 IP-Adressen. IPv6 hat einen deutlich höheren Adressraum von 2^{1} ², oder $3{,}403\times10^{3}$, oder 340.282.366.920.938.000.000.000.000.000.000.000 eindeutigen IP-Adressen. Diese Zahl entspricht auf Englisch etwa 340 Undezimillion, 300 Dezillion.

Von den IPv4-Internetadressen gibt es rund 588 Millionen reservierte IP-Adressen, der Rest ist öffentlich verfügbar. Aufgrund der Zunahme von Internetgeräten waren die nicht zugewiesenen IPv4-Internetadressen 2011 erschöpft. IPv6 bietet zwar eine Lösung für den erschöpften Adressraum, die aktuelle Lösung stellt jedoch eine Abstraktion dar, indem andere Adressierungssysteme – wie Network Address Translation (NAT) – auf IPv4 aufgesetzt werden.

IPv6 hat auch eine große Anzahl reservierter IP-Adressen – bei einem insgesamt viel größere Adressumgebung ist dies jedoch im Vergleich keine signifikante Zahl. Nach aktuellen Schätzungen ist die Adressumgebung unerschöpflich.

In IPv4 wird der Adressname durch eine numerische Adresse mit vier Dezimalzahlen (im Bereich von 0–255) dargestellt, die jeweils acht Bit repräsentieren, getrennt durch drei Punkte: z.B. 192.169.128.1

In IPv6 wird der Adressname durch acht Hexadezimalzahlen dargestellt, die aus Zahlen (0–9) und Buchstaben (A–F) bestehen, die jeweils für vier Bit stehen und durch Doppelpunkte getrennt sind: z.B. *2600:1400:d:5a3::3bd4*

Bei IPv4 ist ein DHCP-Server (Dynamic Host Configuration Protocol) erforderlich, um die IP-Adresszuweisung abzuwickeln und Computer zu identifizieren, die mit einem Netzwerk verbunden sind.

In IPv6 wird Stateless Address Autoconfiguration (SLAAC) verwendet, bei der das Gerät selbst seine eigene Adresse ohne externe Partei oder Protokoll automatisch konfigurieren kann. Da kein DHCP mehr erforderlich ist, wird auch der Gesamtverkehr im Netzwerk reduziert.

IPv4-Adressraum:

Der IPv4-Adressraum umfasst 32 Bit und reicht von 0.0.0.0 bis 255.255.255.255. Rein rechnerisch ergibt sich aus einer 32-Bit-Adresse eine Anzahl von 2 hoch 32 Adressen. Das entspricht über 4 Milliarden Adressen. Als man den Adressraum definierte, entsprach das damals ungefähr der Weltbevölkerung. Damals war es undenkbar, dass jeder Mensch irgendwann mal eine IPv4-Adresse brauchen, geschweige denn, dass jemand ein persönliches Endgerät (Smartphone) mit einer IPv4-Adresse mit sich herumtrage würde.

Für jede IP-Adresse müsste ein IP-Router wissen, wo sich der entsprechende Host befindet. Das wäre bei 4 Milliarden IPv4-Adressen ein sehr großer Datenbestand, der bei jedem Datenpaket erneut durchlaufen werden müsste, um den Host zu finden. Außerdem müsste jeder Router auf dem Weg zum Host den Vorgang wiederholen. Das würde viel Rechenleistung und Speicherkapazität voraussetzen, die in der Anfangszeit von TCP/IP undenkbar war. Aus diesem Grund hat man dem IPv4-Adressraum eine gewisse Struktur gegeben, um die Routing-Entscheidungen in den Routern einfacher zu machen. Insbesondere vor dem Hintergrund, dass damals die Verfügbarkeit von Rechenleistung und Speicher geringer war.

Jede IPv4-Adresse besteht im Prinzip aus zwei Teilen. Dem Netz (Subnetz) bzw. der Netzadresse (Netz-ID) und dem Host bzw. der Hostadresse (Host-ID). Beide Teile werden in der IP-Adresse abgebildet.

Für das IP-Routing ist nur die Netzadresse wichtig. Und die Hostadresse ist nur für den Router wichtig, in dessen Netz sich der Host befindet.

Bei einer IPv4-Adresse ist der vordere Teil die Netzadresse und der hintere Teil die Hostadresse. Die Teilung findet typischerweise an einem Punkt (".") statt. Aber nicht immer. An welcher Stelle genau die IPv4-Adresse in Netz und Host geteilt wird, dass entscheidet die Netzklasse, die Subnetzmaske oder das CIDR-Suffix.

Die erste und letzte IPv4-Adresse eines Subnetzes sind reserviert

- Die erste IPv4-Adresse eines Subnetzes adressiert das Netz und ist somit die Netz-Adresse.
- Die letzte IPv4-Adresse eines Subnetzes adressiert alle Teilnehmer in dem Netzwerk und ist somit die Broadcast-Adresse.

Nicht routbare IPv4-Adressen

- 0.0.0.0/8 (0.0.0.0 bis 0.255.255.255): Standard- bzw. Default-Route im Subnetz (Current Network).
- 127.0.0.0/8 (127.0.0.0 bis 127.255.255.255): Reserviert für den Local Loop bzw. Loopback.

Private IPv4-Adressen

- 10.0.0.0/8 (10.0.0.0 bis 10.255.255.255): Reserviert für die Nutzung in privaten Netzwerken. Nicht im Internet routbar.
- 172.16.0.0/12 (172.16.0.0 bis 172.31.255.255): Reserviert für die Nutzung in privaten Netzwerken. Nicht im Internet routbar.
- 192.168.0.0/16 (192.168.0.0 bis 192.168.255.255): Reserviert für die Nutzung in privaten Netzwerken. Nicht im Internet routbar.
- 169.254.0.0/16 (169.254.0.0 bis 169.254.255.255): Link-local Adresses für IPv4LL.

Class D (Multicast)

- 224.0.0.0 bis 239.255.255.255: Nicht im Internet, sondern nur lokal in den eigenen Netzen routbar.

Class E (reservierte Adressen)

- 240.0.0.0 bis 255.255.255.255: Alte IPv4-Stacks, die nur mit Netzklassen arbeiten, kommen damit nicht klar.

Localhost oder Local Loop:

Der gesamte Adressbereich von 127.0.0.0 bis 127.255.255.255 ist für den Local Loop bzw. Loopback reserviert.

Die IPv4-Adresse 127.0.0.1 hat jeder IPv4-Host. Diese IPv4-Adresse wird auch als Localhost (Namensauflösung: localhost) bezeichnet. Es handelt sich dabei um ein virtuelles Interface. Das aber keiner Hardware zugeordnet ist. Dieses virtuelle Interface wird von Anwendungen verwendet, die über das Netzwerk kommunizieren wollen/müssen, dabei aber nicht das lokale Netzwerk in Anspruch nehmen können/wollen. Wird ein Datenpaket mit der Ziel-Adresse 127.0.0.1 verschickt, so wird sie an den Absender selber verschickt. Diese IPv4-Adresse kann zum Testen verwendet werden. Zum Beispiel, ob TCP/IP oder eine darüber erreichbare Anwendung korrekt installiert und konfiguriert ist.

IPv4LL - Local Link Addressen:

Beim Adressbereich von 169.254.0.0 bis 169.254.255.255 (169.254.0.0/16) handelt es sich um link-lokale IPv4-Adressen. Dieser Adressbereich wird von Rechnern genutzt, bei denen die automatische IPv4-Konfiguration per BOOTP oder DHCP fehlgeschlagen ist. Durch die Selbstzuweisung link-lokaler IPv4-Adressen sind alle Rechner im selben Adressbreich in einem gemeinsamen lokalen Netzwerk in der Lage miteinander zu kommunizieren.

Broadcast-Adresse:

Datenpakete mit der Broadcast-Adresse als Zieladresse werden in dem jeweiligen Subnetz an alle Hosts geschickt. Eine Broadcast-Adresse innerhalb eines Netzwerks dient dazu, alle Hosts innerhalb eines Netzwerks zu erreichen. Beispielsweise um Dienste im Netzwerk in Anspruch zu nehmen, bei denen die Adresse noch nicht bekannt ist. Zum Beispiel DHCP für die IPv4-Konfiguration, Datei- und Druckerfreigaben oder einen Gaming-Server.

Private IP-Adressen / Address zuweisung für private Internets (RFC1918):

IPv4-Adressen sind begrenzt und müssen offiziell beantragt und zugeteilt werden. Man kann also nicht irgendeine IPv4-Adresse verwenden. Allerdings gibt es für die private und nicht-öffentliche Nutzung von TCP/IP spezielle Adressräume, die innerhalb von privaten Netzen frei zur Verfügung stehen und nicht im öffentlichen Internet geroutet werden. Wenn man nun ein privates lokales Netzwerk aufbauen möchte, verwendet man solche privaten IPv4-Adressen, wenn man zu wenige oder keine öffentlichen IPv4-Adressen hat. Die privaten IPv4-Adressen haben aber den Nachteil, dass sie nur im jeweiligen lokalen Netzwerk gültig sind und nicht in öffentliche Netzen geroutet werden. Datenpakete mit privaten IPv4-Adressen verbleiben in den lokalen Netzwerken. Umgekehrt heißt das auch, dass Hosts, die nur eine private IPv4-Adresse haben, nicht direkt aus dem Internet erreichbar sind.

Von	Bis	Suffix	Netzklasse	Anzahl Netze	Hosts pro Netz
10.0.0.0	10.255.255.255	/8	A (255.0.0.0)	1	16.777.214
172.16.0.0	172.31.255.255	/12	B (255.255.0.0)	16	65.534
192.168.0.0	192.168.255.255	/16	C (255.255.255.0)	256	254

Wenn ein lokaler Host mit dem Internet verbunden werden soll, dann benötigt er eine öffentliche IPv4-Adresse. Leider hat die großzügige Zuteilung der öffentlichen IPv4-Adressen dazu geführt, dass es keine öffentlichen IPv4-Adressen für jeden Host gibt. Bei Internet-Zugängen löst man die Problematik mit NAT. Dabei bekommt nur der Internet-Zugangs-Router eine öffentliche IPv4-Adresse und alle anderen Hosts in seinem Netzwerk eine private IPv4-Adresse. Das NAT-Protokoll sorgt nun dafür, dass sich mehrere lokale Hosts eine öffentliche IP-Adresse teilen können.