Ports, IP- und Mac-Adressen

Was ist ein Computerport?

Ein Port in der IT-Technik hat drei Hauptbedeutungen in Netzwerken, Computerhardware und Software:

- Ein Port in einem Netzwerk ist eine softwaredefinierte Nummer, die einem Netzwerkprotokoll zugeordnet ist und Kommunikation für einen bestimmten Dienst empfängt oder überträgt.
- Ein Port bei der Computerhardware ist eine Buchse oder ein Sockel, an den Peripheriegeräte oder das Netzwerk angeschlossen werden.
- Ein Port oder einer Portierung bei der Computersoftware bedeutet, dass eine Software übersetzt oder konvertiert wurde, um auf einer anderen Hardware oder einem anderen Betriebssystem zu laufen, als sie ursprünglich konzipiert wurde.

Was ist ein Port in einem Netzwerk?

Ein Port in Computernetzwerken bedeutet, dass ein Computer eine einzige physische Netzwerkverbindung nutzen kann, um viele eingehende und ausgehende Anfragen zu bearbeiten, indem er jeder eine Portnummer zuweist. Die Nummern reichen von 0 bis 65535, was eine 16-Bit-Zahl entspricht.

Einige dieser Portnummern sind speziell definiert und immer mit einer bestimmten Art von Dienst verbunden, zum Beispiel hat das File Transfer Protocol (FTP) immer die Portnummer 21 und der HTTP-Webverkehr (Hypertext Transfer Protocol) immer den Port 80. Sie werden als bekannte Ports bezeichnet, deren Bereich sich von 0 bis 1023 erstreckt.

Die Nummern ab 1024 bis 49151 werden als registrierte Ports bezeichnet und lassen sich bei der Internet Assigned Numbers Authority (IANA) für einen bestimmten Zweck registrieren. Die Nummern 49152 bis 65535 sind nicht zugewiesen, können von jeder Art von Dienst verwendet werden und sind als dynamische Ports, private Ports oder Ephemeral Ports bekannt.

Zur Veranschaulichung: Stellen Sie sich eine Portnummer wie eine Telefondurchwahl in einem Unternehmenstelefonsystem vor. Die allgemeine Telefonnummer des Unternehmens ist vergleichbar mit der IP-Adresse (Internet Protocol) oder der URL (Uniform Resource Locator) eines Computers. Diese Telefonnummer verbindet die Benutzer mit dem richtigen Unternehmen, legt aber nicht fest, mit wem sie im Unternehmen sprechen wollen. Erst eine Telefondurchwahl verbindet Sie mit der richtigen Person in einer Organisation. Der Port verbindet Sie dagegen mit dem richtigen Dienst auf einem Computer. Die Durchwahl 0 zu wählen, um mit einer Vermittlung zu sprechen, ist in allen Telefonanlagen weit verbreitet und entspricht einem der bekannten Ports, die immer bestimmte Dienste definieren.

Ein Port ist immer mit einem Protokoll verbunden. In der Regel handelt es sich dabei um das Transmission Control Protocol (TCP) oder das User Datagram Protocol (UDP) für die Kommunikation, aber auch ICMP-Nachrichten (Internet Control Message Protocol) verwenden bestimmte Ports. Der Port wird durch die URL oder IP-Adresse, gefolgt von einem Doppelpunkt und der Portnummer, angegeben - zum Beispiel 10.0.0.1:80 oder www.techtarget.de:443 (das ist der Port für HTTPS). Bei jeder Internetkommunikation gibt es immer einen zugehörigen Port, der dem Benutzer jedoch nicht unbedingt angezeigt wird, da die Art der Kommunikation ihn oft voraussetzt.

Ein Computer kann viele gleichzeitige Verbindungen über einen einzigen eingehenden Port verwalten. Das liegt daran, dass die lokale IP-Adresse, der lokale Port, die entfernte IP-Adresse und der entfernte Port jede Verbindung spezifizieren. Ein abhörender Port bedeutet, dass der Computer aktiv auf eingehende Anfragen an dieser Portnummer wartet und diese Verbindungen zulässt. Bei der Portweiterleitung wird die Kommunikation an eine Adresse an einem bestimmten Port zur Verarbeitung an einen anderen Computer gesendet oder weitergeleitet.

Wie wirken sich Netzwerkports auf die Cybersicherheit aus?

Netzwerkports sind ein wichtiger Faktor für die Netzwerksicherheit und die Cybersicherheit im Allgemeinen.

Beim Port-Scanning werden zum Beispiel alle Ports einer Adresse überprüft, um festzustellen, welche offen sind und abgehört werden. Angreifer können dies nutzen, um anfällige Dienste zu finden, die sie dann angreifen können.

Firewalls berücksichtigen die Portnummer, wenn sie entscheiden, ob sie die Kommunikation zulassen oder blockieren. Sie sind so konfiguriert, dass sie nur die Kommunikation mit den für einen Dienst benötigten Ports erlauben und andere nicht benötigte Ports blockieren, damit sie nicht ausgenutzt werden können.

Ein Beispiel für die Verwendung von Ports: Ein Unternehmen möchte eine Webseite, E-Mail und einen sicheren Dateitransferdienst im Internet anbieten. Die Firewall würde eingehende Verbindungen zu den Ports 80 und 443 für Webverkehr, Port 25 für eingehende E-Mails und Port 22 für Secure Shell FTP (SFTP) zulassen. Sie leitet diese Ports an die spezifischen Server für jeden Diensttyp weiter. Alle anderen Ports werden von der Firewall blockiert.

Wenn also ein Mitarbeiter fälschlicherweise probiert, FTP an Port 21 statt SFTP zu verwenden, wird dies blockiert. Oder wenn ein Angreifer versucht, eine Verbindung zu Port 3389 für Windows Remote Desktop herzustellen, um die Kontrolle über einen Server zu erlangen, blockiert die Firewall die Verbindung.

IP-Adresse

Eine IP-Adresse ist eine Adresse in Computernetzen, die – wie das Internet – auf dem Internetprotokoll (IP) basieren. Sie wird Geräten zugewiesen, die an das Netz angebunden sind, macht die Geräte so adressierbar und damit erreichbar. Die IP-Adresse kann einen einzelnen Empfänger oder eine Gruppe von Empfängern bezeichnen (Multicast, Broadcast). Umgekehrt können einem Computer mehrere IP-Adressen zugeordnet sein.

Die IP-Adresse wird vor allem verwendet, um Daten von ihrem Absender zum vorgesehenen Empfänger zu transportieren. Ähnlich der Postanschrift auf einem Briefumschlag werden Datenpakete mit einer IP-Adresse versehen, die den Empfänger eindeutig identifiziert. Aufgrund dieser Adresse können die „Poststellen“, die Router, entscheiden, in welche Richtung das Paket weitertransportiert werden soll. Im Gegensatz zu Postadressen sind IP-Adressen nicht an einen bestimmten Ort gebunden.

Die bekannteste Notation der heute geläufigen IPv4-Adressen besteht aus vier Zahlen, die Werte von 0 bis 255 annehmen können und mit einem Punkt getrennt werden, beispielsweise 192.0.2.42. Technisch gesehen ist die Adresse eine 32-stellige (IPv4) oder 128-stellige (IPv6) Binärzahl.

Grundlagen

Um eine Kommunikation zwischen zwei technischen Geräten aufzubauen, muss jedes der Geräte in der Lage sein, dem anderen Gerät Daten zu senden. Damit diese Daten bei der richtigen Gegenstelle ankommen, muss diese eindeutig benannt (adressiert) werden. Dies geschieht in IP-Netzen mit einer IP-Adresse. So wird zum Beispiel ein Webserver von einem Webbrowser direkt über seine IP-Adresse angesprochen. Der Browser fragt dazu bei einem Nameserver die IP-Adresse ab, die einer Domain (zum Beispiel „www.example.com“) zugeordnet ist. Anschließend nutzt er diese IP-Adresse, um Daten an den Webserver zu senden.

IP-Adresse in IP-Datenpaketen

Jedes IP-Datenpaket beginnt mit einem Informationsbereich für die Beförderung durch die IP-Schicht, dem IP-Header. Dieser Header enthält auch zwei Felder, in welche die IP-Adressen sowohl des Senders als auch des Empfängers eingetragen werden, bevor das Datenpaket verschickt wird. Die Vermittlung geschieht auf der Schicht 3 im OSI-Modell, der Vermittlungsschicht.

IPv4

IPv4 (Internet Protocol Version 4), vor der Entwicklung von IPv6 auch einfach IP, ist die vierte Version des Internet Protocols (IP). Es war die erste Version des Internet Protocols, welche weltweit verbreitet und eingesetzt wurde, und bildet als Teil der Internetprotokollfamilie eine wichtige technische Grundlage des Internets. Es wurde in RFC 791 im Jahr 1981 definiert und stellt einen Internetstandard der Internet Engineering Task Force dar. IPv4 verwendet 32 Bit lange IP-Adressen.

Geschichte

IPv4 wurde als Teil der Internetprotokollfamilie für das Arpanet entwickelt und kam darin ab 1983 zum Einsatz. Damals waren nur einige hundert Rechner an das Netz angeschlossen. Das Arpanet entwickelte sich zum Internet und überschritt 1989 die Grenze von 100.000 Rechnern. Durch seine Verbreitung im Internet hat IPv4 schließlich auch LAN-Protokolle wie DECnet oder IPX verdrängt. NetWare, AppleTalk und NetBIOS wurden als neue Versionen hervorgebracht, die auf IP aufsetzen.

Am Anfang der 1990er Jahre war erkennbar, dass IP-Adressen bald knapp würden, da die damals übliche Netzklassen-basierte Adressvergabe erheblichen Verschnitt verursachte. Als kurzfristige Lösung wurde 1993 Classless Inter-Domain Routing eingeführt, das eine deutlich effizientere Adressvergabe ermöglichte. Eine weitere kurzfristige Lösung war das 1994 eingeführte Network Address Translation (NAT), das die Wiederverwendung von IP-Adressen ermöglichte. In der Variante Network Address Port Translation (NAPT) ermöglichte es die gleichzeitige Mehrfachverwendung von IP-Adressen. Mit diesen Maßnahmen konnte der Adressbedarf soweit gedämpft werden, dass der Adressraum trotz immensen Wachstums des Internet erst in den 2010er Jahren knapp wurde.

Als langfristige Lösung der Adressknappheit sollte ein neues Protokoll mit größerem Adressraum entwickelt werden. Dies führte zuerst zur Entwicklung des experimentellen Protokolls TP/IX, das die Versionsnummer 7 trug und 1993 veröffentlicht wurde. TP/IX sollte dabei einen 64-Bit-Adressbereich unterstützen, wurde dann aber zugunsten von IPv6 verworfen. Die erste Fassung von IPv6 wurde 1995 veröffentlicht und verwendete einen 128-Bit-Adressraum. Die Versionsnummer 5 wurde nicht für einen IPv4-Nachfolger verwendet, da sie bereits 1990 durch das experimentelle Internet Stream Protocol Version 2 (ST2) belegt war, einem für Streaming optimierten Protokoll.

Adressformat

IPv4 benutzt 32-Bit-Adressen, wodurch ein Adressraum von knapp 4,3 Milliarden Adressen zur Verfügung steht. IPv4-Adressen werden meist in Dezimalpunktschreibweise dargestellt: vier Oktetts (je 8 Bit) werden durch Punkt getrennt mit vier Zahlen von 0 bis 255 dargestellt.

Beispiel: 192.0.2.155

Eine IPv4-Adresse kann in dezimal, binär, oktal und hexadezimal sowohl in der Punkt-, als auch in der Nichtpunktnotation dargestellt werden. Eine führende Null zeigt eine Oktalzahl an. Daher dürfen in der Dezimalpunktschreibweise ein- und zweistellige Zahlen nicht auf ein gleichförmiges Längenformat gebracht werden (nicht: 192.000.002.155).

Jedes der vier Oktette besteht aus 8 Bit und stellt somit 28 = 256 verschiedene Werte dar. Daraus ergibt sich eine Gesamtzahl von 256 × 256 × 256 × 256 = 2564 = 232 = 4.294.967.296 IPv4-Adressen.

Netzanteil und Hostanteil

Eine IP-Adresse besteht aus einem Netzanteil und einem Hostanteil. Der Netzanteil identifiziert ein Teilnetz, der Hostanteil identifiziert ein Gerät (Host) innerhalb eines Teilnetzes.

Die genaue Aufteilung zwischen Netzanteil und Hostanteil wird durch eine Subnetzmaske festgelegt, beispielsweise 255.255.255.0, was in binärer Darstellung 11111111.11111111.11111111.00000000 entspricht. Die Bits der Subnetzmaske, die „1“ lauten, legen die Stellen der IP-Adresse fest, die zum Netzanteil gehören. Alle restlichen Stellen der IP-Adresse, die entsprechend in der Subnetzmaske auf „0“ gesetzt sind, gehören zum Hostanteil. In der CIDR-Notation wird die Länge des Netzanteils durch die Anzahl Bits angegeben und mit Schrägstrich getrennt als Suffix an die IP-Adresse angehängt, beispielsweise /24. Somit ist der Netzanteil 24 Bits lang, was der Subnetzmaske 255.255.255.0 entspricht. Die übrigen 8 Bits gehören somit zum Hostanteil.

<u>Beispiel:</u>

	dezimal			binär	
IP-Adresse	192.0.2	.155	→	11000000.00000000.00000010	.10011011
Subnetzmaske	255.255.255	.0	→	11111111.11111111.11111111	.00000000
	Netzanteil	*Hostanteil*		*Netzanteil*	*Hostanteil*
CIDR-Notation	192.0.2.155/24				

Die Unterscheidung zwischen Netzanteil und Hostanteil ist erforderlich für die Entscheidung, ob sich eine Zieladresse in demselben lokalen Netz oder in einem anderen Netz befindet. Wenn der Netzanteil identisch ist, können die Endgeräte innerhalb einer Broadcast-Domäne direkt miteinander kommunizieren, beispielsweise per Ethernet oder WLAN. Im selben Teilnetz darf der Hostanteil nicht mehrfach vergeben sein, da es ansonsten zu einem IP-Adresskonflikt kommt. Für jedes Endgerät vergibt der zuständige Netzwerkadministrator den Hostanteil eindeutig durch eine manuelle oder automatische IP-Adresszuweisung.

Für die Kommunikation zwischen unterschiedlichen Netzen wird ein Router benötigt. Der Netzanteil muss ebenfalls eindeutig sein, damit es nicht zu Routing-Konflikten führt. Die Vergabe von IP-Netzbereichen erfolgt durch eine hierarchische Organisationsstruktur zwischen der Internet Assigned Numbers Authority, den Regional Internet Registrys und den Local Internet Registrys.

Subnetting

Ein Netz kann in weitere Teil- oder Subnetze unterteilt werden. Dies erfolgt, indem ein oder mehrere höchwertige Bits des Hostanteils zur Unterscheidung des Subnetzes verwendet werden. Innerhalb eines Subnetzes wird die Subnetzmaske angepasst, um den verkleinerten Hostanteil widerzuspiegeln. Subnetting wird zur Segmentierung von Netzen verwendet. Für die Kommunikation zwischen den Subnetzen ist ein Router erforderlich.

Beispiel:

	Netzadresse (CIDR)	Subnetzmaske	Adressbereich	Netz-, Subnetz- und Hostanteil (binär)
Netz	192.0.2.0/24	255.255.255.0	192.0.2.0 – 192.0.2.255	11000000.00000000.00000010.xxxxxxxx
Subnetz	192.0.2.0/25	255.255.255.128	192.0.2.0 – 192.0.2.127	11000000.00000000.00000010.0xxxxxxx
Subnetz	192.0.2.128/26	255.255.255.192	192.0.2.128 – 192.0.2.191	11000000.00000000.00000010.10xxxxxx
Subnetz	192.0.2.192/26	255.255.255.192	192.0.2.192 – 192.0.2.255	11000000.00000000.00000010.11xxxxxx

Nach außen hin wird das Netz beim Routing als ein ganzes adressiert. Die innere Unterteilung in Subnetze ist nicht direkt ersichtlich. Das Gegenteil von Subnetting ist Supernetting und beschreibt die Zusammenfassung von mehreren angrenzenden Netzadressen in einer gemeinsamen Route. Der Zweck ist die Minimierung von Einträgen in einer Routingtabelle. Supernetting wird bei Classless Inter-Domain Routing als Routenaggregation bezeichnet.

Historische Netzklassen (nicht mehr in Gebrauch seit 1993)

Ursprünglich gab es fest vorgeschriebene Einteilungen für Netzklassen mit einer festen Länge des Netzanteils. Die Größe des Netzanteils ergab sich aus den ersten Bits der Adresse; eine Subnetzmaske musste nicht angegeben werden. Da diese Einteilung sehr unflexibel ist, wird seit 1993 ausschließlich das Verfahren Classless Inter-Domain Routing angewandt, welches bitvariable Netzmasken ermöglicht. Obwohl das Konzept von Netzklassen seitdem nicht mehr im Einsatz ist, blieb der Begriff der Netzklasse über Jahre verbreitet. Hierbei steht „Klasse A“ für ein Netz der CIDR-Präfixlänge /8, „Klasse B“ für /16 und „Klasse C“ für /24. Die ursprüngliche Zuordnung zu festgelegten Adressbereichen wird für gewöhnlich ignoriert, sodass diese Begrifflichkeit nicht mit dem ursprünglichen Konzept der Netzklassen konform ist.

Nutzbare Adressen

Die jeweils erste und letzte Adresse eines Subnetzes haben eine besondere Bedeutung und stehen üblicherweise nicht zur Vergabe an Hosts zur Verfügung. Die maximale Anzahl der zu vergebenen Hostadressen in einem Netz beträgt somit effektiv:

$2^{\text{Anzahl Bits der Hostadresse}} - 2.$

Diese Einschränkung geht auf die Praxis zurück, Adressen mit „0“ an allen Stellen als „dieses Netz“ und Adressen mit „1“ an allen Stellen als „alle Hosts“ zu interpretieren. Die erste Adresse eines Subnetzes (zum Beispiel 192.0.2.0) bezeichnet das Netz selbst. Die letzte Adresse (zum Beispiel 192.0.2.255) bezeichnet die Broadcast-Adresse, unter der alle Hosts im Netz angesprochen werden können. Ein Versuch, diese Einschränkung aufzuheben, hat sich nicht durchgesetzt, sodass auch heute noch in praktisch jedem Netz beide Adressen reserviert sind. Gängig ist außerdem, das Default Gateway auf die zweite oder die vorletzte IP-Adresse im Netz zu legen (zum Beispiel 192.0.2.1 oder 192.0.2.254), wobei es dafür keinerlei Vorgaben gibt.

Besondere Netzadressen

Einige Netzadressen sind für spezielle Zwecke reserviert:

Adressblock (Präfix)	Verwendung	Referenz
0.0.0.0/8	Das vorliegende Netzwerk	RFC 1122
10.0.0.0/8	Private Netze	RFC 1918
100.64.0.0/10	Shared Transition Space	RFC 6598
127.0.0.0/8	Loopback (Lokaler Computer)	RFC 1122
169.254.0.0/16	Automatische Adresskonfiguration (link local), APIPA	RFC 3927
172.16.0.0/12	Private Netze	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 6890
192.0.2.0/24	Dokumentationszwecke	RFC 6890
192.88.99.0/24	IPv6 zu IPv4 Relay (Veraltet)	RFC 7526
192.168.0.0/16	Private Netze	RFC 1918
198.18.0.0/15	Netzwerk-Benchmark-Tests	RFC 2544
198.51.100.0/24	Dokumentationszwecke	RFC 6890
203.0.113.0/24	Dokumentationszwecke	RFC 6890
224.0.0.0/4	Multicasts	RFC 5771
240.0.0.0/4	Reserviert	RFC 1700
255.255.255.255/32	Limited Broadcast	RFC 919, RFC 922

Private IP-Adressen

Bestimmte IP-Adressbereiche stehen zur freien Verfügung und können ohne vorherige Registrierung für private Netze verwendet werden. Im Internet werden diese IP-Adressbereiche nicht geroutet. Historisch befand sich jeder der Adressbereiche in einer anderen Netzklasse. Aus Gewohnheitsgründen ist es gängig für Subnetze im Adressblock 172.16.0.0/12 die Präfixlänge /16 und im Adressblock 192.168.0.0/16 die Präfixlänge /24 zu verwenden. Eine Vorgabe existiert diesbezüglich nicht.

Paketformat

Ein IP-Paket besteht aus einem Header und den eigentlichen Nutzdaten. Der IPv4-Header ist normalerweise 20 Bytes lang, kann aber durch zusätzliche Optionen in jeweils 4-Byte-Schritten auf bis zu 60 Bytes verlängert werden. Die Optionen sind größtenteils ungenutzt und IPv4-Pakete mit Optionen werden oft blockiert.

IPv4 dient als Grundlage, um darüber andere Protokolle zu transportieren. In dem Datenteil eines IP-Pakets werden der Header, die Nutzdaten und ein eventueller Trailer eines anderen Netzwerkprotokolls gekapselt. Typische Beispiele sind TCP, UDP oder ICMP. Um welches Protokoll es sich handelt, wird durch eine Nummer im Protokoll-Feld des IP-Headers festgelegt. Die Internet Assigned Numbers Authority verwaltet eine Liste der registrierten Protokollnummern.

Die maximale Länge eines IP-Pakets beträgt 65535 Bytes (216−1) und die maximale Datenlänge 65515 Bytes (Paketlänge – minimale Headerlänge von 20 Byte). Die Paketlänge wird jedoch normalerweise von dem zugrundeliegenden Netzwerkprotokoll auf Netzzugangsschicht weiter eingeschränkt, woraus sich eine für das Netz spezifische maximale IP-Paketlänge ergibt, die Maximum Transmission Unit (MTU) genannt wird. Bei Ethernet beispielsweise beträgt die MTU 1500 Bytes. Die MTU reduziert sich, wenn ein IP-Paket über einen Tunnel oder ein Virtual Private Network transportiert wird. Die minimale Frame-Länge von Ethernet hat hingegen keine Auswirkung auf IPv4, da durch das Längenfeld im IPv4-Header ein beliebig kurzes IPv4-Paket transportiert werden kann, selbst wenn der Ethernet-Frame mit Nullbytes aufgefüllt werden muss.

Eine spezielle Bedeutung kommt in modernen Implementierungen dem früheren Feld Type of Service (ToS) im zweiten Oktett des IPv4-Headers zu. Ursprünglich diente dieses Feld bei der Vermittlung eines

Datenpaketes als Entscheidungshilfe für die beteiligten Router bei der Wahl der Übertragungsparameter. In modernen Implementierungen wird dieses Feld im Zusammenhang mit der network congestion avoidance (Vermeidung von Überlastungen) verwendet. Das ToS-Feld wurde durch das DS-Feld (differentiated services) ersetzt, dessen erste sechs Bits als differentiated services code point (DSCP) und dessen letzte beiden Bits als explicit congestion notification (ECN) benutzt werden.

Routing

IPv4 unterscheidet nicht zwischen Endgeräten (Hosts) und Vermittlungsgeräten (Router). Jeder Computer und jedes Gerät kann gleichzeitig Endpunkt und Router sein. Ein Router verbindet dabei verschiedene Netze. Die Gesamtheit aller über Router verbundenen Netze bildet das Internet.

IPv4 ist für LANs und WANs gleichermaßen geeignet. Ein Paket kann verschiedene Netze vom Sender zum Empfänger durchlaufen, die Netze sind durch Router verbunden. Anhand von Routingtabellen, die jeder Router individuell pflegt, wird der Netzteil einem Zielnetz zugeordnet. Die Einträge in die Routingtabelle können dabei statisch oder über Routingprotokolle dynamisch erfolgen. Die Routingprotokolle dürfen dabei sogar auf IP aufsetzen.

Bei Überlastung eines Netzwerks oder einem anderen Fehler darf ein Router Pakete auch verwerfen. Pakete desselben Senders können bei Ausfall eines Netzes auch alternativ „geroutet“ werden. Jedes Paket wird dabei einzeln „geroutet“, was zu einer erhöhten Ausfallsicherheit führt.

Beim Routing über IP können daher

- einzelne Pakete verlorengehen,
- Pakete doppelt beim Empfänger ankommen,
- Pakete verschiedene Wege nehmen,
- Pakete fragmentiert beim Empfänger ankommen.

Wird TCP auf IP aufgesetzt (d. h. die Daten jedes IP-Pakets enthalten ein TCP-Paket, aufgeteilt in TCP-Header und Daten), so wird neben dem Aufheben der Längenbeschränkung auch der Paketverlust durch Wiederholung korrigiert. Doppelte Pakete werden erkannt und verworfen. Die Kombination TCP mit IP stellt dabei eine zuverlässige bidirektionale Verbindung eines Datenstroms dar.

Paketfragmentierung

Auf dem Weg vom Sender zum Empfänger kann es vorkommen, dass ein IP-Paket ein Netz durchlaufen muss, bei dem das Paket länger ist als die vom Netz maximal unterstützte Paketlänge (MTU). In einem solchen Fall kann der Router entweder eine Fehlermeldung zurücksenden oder das Paket in Fragmente aufteilen und in separaten IP-Paketen weiter versenden. Jedes der Fragmente trägt dieselbe Identifikationsnummer im Header, mit denen der Empfänger eine Zusammensetzung vornehmen kann. Die Fragmentierung erfolgt in folgenden Schritten:

- Aufteilen der Nutzdaten an einer 8-Byte-Grenze (das letzte Fragment enthält dann nicht unbedingt ein Vielfaches von 8 Byte Daten).
- Kopieren der IP-Headerdaten des Originalpakets in die neuen Header der Fragmente.
- Setzen des Felds „More Fragments“ auf den Wert 1 bei allen bis auf das letzte Fragment.
- Beim letzten Fragment wird der Wert von „More Fragments“ aus dem Originalpaket kopiert. Im Regelfall ist der Wert 0, kann aber auch 1 sein, falls das Originalpaket bereits ein Fragment ist.
- Setzen der Längen-Felder und des Fragment-Offsets in den Headern. Das Fragment-Offset gibt die Position eines Datenfragments im Originalpaket an (als Vielfaches von 8 Bytes).

Um ein Paket wieder zusammenzusetzen, kombiniert der Empfänger alle Fragmente, welche die gleiche Identifikationsnummer, den gleichen Absender, Empfänger und das gleiche Protokoll haben. Die Reihenfolge der Fragmente ergibt sich aus dem jeweiligen Fragment-Offset im Header. Das letzte Fragment erkennt der Empfänger daran, dass das Feld „More Fragments“ auf 0 gesetzt ist.

ICMP

IP ist eng verknüpft mit dem Internet Control Message Protocol (ICMP), das zur Fehlersuche und Steuerung eingesetzt wird. ICMP setzt auf IP auf, das heißt ein ICMP-Paket wird im Datenteil eines IP-Pakets abgelegt. Eine IP-Implementierung enthält stets auch eine ICMP-Implementierung. ICMP besteht aus verschiedenen Pakettypen, die unterschiedlichen Funktionen dienen. Ein prominentes Beispiel sind „Echo Request“ und „Echo Reply“, was für das Diagnosewerkzeug Ping verwendet wird. Auch Traceroute verwendet ICMP.

ICMP kann zusammen mit dem Don’t-Fragment-Bit des IP-Pakets auch eingesetzt werden, um die maximale Paketgröße eines Übertragungsweges zu einer Zieladresse zu ermitteln. Dies wird als Path MTU Discovery bezeichnet und ermittelt die kleinste MTU aller passierten Netze. Dadurch kann auf IP-Fragmentierung verzichtet werden, wenn der Sender nur Pakete mit der maximalen Größe der PMTU erzeugt.

Netzzugangsschicht

IPv4 kann auf verschiedene Übertragungsmedien und Protokolle in der Netzzugangsschicht aufsetzen, zum Beispiel das Point-to-Point Protocol oder Serial Line Internet Protocol. In lokalen Netzen wird überwiegend Ethernet oder WLAN eingesetzt. Beide verwenden eine 48 Bit lange MAC-Adresse zur Adressierung von Netzwerkkarten. Ein Sender muss die MAC-Adresse des Ziels kennen, bevor ein IP-Paket gesendet werden kann. Um für eine gegebene IP-Adresse des Ziels die zugehörige MAC-Adresse zu ermitteln, wird das Address Resolution Protocol (ARP) verwendet. Unbekannte MAC-Adressen fragt der Sender mittels einer ARP-Anfrage an, die er als Broadcast an alle Netzwerkgeräte im lokalen Netz sendet. Das Ziel sendet daraufhin eine ARP-Antwort zurück, die die gesuchte MAC-Adresse enthält. Die Kommunikationsteilnehmer speichern die gelernten Zuordnungen von IP-Adresse zu MAC-Adresse in einem Cache zwischen.

Adressknappheit

Aufgrund des unvorhergesehenen Wachstums des Internets herrscht heute Adressknappheit. Im Januar 2011 teilte die IANA der asiatisch-pazifischen Regional Internet Registry APNIC die letzten zwei /8-Adressblöcke nach der regulären Vergabepraxis zu. Gemäß einer Vereinbarung aus dem Jahr 2009 wurde am 3. Februar 2011 schließlich der verbliebene Adressraum gleichmäßig auf die regionalen Adressvergabestellen verteilt: jeweils ein /8-Adressblock pro Vergabestelle. Seitdem hat die IANA auf der globalen Ebene keine weiteren /8-Adressblöcke mehr zu vergeben.

Auf der regionalen Ebene verschärften die Regional Internet Registrys ihre Vergabepraktiken, um aus dem letzten /8-Adressblock möglichst lange schöpfen zu können. Bei der APNIC traten diese am 15. April 2011 in Kraft, da die zuvor erhaltenen beiden /8-Adressblöcke bereits nach drei Monaten aufgebraucht waren. Am 14. September 2012 folgte dann RIPE NCC mit der letzten regulären Zuteilung in der Region Europa/Naher Osten. Mit der neuen Vergabepraxis hatten APNIC- und RIPE-NCC-Mitglieder jeweils nur noch Anspruch auf Zuteilung eines /22-Adressbereichs, selbst wenn sie einen größeren Bedarf nachweisen konnten.

Am 25. November 2019 hat RIPE NCC ihren /8-Adressblock endgültig aufgebraucht. Seitdem werden nur noch /24-Kleinstblöcke per Warteliste aus Rückläufern vergeben.

Adressfragmentierung

Die historische Entwicklung des Internets wirft ein weiteres Problem auf: Durch die mit der Zeit mehrmals geänderte Vergabepraxis von Adressen des IPv4-Adressraums ist dieser inzwischen stark fragmentiert, d. h., häufig gehören mehrere nicht zusammenhängende Adressbereiche zur gleichen organisatorischen Instanz. Dies führt in Verbindung mit der heutigen Routingstrategie (Classless Inter-Domain Routing) zu langen Routingtabellen, auf welche Speicher und Prozessoren der Router im Kernbereich des Internets ausgelegt werden müssen. Zudem erfordert IPv4 von Routern, Prüfsummen jedes weitergeleiteten Pakets neu zu berechnen, was eine weitere Prozessorbelastung darstellt.

IPv6

Weil die IPv4-Adressen auszugehen drohten, wurde IPv6 als 128-Bit-Adressen entwickelt. Diese werden in acht hexadezimale 4er-Gruppen dargestellt und die Gruppen durch Doppelpunkte getrennt. Damit können 2128 = 65.5368 ≈ 340 Sextillionen IPv6-Adressen vergeben werden, eine extrem hohe Zahl. Zusätzlich wurde die Systematik der Adress-Struktur wesentlich verbessert. Verfügbar sind die Adressen seit 2017.

IPv6-Beispiel: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344

IPv6

IPv6 (Internet Protocol Version 6) ist eine IP-Protokollversion, die von der Internet Engineering Task Force (IETF) erarbeitet wurde. Diese Protokollversion soll das bisher verwendete IP-Protokoll Version 4 (IPv4) ablösen und stellt ein standardisiertes Verfahren zur Übertragung von Datenpaketen in Rechnernetzen dar. Zentrale Funktionen von IPv6 sind die Adressierung von Netzwerkelementen über sogenannte IPv6-Adressen sowie die Paketweiterleitung zwischen Teilnetzen (Routing). Einer der Hauptgründe für die Entwicklung von IPv6 ist die Knappheit an öffentlichen Internetadressen. IPv4 verwendet 32-Bit-Adressen. Daraus ergibt sich ein Adressraum mit ca. 4,3 Milliarden Adressen. IPv6 verwendet dahingegen IPv6-Adressen mit einer Länge von 128 Bit. Diese Adresslänge erlaubt eine unvorstellbare Menge von 2^ 128 oder 3,4 x 10^38 IPv6-Adressen.

Aufbau einer IPv6-Adresse

IPv6-Adressen bestehen aus 8 Blöcken zu 16 Bit mit jeweils vierstelligen hexadezimalen Zahlen. Diese Blöcke werden jeweils durch einen Doppelpunkt getrennt. Beispiel:

- 2001:0620:0000:0000:0211:24FF:FE80:C12C

Die vorderen 64-Bit werden für das Routing verwendet und bezeichnen das Netzwerkpräfix. Das Netzwerkpräfix kennzeichnet das Netzwerk, das Subnetz bzw. den Adressbereich. Die hinteren 64-Bit werden als Interface Identifier (IID) bezeichnet. Der Interface Identifier kennzeichnet einen Host in diesem Netz und wird aus der 48-Bit-MAC-Adresse des Interfaces gebildet und in eine 64-Bit-Adresse umgewandelt. Hierbei handelt es sich um das modifizierte EUI-64-Format. Somit ist das Interface unabhängig vom Netzwerkpräfix eindeutig identifizierbar.

Die von IPv4 bekannte Netz- bzw. Subnetzmaske fällt bei IPv6 ersatzlos weg. Um trotzdem eine Segmentierung durchführen zu können, wird die Präfixlänge definiert und mit einem "/" (Slash) an die eigentliche IPv6-Adresse angehängt. Beispiel:

Ein Subnetzwerk mit den IPv6-Adressen 2001:0820:9511:0000:0000:0000:0000:0000 bis 2001:0820:9511:FFFF:FFFF:FFFF:FFFF:FFFF kann mit der Notation 2001:0820:9511::/48 beschrieben werden.

Adresszuweisung

In der Regel bekommen Internetprovider (ISP) von der RIR /32-Netze zugeteilt, die diese wiederum in Subnetze gliedern. An Endkunden werden entweder /48-Netze oder /56-Netze vergeben.

Privacy Extensions

Eine IPv6-Adresse, die auf dem modifizierten EUI-64-Format beruht, lässt Rückschlüsse auf die zugrundeliegende MAC-Adresse zu. Da dies bei Nutzern Bedenken bezüglich des Datenschutzes hervorrufen könnte, wurde mit Privacy-Extensions ein Verfahren entwickelt, um den Hostanteil der IPv6-Adressen zu anonymisieren. Zu diesem Zweck hebt Privacy Extensions die Kopplung von Interface Identifier und MAC-Adresse auf und generiert temporäre Interface Identifier für ausgehende Verbindungen.

Notationsregeln

Weil IPv6-Adressen sehr lang sein können, werden sie in der Regel gekürzt. In RFC 5952 wurden diesbezüglich verbindliche Notationsregeln definiert. Diese beinhalten unter Anderem folgende Regeln:

- Führende Nullen innerhalb eines Blockes dürfen ausgelassen werden.
- Ein einzelner Block aus 4 Nullen wird zu einer Null zusammengefasst.
- Aufeinanderfolgende Blöcke deren Wert 0 bzw. 0000 beträgt, werden durch zwei Doppelpunkte ("::") gekürzt. Diese Kürzung darf jedoch nur einmal in einer Adresse vorgenommen werden, da sonst die Eindeutigkeit verloren geht. Beispiel:
  - Die Adresse 2001:0dc8:0:0:8d5:0:0:0 muss somit wie folgt gekürzt werden: 2001:0dc8:0:0:8d5:0:: oder 2001:0dc8:0::8d5:0:0:0
- Sind mehrere Null-Sequenzen in der Adresse enthalten, darf nur die am weitesten links stehende Sequenz ersetzt werden.

URL-Notation

In einer URL werden IPv6-Adressen in eckige Klammern eingeschlossen. Beispiel:

http://[2001:0db8:83a3:08d3::0380:7344]/

Portnummern müssen hinter der schließenden Klammer stehen. Diese werden mit einem Doppelpunkt abgetrennt.

http://[2001:0db8:83a3:08d3::0380:7344]:8080/

Das Prozentzeichen (%) wird weiterhin für die Kennzeichnung der hexadezimalen Zeichencodierung in URLs verwendet. Innerhalb der URL muss das Prozentzeichen durch seinen eigenen Hex-Code "%25" ersetzt werden (RFC 6874). Dies ist notwendig, wenn man die Verbindung über eine bestimmte Schnittstelle erzwingen will.

IPv6-Adresstypen

Wie bei IPv4 wurden auch bei IPv6 verschiedene Adressbereiche mit speziellen Aufgaben und Eigenschaften definiert. Diese wurden in RFC 4291 und RFC 5156 spezifiziert und lassen sich bereits durch die ersten Bits einer IPv6-Adresse, das sogenannte Formatpräfix, identifizieren.

Loopback-Addressen:

Die Adresse 0:0:0:0:0:0:0:1 (auch ::1/128) wird Loopback-Adresse genannt. Es handelt sich um die Adresse des eigenen Standorts.

Link-Local-Adressen:

Link-Local-Adressen sind nur innerhalb von lokalen Netzwerken gültig und beginnen mit dem Formatpräfix FE80::/10. Diese Adressen werden zur Adressierung von Elementen innerhalb eines lokalen Netzwerks sowie zur Autokonfiguration oder für die Neighbour-Discovery verwendet. In der Regel reicht der Geltungsbereich einer Link-Local-Adresse bis zum nächsten Router, sodass jedes an das Netzwerk angebundene Gerät in der Lage ist, mit diesem zu kommunizieren, um sich eine globale IPv6-Adresse zu generieren. Dieser Prozess wird Neighbor Discovery genannt.

Unique-Local-Adressen:

Für private lokale Netze wurden für das IPv6-Protokoll reservierte Adressbereiche definiert. Diese werden in RFC 4193 beschrieben und haben eine ähnliche Funktion wie die privaten Adressebereiche, die im IPv4-Protokoll festgelegt sind. Unique-Local-Adressen befinden sich im Adressbereich "fc00::/7" (fc00… bis fdff…) und werden nicht im Internet geroutet. Vielmehr sind sie nur inerhalb eines definierten Netzwerkbereichs gültig. Unterscheiden muss man zwischen dem Präfix "fc" und "fd", da diese unterschiedliche Bedeutungen haben. Während IPv6-Adressen mit dem Präfix fc vom Provider vergeben werden, können IPv6-Adressen mit dem Präfix fd im eigenen lokalen Netzwerk verwendet werden.

Global-Unicast Adressen:

Bei Global-Unicast-Adressen handelt es sich um weltweit einmalige Adressen, die weltweit geroutet werden. Diese werden von einem Netzwerkgerät benötigt, um eine Verbindung zum Internet aufzubauen. Ein Host kann mehrere dieser IPv6-Adressen besitzen. Diese werden vom Host mittels Autokonfiguration bezogen.

Multicast-Adressen:

Mit Multicast-Adressen kann man eine Eins-zu-viele-Kommunikation realisieren. Pakete, die an eine Multicast-Adresse gesendet werden, erreichen alle Netzwerkgeräte, die Teil der Multicast-Gruppe sind. Hierbei kann ein Gerät parallel mehreren Multicast-Gruppen angehören. Wird für ein Netzwerkgerät eine IPv6-Unicast-Adresse erstellt, wird dieses automatisch Mitglied von bestimmten Multicast-Gruppen, die für die Erkennung, Erreichbarkeit und Präfixermittlung benötigt werden. Multicast-Adressen sind durch das Präfix "ff::/8" gekennzeichnet. Danach folgen 4 Bit für Flags und weitere 4 Bit für die Angabe des Multicast Scopes.

Multicast-Adressen enden mit einer Nummer, die für eine Multicast-Gruppe steht. Eine Liste der Multicast-Gruppen finden Sie unter https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

Anycast-Adressen:

Adressen dieses Typs können an Gruppen von Empfängergeräten adressiert werden. Die Datenpakete werden hierbei nur an das Gerät gesendet, das dem Sender am nächsten ist. Anycast-Adressen kommen daher im Rahmen der Lastenverteilung und Ausfallsicherheit zum Einsatz.

IPv6-Paketformat

Das IPv6-Protokoll zeichnet sich durch ein vereinfachtes Paketformat aus. Der Header verfügt über eine feste Länge von 40 Bytes. Optionale Informationen werden in Extension Headers zwischen dem IPv6-Kopfdatenbereich und der eigentlichen Nutzlast ausgelagert. So können Optionen eingefügt werden, ohne dass sich der Header verändert. Zu den Informationen, die IPv6-Kopferweiterungen beinhalten können, zählen unter anderem Knoten-zu-Knoten-Optionen, Zieloptionen, Routing-Optionen sowie Optionen zu Fragmentierung, Authentifikation und Verschlüsselung. Weitere Informationen zum IPv6-Paketformat finden Sie in RFC 2460.

Stateless Address Autoconfiguration

Die Stateless Address Autoconfiguration (SLAAC) ist ein Verfahren zur zustandslosen und automatischen Konfiguration von IPv6-Adressen an einem Netzwerk-Interface. Mittels dieses Verfahrens kann ein Host vollautomatisch eine funktionsfähige Internetverbindung aufbauen. Stateless bedeutet in diesem Zusammenhang, dass die jeweilige IPv6-Adresse nicht zentral vergeben und gespeichert wird. Vielmehr erzeugt der Host zur initialen Kommunikation mit dem Router eine link-lokale IPv6-Adresse und weist sich diese zu. Mit dieser link-lokalen IPv6-Adresse kann ein Gerät mittels des Neighbour Discovery Protocols (NDP) nach den Routern in seinem Netzwerksegment suchen. Dies geschieht durch eine Anfrage an die Multicast-Adresse, über die alle Router eines Segments erreichbar sind.

Nach dem Erhalt einer solchen Anfrage versendet ein Router Informationen zu verfügbaren Präfixen. Um die doppelte Vergabe von IPv6-Adressen zu vermeiden, führt der Host bei einer neu generierten IPv6-Adresse eine Duplicate Address Detection (DAD) durch. Dazu schickt der Host eine Anfrage an die generierte Adresse ins lokale Netz. Als Antwort-Adresse dient eine Multicast-Adresse. Wenn eine andere Station die IPv6-Adresse bereits nutzt, kommt eine Antwort zurück. Wenn keine Antwort von dieser Adresse zurückkommt, verwendet der Host die IPv6-Adresse für die Kommunikation.

*N*eighbour Discovery Protocol

Das Neighbour Discovery Protocol (NDP) ist ein IPv6-Protokoll. Es wird unter anderem verwendet, um IPv6-Adressen in Link-Layer-Adressen (MAC-Adressen) aufzulösen. Darüber hinaus wird es zum Aktualisieren der gecachten Adressen verwendet. Wenn sich ein Knoten nicht im gleichen Netzwerk befindet, wird NDP verwendet, um einen Router zu finden, der die Pakete weiterleiten kann. Ferner erfüllt dieses Protokoll unter anderem noch folgende Aufgaben:

- Parameterermittlung
- Stateless Address Autoconfiguration
- Adressauflösung (Address Resolution mit Neighbor Discovery)
- Erkennung der Nichterreichbarkeit des Nachbarn (Neighbor Unreachability Detection, NUD)
- Erkennung doppelter Adressen (Duplicate Address Detection, DAD)
- Umleitung (Redirect)

DHCP6

DHCP ist ein Protokoll, das für die Verwaltung der IP-Konfiguration in einem TCP/IP-Netzwerk verwendet wird. Dieses ermöglicht es, angeschlossene Clients ohne manuelle Konfiguration der Netzwerkschnittstelle in ein bestehendes Netzwerk einzubinden. In einem IPv6-Netzwerk wird DHCP6 eigentlich nicht benötigt, da diese Aufgabe durch die Stateless Address Autoconfiguration (SLAAC) übernommen wird. Es können jedoch gute Gründe für die Verwendung von DHCP6 sprechen. Dies trifft z. B. zu, wenn der IPv6-Client die Optionen der IP-Konfiguration nicht mittels Stateless Address

Autoconfiguration entgegen nehmen kann. In diesem Fall können mittels Stateless Address Autoconfiguration die IP-Adresse und mittels DHCP6 die restlichen Konfigurationsparameter zugeteilt werden.

Mac-Adressen

Die MAC-Adresse (Media-Access-Control-Adresse, auch Media-Access-Code-Adresse) ist die Nummer eines Gerätes auf einer Datenverbindung. Anhand dieser Nummer werden über die Verbindung laufende Daten den Geräten zugeordnet.

Die MAC-Adresse ist die Hardware-Adresse jedes einzelnen Netzadapters, die als eindeutiger Identifikator des Geräts in einem Rechnernetz dient. Man spricht auch von physischer Adresse oder Geräteadresse. Bei Apple wird sie auch Ethernet-ID, Airport-ID oder Wi-Fi-Adresse genannt.

Einzelheiten

Medium

Die in Rechnernetzen verwendeten Übertragungsmedien sind üblicherweise Kupferkabel (Twisted-Pair-Kabel), Lichtwellenleiter und Funk (WLAN). Über das Übertragungsmedium werden in der Bitübertragungsschicht Bitsequenzen gesendet, die in der nächsthöheren Schicht (Sicherungsschicht) zu Frames zusammengefügt werden. Zur eindeutigen Adressierung von Rechnern auf der Leitungsschicht dient die MAC-Adresse. Jede Ethernet-, WLAN- oder Bluetooth-Netzwerkkarte besitzt solch eine eindeutige MAC-Adresse, unter der sie angesprochen werden kann. Obwohl sie effektiv nur in lokalen Netzen eine Bedeutung haben, sind MAC-Adressen üblicherweise global eindeutig und besitzen keinerlei Strukturmerkmale, die für die Wegewahl (Routing) genutzt werden können.

Physische Adresse

Die MAC-Adresse wird auch als physische Adresse bezeichnet, weil er teilweise vom Hersteller in ein Gerät fest und nicht veränderbar einprogrammiert ist. Sofern Betriebssystem und Hardware dies unterstützen, kann die MAC-Adresse jedoch auch von dem Benutzer geändert werden. Dazu wird seit 2020 auf die Randomisierung von MAC-Adressen gesetzt, wie das seit Android 10 oder iOS 14 standardmäßig der Fall ist. Damit soll ein Nachverfolgen von Nutzern verhindert werden, da dies ein Datenschutzrisiko darstellt.

Zugriffssteuerung (Access Control)

Zugriff vom Medium (Media Access Control)

Auf einem Funkkanal oder einem Koaxialkabel sind die Daten mehrerer Geräte unterwegs, die für verschiedene Empfänger bestimmt sind. Anhand der MAC-Adresse sucht der Empfänger die Daten heraus, die für das eigene Gerät bestimmt sind. Dazu beginnt jedes Datenpaket mit der MAC-Adresse des Empfängers. Passt die MAC-Adresse nicht, wird das Datenpaket nicht verarbeitet.

Da die MAC-Adresse vom Hersteller in die Schaltung eingebaut wurde, ist die Schaltung unmittelbar nach dem Einschalten des Stromes betriebsbereit. Das Lesen des Mediums verbraucht keine Rechenzeit. Während der Übertragung von Datenpaketen mit unpassender MAC-Adresse können Teile des Empfängers abgeschaltet werden, um Strom zu sparen.

Bei Ethernet, WLAN und ähnlichen Netzwerktechnologien steuert die MAC-Adresse nicht den schreibenden (sendenden) Zugriff auf das Medium.

Zugriff auf das Netzwerk (Network Access Control)

Die MAC-Adresse kann benutzt werden, um Geräte zu identifizieren und den Zugriff auf ein Netz zu steuern.

Jugendschutz: Im Heimnetz kann den Geräten der Kinder nachts der Zugriff auf das Netz entzogen werden.

Spionageschutz: Im Unternehmen kann Geräten mit unbekannter MAC-Adresse der Zugriff auf das Firmennetz verweigert werden.

Gastnetze: Sowohl im Heim als auch im Unternehmen können fremde Geräte mit speziellen Gastnetzen verbunden werden.

Ein Zugriffsschutz anhand der MAC-Adresse ist begrenzt. Der Zugriff auf das (Funk-)Medium wird nicht unterbunden. So können die im Heimnetz ausgesperrten Kinder u. U. das Netz eines Nachbarn benutzen.

Wenn ein Gerät die Änderung der MAC-Adresse erlaubt, können Sperren umgangen werden.

Um die Anonymität eines Gerätes zu verbessern, benutzen manche Geräte eine MAC-Adresse, die vollständig oder zum Teil aus Zufallszahlen besteht und gelegentlich gewechselt wird. Damit ist die Identifikation eines Gerätes anhand der MAC-Adresse nicht mehr gegeben. Nach dem Wechsel der MAC-Adresse muss das Gerät in den Netzwerken, die nur bekannte Geräte bedienen, erneut bekannt gemacht werden.

Code

In einer MAC-Adresse sind folgende Angaben kodiert:

- Ist die Adresse eindeutig einem Gerät zugeordnet oder betrifft sie mehrere Geräte (Multicast, Broadcast), siehe unten Empfängergruppe
- Ist die Adresse weltweit eindeutig koordiniert oder wurde sie unkoordiniert vergeben, siehe unten Vergabestelle
- Bei den koordinierten Adressen ist der Hersteller enthalten, siehe unten Herstellerkennungen
- Der Hersteller kann in der MAC-Adresse die Seriennummer des Gerätes einbringen

Funktion im Netzwerk

Die MAC-Adresse wird der Sicherungsschicht (Schicht 2) des OSI-Modells zugeordnet; im vom IEEE erweiterten OSI-Modell wird sie der Unterschicht Media Access Control (Schicht 2a) zugeordnet. Um die Sicherungsschicht mit der nächsthöheren Schicht, der Vermittlungsschicht, zu verbinden, wird z. B. bei Ethernet das Address Resolution Protocol im Rahmen von IPv4 verwendet. Im IPv6 übernimmt ein neues Protokoll diese Funktion, das Neighbor Discovery Protocol (NDP).

Netzwerkgeräte brauchen dann eine MAC-Adresse, wenn sie auf Schicht 2 explizit adressiert werden sollen, um Dienste auf höheren Schichten anzubieten; leitet das Gerät dagegen wie ein Repeater oder Hub die Netzwerkpakete nur weiter, so ist es auf der Sicherungsschicht nicht sichtbar und braucht folglich keine MAC-Adresse.

Bridges und Switches untersuchen zwar die Pakete der Sicherungsschicht, um das Netzwerk in mehrere Kollisionsdomänen aufzuteilen, nehmen aber selbst nicht aktiv an der Kommunikation teil, brauchen also für diese Basisfunktionen ebenfalls keine MAC-Adresse. Ein Switch benötigt jedoch eine MAC-Adresse, wenn er selbst über das Rechnernetz administriert wird oder Monitoring-Dienste anbietet (z. B. über

Telnet, SNMP oder HTTP). Eine MAC-Adresse wird ebenfalls benötigt, wenn Bridges oder Switches den Spanning-Tree-Algorithmus zur Vermeidung von Schleifen in redundant ausgelegten Rechnernetzen verwenden.

Form (Syntax)

Im Falle von Ethernet-Netzen besteht die MAC-Adresse aus 48 Bit bzw. sechs Bytes. Die Adressen werden in der Regel hexadezimal geschrieben.

Üblich ist dabei eine byteweise Schreibweise, wobei die einzelnen Bytes durch Bindestriche oder Doppelpunkte voneinander getrennt werden, z. B.

- 00-80-41-ae-fd-7e
- 008041-aefd7e oder
- 00:80:41:ae:fd:7e.

Seltener zu finden sind Angaben wie

- 008041aefd7e oder
- 0080.41ae.fd7e.

Die Reihenfolge der Zeichen ist allerdings nicht bei allen Anwendungen gleich. Man unterscheidet hier zwischen der kanonischen und der „Bit-reversed“-Darstellung. Die kanonische Form wird für Darstellungen bevorzugt.

Kanonische Darstellung

Die übliche Darstellung von MAC-Adressen, wie sie beispielsweise in der Ausgabe von ipconfig/ifconfig erscheint, wird auch als kanonisches Format („canonical form“, „LSB format“ bzw. „Ethernet format“) bezeichnet. Es gibt die Reihenfolge an, in der die Adresse in IEEE 802.3 (Ethernet) und IEEE 802.4 (Token Bus) übertragen wird. Hier startet die Übertragung mit dem niederwertigsten Bit (Least Significant Bit, LSB) eines Oktetts (Ausnahme ist die Frame Check Sequence, FCS).

Bit-reversed-Darstellung

IEEE 802.5 (Token Ring) und IEEE 802.6 starten die Übertragung mit dem höchstwertigen Bit (MSB, most significant bit). Dies kann leicht zu Missverständnissen führen, wenn nicht angegeben wird, ob von der kanonischen Darstellung in normaler Bytedarstellung oder von der umgekehrten Bitübertragungsdarstellung die Rede ist. Eine Adresse, deren kanonische Form beispielsweise 12-34-56-78-9A-BC ist, wird bei der Übertragung mit LSB zuerst (heißt: von rechts nach links gelesen) auf der Leitung in Form der

Bitfolge 01001000 00101100 01101010 00011110 01011001 00111101 übertragen.

In Token-Ring-Netzwerken (MSB zuerst, heißt: von links nach rechts gelesen, also natürlichsprachlich) würde die Übertragung in Form der

Bitfolge 00010010 00110100 01010110 01111000 10011010 10111100 stattfinden.

Wenn dies bei der Umsetzung der Bitfolgen in die kanonische Darstellung nicht konsistent beachtet wird, kann z. B. die letztere Darstellung fälschlicherweise als 48-2C-6A-1E-59-3D (LSB zuerst) interpretiert werden.

Die Darstellung in Token-Ring-Netzwerken wird dann aber als „Bit-reversed order“, „Non-canonical form“, „MSB format“, „IBM format“, oder „Token Ring format“ wie in RFC 2469 aufgeführt bezeichnet.

Funktion

In jedem Frame nach Ethernet-II-Variante wird vor dem Typfeld und den Daten zunächst die MAC-Adresse des Empfängers und des Senders übertragen. Empfänger und Sender müssen Teil des Local Area Networks (LAN) sein. Soll ein Paket in ein anderes Netz geschickt werden, wird es auf Ethernet-Ebene zunächst an einen Router geschickt. Dieser analysiert die Daten auf der untergeordneten Schicht und vermittelt das Paket dann weiter. Er erzeugt dazu einen neuen Ethernet-Frame, wenn es sich bei dem Nachbarnetz ebenfalls um ein Ethernet handelt. Dazu ersetzt ein Router die MAC-Adressen, d. h. wenn Router R1 ein Ethernet-Frame empfängt und es an den Router R2 weitergeben soll, ersetzt R1 die Quelladresse mit seiner eigenen MAC-Adresse und die Zieladresse mit der Mac-Adresse von R2.

Pseudo-Empfänger „Broadcast-Adresse“

Die MAC-Adresse, bei der alle 48 Bits auf 1 gesetzt sind (ff-ff-ff-ff-ff-ff), wird als Broadcast-Adresse verwendet, die an alle Geräte in einem LAN gesendet wird. Broadcast-Frames werden ohne besondere Maßnahmen nicht in ein anderes LAN übertragen.

Besondere Kennungen

Empfängergruppe

Das niederwertigste Bit (engl. Least Significant Bit, LSB) des ersten Bytes (Bit 0) einer MAC-Adresse gibt an, ob es sich um eine Einzeladresse oder Gruppenadresse (I/G für Individual/Group) handelt. Bei einem Broadcast oder Multicast wird I/G = 1 gesetzt, sonst und bei Quelladressen ist I/G = 0.

Kurz: I/G ist

- 0 für I (Individual) oder
- 1 für G (Group).

Die meisten Protokolle, welche auf OSI Layer 2 arbeiten, haben besondere MAC-Adressen, sogenannte MAC-Multicast-Adressen. Das VLAN Trunking Protocol beispielsweise verwendet die Adresse 01-00-0C-CC-CC-CC. Dadurch ist ein Frame an alle Switches gleichzeitig adressiert. Es gibt auch ganze Gruppen von MAC-Multicast-Adressen: Das TRILL-Protokoll beispielsweise verwendet unter anderem 01-80-C2-00-00-00 bis 01-80-C2-00-00-0F. Auch andere Protokolle besitzen besondere, fest zugewiesene, MAC-Adressen.

Vergabestelle

Das folgende 2. Bit (Bit 1, genannt U/L für Universal/Local) zeigt an, ob die MAC-Adresse global eindeutig ist (Universally Administered Address (UAA); U/L = 0) oder lokal administriert wird und nur dort eindeutig ist (Locally Administered Address (LAA); U/L = 1).

Kurz: U/L ist

- 0 für U (Universal) oder
- 1 für L (Local).

Die folgenden Adressbereiche sind lokal und können z. B. für virtuelle Maschinen verwendet werden:

x2:xx:xx:xx:xx:xx

x6:xx:xx:xx:xx:xx

xA:xx:xx:xx:xx:xx

xE:xx:xx:xx:xx:xx

Herstellerkennungen

In den nächsten 22 Bits (Bit 2 bis 23) wird eine von der IEEE vergebene Herstellerkennung (auch OUI – Organizationally Unique Identifier genannt) beschrieben, die weitgehend in einer Datenbank einsehbar sind. Die verbleibenden 24 Bits (Bit 24 bis 47) werden vom jeweiligen Hersteller für jede Schnittstelle individuell festgelegt. Compaq zum Beispiel hat eine OUI mit der Adresse 00-50-8b. Innerhalb dieser OUI darf Compaq alle verfügbaren Adressen verwenden, also 00-50-8b-xx-xx-xx. Es ergeben sich 224 = 16777216 (16,8 Millionen) individuelle Adressen.

Neben der OUI existieren zwei kleinere Adressbereiche:

- ein OUI-28, oder MAC Address Block Medium (MA-M), bestehend aus 28 Bits
- ein OUI-36, oder MAC Address Block Small (MA-S), bestehend aus 36 Bits

Diese sind für Privatpersonen und kleinere Firmen und Organisationen vorgesehen, die nicht so viele Adressen benötigen. Die OUI-36 Adresse beginnt mit 36 Bits, die für eine Organisation vergeben werden. Damit verbleibt der Adressbereich innerhalb der Bits 11 bis 0 nutzbar, wodurch 212 = 4096 individuelle Adressen möglich sind. Die MA-M werden durch 28 Bits eindeutig gekennzeichnet und ergeben mit den restlichen 20 Bits: 220 = 1.048.576 individuelle Adressen nach EUI-48. Mehr Geräte können adressiert werden, wenn EUI-64 verwendet wird.

Die Adressen der Schnittstellen jedes netzwerkfähigen Geräts sollten theoretisch weltweit eindeutig vorbelegt sein (es sind aber schon Einzelfälle bekannt geworden, bei denen zwei Netzwerkkarten im selben Netzwerk identische MAC-Adressen besaßen, was zu zunächst völlig unerklärlichen Fehlern führte). Dies kann zur automatischen Konfiguration von Geräten eingesetzt werden und wird von Protokollen wie RARP, BOOTP und DHCP genutzt. Die Software unterstützt es jedoch auch häufig, jeden beliebigen Wert als MAC-Adresse verwenden zu können. Dies wird zum Beispiel bei Backup-Systemen genutzt, wo Ersatzgeräte die MAC-Adresse eines ausgefallenen Geräts übernehmen können.

Manche Software verwendet die MAC-Adresse der ersten Netzwerkkarte zur Identifikation des Rechners, auf dem lizenzierte Programme ausgeführt werden dürfen. Auch die Berechnung einer universellen Identifikation (UUID oder GUID) verwendet neben anderen Teilen diese MAC-Adresse. Da die MAC-Adresse geändert werden kann, raten Sicherheitsexperten allerdings davon ab, die MAC-Adresse als alleiniges Authentifizierungskriterium zu verwenden.

Herstellerunabhängige Kennungen

Neben der Broadcast-Adresse FF-FF-FF-FF-FF-FF, die alle Geräte in einem lokalen Netzwerk adressiert, werden für IPv4-Multicast MAC-Adressen im Bereich 01-00-5e-00-00-00 bis 01-00-5e-7f-ff-ff verwendet. Dabei werden dann die unteren 23 Bit der IP-Multicast-Adresse direkt auf die untersten 23 Bit der MAC-Adresse abgebildet. Der IP-Multicast-Adresse 224.0.0.1 ist somit die Multicast-MAC-Adresse 01-00-5e-00-00-01 fest zugeordnet.

Neben den obersten vier Bit, die bei IPv4-Multicast-Adresse stets 1110 sind, verbleiben 5 Bits der IP-Adresse, die nicht in der MAC-Multicast-Adresse abgebildet werden können. Dadurch ist es möglich, dass ein Host MAC-Multicast-Pakete einer Multicast-Gruppe empfängt, zu der er nicht gehört. Diese Pakete werden dann von der IP-Schicht verworfen, da dort die Erkennung auf Basis der IP-Multicast-Adresse möglich ist.

Für IPv6-Multicast wurde der MAC-Adressbereich 33-33-xx-xx-xx-xx reserviert. Dabei werden die untersten 32 Bit der IPv6-Multicast-Adresse in die MAC-Adresse eingebettet.

Für hochverfügbare logische Router nach VRRP ist die herstellerunabhängige Kennung 00-00-5E-00-01-ID (im Bereich 00-00-5E) reserviert, wobei das letzte Byte ID für die Kennung des virtuellen Routers steht. Sie bleibt gleich, selbst wenn ein anderer Router den Dienst übernimmt.

Stolperfalle: Kennzeichnung „PRIVATE“

Die Herstellerkennungen, die – wie zum Beispiel AC-DE-48 – in der OUI-Datenbank als „PRIVATE“ gekennzeichnet wurden, sind für Firmen registriert, die ihre Identität nicht öffentlich preisgeben wollen. Adressen aus diesen Bereichen können daher nicht, wie man vermuten würde, für lokale Zwecke eingesetzt werden. (Für lokale Zwecke wird das unter „Vergabestelle“ beschriebene „U/L address bit“ verwendet.)