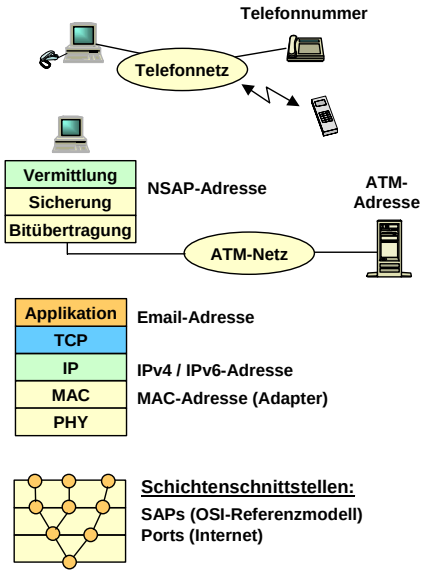
## 1.4 Grundlagen: Nummerierung und Adressierung

Version: Jan. 2003

**Inhalt**

- Nummerierung im Telefonnetz und ISDN (Integrated Services Digital Network)
- Adressierung zwischen Protokollschichten mit SAPs (Service Access Point) oder Ports
- Adressierung in OSI-Systemen
- Adressierung in ATM (Asynchronous Transfer Mode)
- Adressierung in IEEE LANs
- Adressierung im Internet (IPv4, IPv6)
- Adressierung im Internet (Email-Adresse, Adressauflösung, DNS, URL)

| | |
|---|---|
| POTS | Telefonnetz |
| ISDN | Integrated Services Digital Network |
| NSAP | Network Service Access Point |
| ATM | Asynchronous Transfer Mode |
| Email | Electronic Mail |
| IPv4 | Internet Protocol Version 4 |
| IPv6 | Internet Protocol Version 6 |
| IEEE MAC | IEEE Medium Access Control |
| Identifier | interne Netzadressierung |
| SAP | Service Access Point (Protokoll-Pfade) |




Der Aufbau von Kommunikationsbeziehungen erfolgt über Adressen, die der Lokalisierung von Endeinrichtungen, Teilnehmern oder Netzinstanzen dienen. Nummerierung und Adressierung hängen eng mit der Netzstruktur zusammen. Im folgenden wird in die Definition und Prinzipien von Nummerierung und Adressierung eingeführt.

1. Namensgebung,
2. Nummerierung,
3. Adressierung,
4. Labels.

### 1. Namensgebung

Ein Name ist eine ortsunabhängige Kennung für Instanzen oder Einrichtungen eines Nachrichtennetzes. Der Bereich, innerhalb dessen Namen in eindeutiger Weise festgelegt sind, heißt Namensraum (name space). Die Gesamtheit der vergebenen Namen kann in einem Namenserver (name server) gespeichert sein, der der Netzverwaltung dient.

Namen sind i.a. aus alphanumerischen Zeichen aufgebaut. Verwandt mit dem Namensbegriff ist der Begriff „Kennung“ (identifier). Je nach Anwendung werden unterschieden

Teilnehmerkennung (subscriber identity)
Gerätekennung (equipment identity)

### 2. Nummerierung

Die Nummerierung ist die wohl bekannteste Art, Teilnehmerendeinrichtungen oder Netze zu kennzeichnen. Die Nummerierung (numbering) verwendet dazu in der Regel Ziffernfolgen, gegebenenfalls ergänzt durch wenige Sonderzeichen (wie z.B. bei Tastwahl-Telefonen). Die Festlegung der Nummerierung erfolgt in einem Nummerierungsplan (numbering plan). Es werden verschiedene Arten von Nummerierungsprinzipien unterschieden:

**Netzgebundene/Freie Nummerierung**

- Bei der **netzgebundenen Nummerierung** richtet sich die Nummernvergabe nach der Netzstruktur; bei freier Nummerierung kann die Vergabe von Nummern ohne Rücksicht auf Netzstruktur oder Teilnehmerlage erfolgen.
- **Hierarchische/Nichthierarchische Nummerierung.** Bei der hierarchischen Nummerierung lehnt sich die Nummernvergabe an die Netzhierarchie.
- **Nummerierungsbereich.** Der Nummerierungsbereich (numbering area) ist der Bereich eines Nachrichtennetzes, innerhalb dessen die Nummerierung eindeutig ist.
- **Kennzahl.** Unter einer Kennzahl (Code) wird die Kennzeichnung eines Netzknotens, eines Nummerierungsbereiches, eines nationalen Netzes oder eines Dienstes verstanden.

Die Rufnummer (number) ist die Ziffernfolge zur Kennzeichnung eines Teilnehmeranschlusses.

| | | |
|---|---|---|
| Teilnehmerrufnummer | subscriber number | innerhalb eines Nummerierungsbereichs |
| Nationale Rufnummer | national number | innerhalb eines Landesnetzes |
| Internationale Rufnummer | international number | innerhalb des weltweiten Netzes |
| Durchwahlrufnummer | direct dialling-in number | Teilnehmerrufnummer einer Nebenstelle |

**3. Adressierung**

Unter Adressierung (addressing) wird allgemein die Kennzeichnung von Instanzen innerhalb eines Kommunikationsnetzes mittels einer Adresse verstanden. Die Adresse besteht im allgemeinen aus alphanumerischen Zeichen und folgt einem allgemeingültigen Adressierungsschema innerhalb eines Adressierungsbereichs.

**Hierarchische/Flache Adressierung**

Die hierarchische Adressierung folgt nach einem baumförmig strukturierten Adressraum, der sich an der Netzstruktur orientieren kann. Bei flacher Adressierung erfolgt eine (weltweit) eindeutige Adressierung nach einem einstufigen Schema.

**Spezielle Adressierungen**

Die Adressierung kann sich auf unterschiedliche Kriterien beziehen wie
- Anschlussbezogene Adressierung (subscriber line addressing)
- Benutzerbezogene Adressierung (user addressing)
- Endgerätebezogene Adressierung (equipment addressing)
- Symbolische Adressierung (symbolic addressing)
- Unteradressierung (subaddressing)

Adressen sind (numerische) Werte, die einen Knoten in einem Netz eindeutig bestimmen. Je nach OSI-Schicht existieren verschiedene Typen von Adressen. **Namen** sind (logische) Werte, die an Stelle einer numerischen Adresse verwendet werden können. Adressen entsprechen Telefonnummern, Namen entsprechen dem Eigen- oder Firmennamen des Inhabers der Telefonnummer. Die Abbildung von Namen auf Adressen wird durch **Namensdienste** bzw. **Verzeichnisdienste** geleistet, die somit einem Telefonbuch entsprechen.

Adressen lassen sich abhängig von ihrem Typ einer Schicht des OSI-Modells zuordnen. OSI selbst ordnet den Schichten 3-6 Adressen zu, die als SAP (Service Access Point) in Verbindung mit der jeweiligen Schicht benannt sind:
- PSAP: Presentation SAP auf Schicht 6.
- SSAP: Session SAP auf Schicht 5.
- TSAP: Transport SAP auf Schicht 4.
- NSAP: Network-SAP auf Schicht 3.

NSAP ist die netzweit eindeutige Adresse eines Knotens; TSAP, SSAP und PSAP sind Selektoren. Sie geben an, welcher Anwendungsprozess gerade die genannte Schicht nutzt. Die gesamte Adresse eines Anwendungsprozesses ergibt sich also aus der Aneinanderreihung der einzelnen Adressen zu PSAP + SSAP + TSAP + NSAP.

Meistens stellt eine Adresse eine **Individualadresse** dar. Sie identifiziert also genau einen Teilnehmer. Weiter gibt es **Gruppenadressen** (für Multicast) und **Broadcast-Adressen** (für die Adressierung aller Teilnehmer in einem Netz). Ein Adressraum ist die Gesamtheit aller Adressen in einem Netz.

Adressen können **lokal** sein, sie sind dann nur innerhalb eines Teilnetzes (Subnetzes) eindeutig. **Globale Adressen** sind in einem gesamten Netz eindeutig. Adressräume können flach oder hierarchisch strukturiert sein. Bei **flachen Adressräumen** besteht kein Zusammenhang zwischen der Adresse und der geografischen Lage (Position) einer Station. **Hierarchische Adressen** bestehen aus einzelnen Teilen, die einem hierarchischen Aufbau eines Netzes entsprechen. Dann haben benachbarte Stationen weitgehend benachbarte Adressen. Von den nachfolgend behandelten Adressen sind MAC-Adressen flach, aber global (zumindest für U/L = 0); IP-, OSI-, ATM- und X. 121 -Adressen sind hierarchisch und global.

**4. Labels**

In dem oben behandelten Adressierungsschema bezeichnen die Adressen ein Endsystem (global oder lokal) eindeutig. Bei verbindungsloser Kommunikation muss jedes Paket (jede N-PDU) mit einer Zieladresse versehen sein. In verbindungsorientierten Netzen ist diese Forderung nach abgeschlossenem Verbindungsaufbau nicht mehr notwendig. Stattdessen können sich die Zwischensysteme (Router) darauf beschränken, für jede bestehende Verbindung logische Kanalnummern zu verwenden. Diese Nummern werden als **Labels** bezeichnet, sie sind nur lokal für jeweils eine Teilstrecke gültig (global gültige Labels wären nicht handhabbar und zu lang). Dabei muss das Zwischensystem lediglich die logische Nummer des Eingangskanals auf die des Ausgangskanals abbilden. Eine Verbindung zwischen zwei Endsystemen ist demnach eine Folge von Teilstrecken, von denen jede mit einem Label versehen ist. Eine solche Verbindung wird als **virtuelle oder logische Verbindung**

bezeichnet. Da lokale Labels kürzer sind als globale Adressen, wird die NPDU durch die Verwendung von Labels kürzer. Labels werden in unterschiedlichen Netzen verwendet.

Einige Labels und ihre Anwendung

| Bezeichnung | Verwendung |
|---|---|
| LCN: Logical Channel Number | X.25 |
| DLCI: Data Link Connection Identifier | Frame Relay |
| VPI/VCI: Virtual Channel Identifier/Virtual Path Identifier | ATM |

# Nummerierung im Telefonnetz und ISDN (Integrated Services Digital Network)

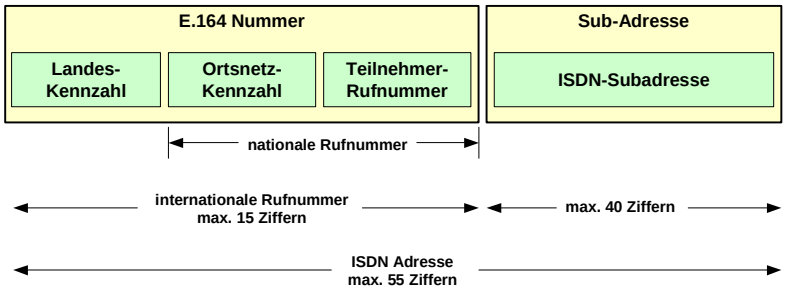



Bild: ISDN Adressstruktur nach E.164

**Spezielle Formen der Kennzahlen sind:**

- Landeskennzahl (country code)
  z.B. Österreich: 43, Frankreich: 33
- Ortsnetzkennzahl (area code)
  z.B. Wien: 1, Graz: 316,
  Bad Gleichenberg: 3159

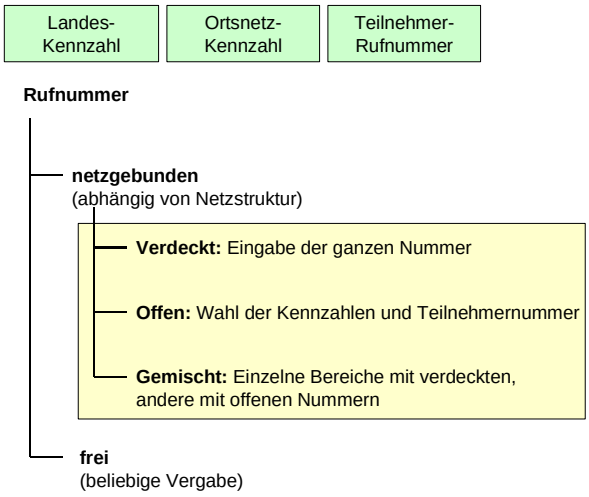



Bild: Rufnummernsysteme in der Telefonie

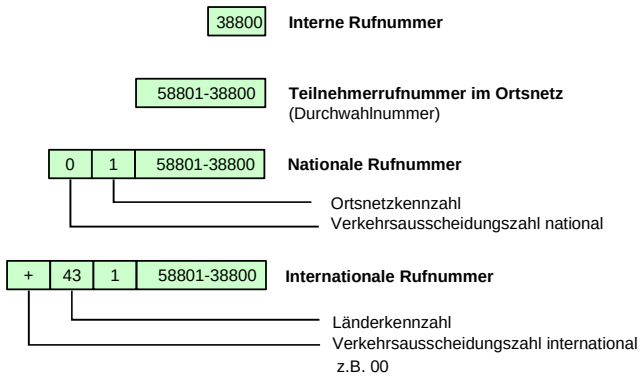



Bild: Telefonnetz - Offene Nummerierung

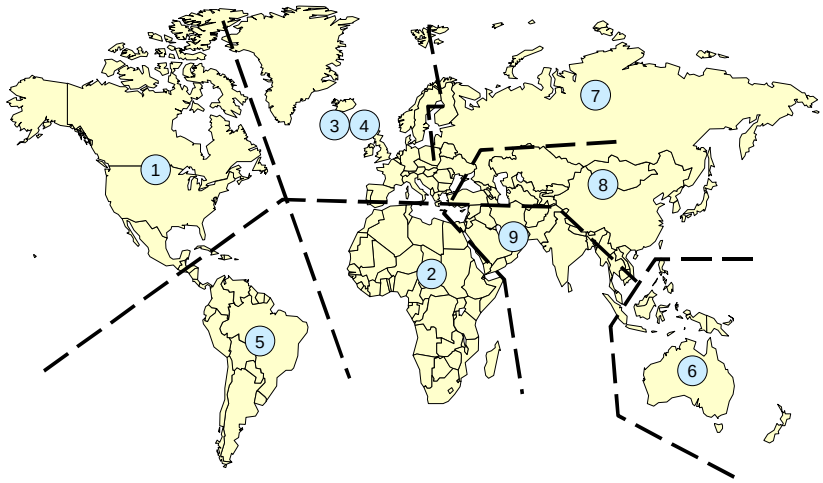



Bild: Internationaler Nummerierungsplan

Der erste Ziffer der Vorwahlnummer bestimmt die kontinentalen Bereiche des Nummerierungsplans nach E.164.

1: Nordamerika
2: Afrika
3: Europa
4: Europa
5: Süd-Amerika
6: Ozeanien
7: Russland
8: Asien
9: Mittelost


Bild: Nordamerikanischer Nummerierungsplan (Vorwahl 001)

**Bei freier Nummerierung** existiert für den Vorwahlnummer kein Zusammenhang bezüglich der geographischen Lage des Teilnehmers.

Anwendung: Nord-Amerika.

**Afrika 002**

| | |
|---|---|
| Ägypten | 20 |
| Algerien | 213 |
| Angola | 244 |
| Äthiopien | 251 |
| Benin | 229 |
| Botsuana | 267 |
| Burundi | 257 |
| Ivorküste | 225 |
| Dschibuti | 253 |
| Eritrea | 291 |
| Gabun | 241 |
| Gambia | 220 |
| Ghana | 233 |
| Guinea | 224 |
| Kamerun | 237 |
| Kap Verde | 238 |
| Kenia | 254 |
| Kongo | 242 |
| Liberia | 231 |
| Libyen | 218 |
| Malawi | 265 |
| Mauritius | 230 |
| Mosambik | 258 |
| Namibia | 264 |
| Niger | 227 |
| Nigeria | 234 |
| Ruanda | 250 |
| Sambia | 260 |
| Senegal | 221 |
| Simbabwe | 263 |
| Somalia | 252 |
| Sudan | 249 |
| Südafrika | 27 |
| Swasiland | 268 |
| Tunesien | 216 |
| Tschad | 235 |
| Uganda | 256 |

**Europa 003 / 004**

| | |
|---|---|
| Albanien | 355 |
| Andora | 376 |
| Armenien | 374 |
| Belarus | 375 |
| Belgien | 32 |
| Bosnien | 387 |
| Bulgarien | 359 |
| Dänemark | 45 |
| Deutschland | 49 |
| Finnland | 358 |
| Frankreich | 33 |
| Gibraltar | 350 |
| Griechenland | 30 |
| UK | 44 |
| Irland | 353 |
| Island | 354 |
| Italien | 39 |
| Jugoslawien | 381 |
| Kroatien | 365 |
| Lettland | 371 |
| Litauen | 370 |
| Luxemburg | 352 |
| Malta | 356 |
| Moldau | 373 |
| Monaco | 377 |
| Niederlande | 33 |
| Norwegen | 47 |
| Österreich | 43 |
| Polen | 48 |
| Portugal | 351 |
| Rumänien | 40 |
| Schweden | 46 |
| Schweiz | 41 |
| Slowakei | 421 |
| Slowenien | 386 |
| Spanien | 34 |
| Tschechien | 429 |
| Ukraine | 380 |
| Ungarn | 36 |
| Vatikan | 39 |
| Zypern | 357 |

**Süd-Amerika 005**

| | |
|---|---|
| Argentinien | 54 |
| Brasilien | 55 |
| Bolivien | 591 |
| Chile | 56 |
| Costa Rica | 506 |
| Ecuador | 593 |
| El Salvador | 503 |
| Guayana | 592 |
| Haiti | 509 |
| Honduras | 504 |
| Kuba | 53 |
| Mexiko | 52 |
| Nicaragua | 5505 |
| Panama | 507 |
| Peru | 51 |
| Surinam | 597 |
| Uruguay | 598 |
| Venezuela | 58 |

**Ozeanien 006**

| | |
|---|---|
| Australien | 61 |
| Indonesien | 62 |
| Malaysia | 60 |
| Neuseeland | 64 |
| Philippinen | 63 |
| Samoa | 685 |
| Thailand | 66 |

**Russland 007**

| | |
|---|---|
| Russland | 7 |
| Kasachstan | 7 |
| Tadschikistan | 7 |

**Fern-Asien 008**

| | |
|---|---|
| China | 86 |
| Hongkong | 852 |
| Japan | 81 |
| Korea | 82 |
| Laos | 856 |
| Taiwan | 886 |
| Vietnam | 84 |

**Nahost-Asien 009**

| | |
|---|---|
| Aserbaidschan | 994 |
| Bahrain | 973 |
| Georgien | 995 |
| Indien | 91 |
| Irak | 964 |
| Iran | 98 |
| Israel | 972 |
| Jemen | 967 |
| Jordanien | 962 |
| Libanon | 961 |
| Mongolei | 976 |
| Nepal | 977 |
| Oman | 968 |
| Pakistan | 92 |
| Saudi Arabien | 966 |
| Sri Lanka | 94 |
| Syrien | 963 |
| Türkei | 90 |
| Turkmenistan | 993 |

Bild: Internationale Vorwahlnummern

**Satellitennetze**

| | | |
|---|---|---|
| 881 | 0 / 1 | ICO |
| 881 | 2 / 3 | Ellipso |
| 881 | 4 / 5 | |
| 881 | 6 / 7 | Iridium |
| 881 | 8 / 9 | Globalstar |

**Globale Netzbetreiber**

| | | |
|---|---|---|
| 882 | 10 | BT |
| 882 | 11 | ST Telecommunications PTE |
| 882 | 12 | WorldCom |
| 882 | 13 | Telespazio |
| 882 | 14 | Verizon |
| 882 | 15 | Telstra |
| 882 | 16 | Thuraya |
| 882 | 17 | AT&T |
| 882 | 18 | Teledesic |
| 882 | 19 | Telecom Italia |
| 882 | 20 | ACeS |
| 882 | 21 | Ameritech |
| 882 | 22 | Cable & Wireless |
| 882 | 23 | Sita-Equant |
| 882 | 24 | Telia |
| 882 | 25 | Constellation Comms |
| 882 | 26 | SBC Communications Inc. |
| 882 | 27 | Williams Communications Inc. |
| 882 | 28 | Deutsche Telekom |
| 882 | 29 | Q-Tel (NZ) Ltd |
| 882 | 30 | Singapore Telecom |
| 882 | 31 | Telekom Malaysia |

Bild: Vorwahlnummern von Satellitennetzen (881) und globalen Netzbetreiber (882)

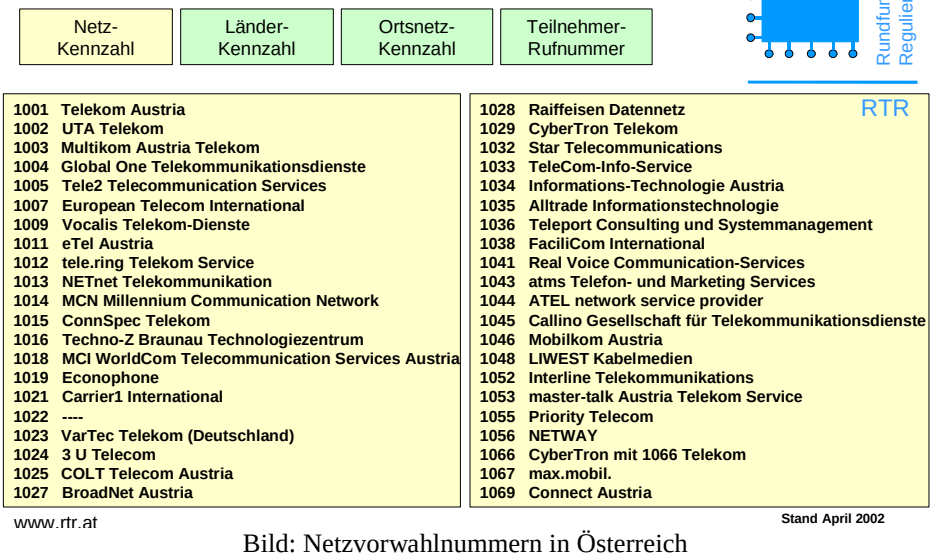



Bild: Netzvorwahlnummern in Österreich

Über **Netzvorwahlnummer** kann ein Netzbetreiber oder Netzanbieter nach eigener Wahl erreicht werden. Gehört der Netzanschluss dem Netzbetreiber selbst, ist der Netzkennzahl nicht notwendig.

Im Ortsvermittlungsknoten des Teilnehmers findet die Vermittlung der Verbindung zum gewählten Netz statt.

Bedingungen und Nummern werden in Österreich von der RTR (Rundfunk & Telekom Regulierungsbehörde) vorgegeben.

In den Ortvermittlungsknoten geschieht im allgemeinen auch die Trennung zwischen der Durchschaltevermittlung (Telefonnetz) und der Paketvermittlung (Internet, X.25, FR, ATM)

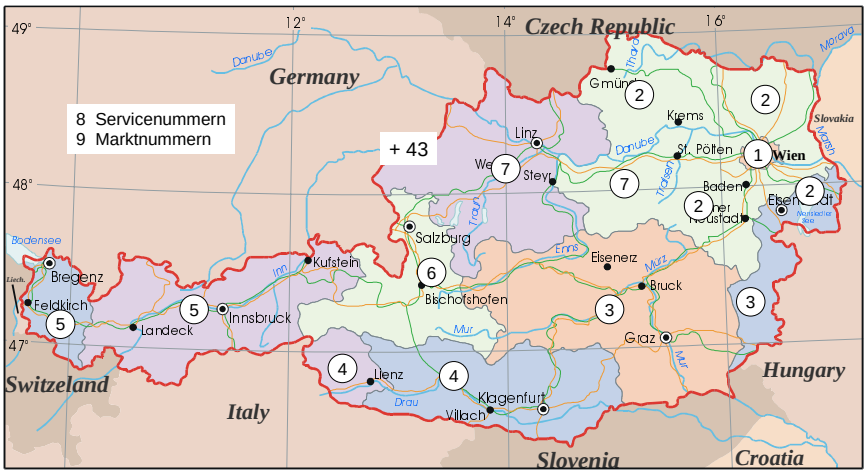
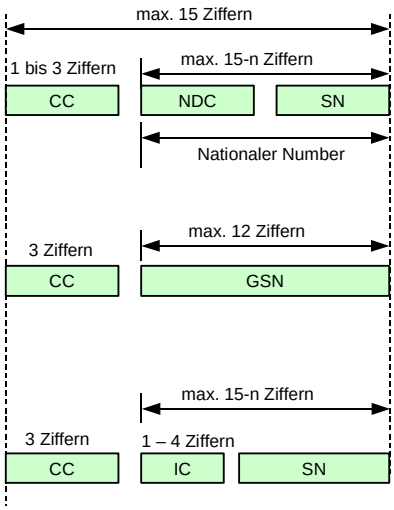



Bild: Festnetznummernplan in Österreich

Bei der **offenen Nummerierung** (open numbering) werden Kennzahlen und Verkehrsausscheidungszahlen (prefix) im Verkehr zwischen unterschiedlichen Nummerierungsbereichen angewandt. D.h. bei Ortsrufen müssen Landes- und Ortszahlen nicht mitgewählt werden bzw. bei einem Landesruf muss die Landeszahl nicht mitgewählt werden.

Bei der **verdeckten Nummerierung** (closed numbering) ist die Kennzahl fester Bestandteil der Rufnummer. D.h. auch bei Ortsrufen müssen Landes- und Ortszahlen mitgewählt werden.

Bei der **gemischten Nummerierung** (mixed numbering) ist der festen Mitwahl von Landes- und Ortszahlen von der geographischen Lage abhängig.




**Geographische Bereiche**

| | |
|---|---|
| CC: | Country Code |
| NDC: | National Destination Code (optional) |
| SN: | Subscriber Number |
| n: | Anzahl der Stellen im Country Code |

**Globale Dienste**

| | |
|---|---|
| CC: | Country Code für den globalen Dienst |
| GSN: | Global Subscriber Number |

**Netze**

| | |
|---|---|
| CC: | Country Code für Netze |
| IC: | Identification Code |
| SN: | Subscriber Number |
| n: | Anzahl der Stellen im Identification Code |

Das E.164 Nummernsystem legt für die maximal 15 Ziffern drei Nummerierungsmöglichkeiten fest:
- nach geographischen Bereichen,
- nach globalen Diensten,
- nach Netzen.

Je nach Verwendung ist die Einteilung der Ziffern verschieden.

Bild: E.164 Nummernsystem

**GSM-Netze**

| | |
|---|---|
| 650 | GSM-Netz der tele.ring |
| 664 | GSM-Netz der Mobilkom Austria |
| 676 | GSM-Netz der T-Mobile Austria |
| 699 | GSM-Netz der Firma Connect Austria |

**Weitere Mobilfunknetze**

| | |
|---|---|
| 660 | Hutchison 3G Austria |
| 663 | Mobilfunknetz D der Mobilkom Austria |
| 666 | Pagerdienst der Mobilkom Austria |
| 669 | Pagerdienst der Mobilkom Austria |
| 678 | TETRA-Netz der TetraCall Bündelfunk |
| 680 | 3G Mobile Telecommunications |

Bild: Mobilnetzvorwahlnummern in Österreich

**Europa 2xx**

| | |
|---|---|
| Albanien | 276 |
| Andora | 213 |
| Armenien | xxx |
| Belarus | 257 |
| Belgien | 206 |
| Bosnien | 218 |
| Bulgarien | 284 |
| Dänemark | 233 |
| Deutschland | 262 |
| Estland | 248 |
| Finnland | 244 |
| Frankreich | 208 |
| Georgien | 282 |
| Gibraltar | 266 |
| Griechenland | 202 |
| Irland | 272 |
| Island | 274 |
| Italien | 222 |
| Jugoslawien | 220 |
| Kroatien | 219 |
| Lettland | 247 |
| Litauen | 246 |
| Luxemburg | 270 |
| Malta | 278 |
| Moldau | 259 |
| Monaco | 212 |
| Niederlande | 204 |
| Norwegen | 242 |
| Österreich | 232 |
| Polen | 260 |
| Portugal | 268 |
| Rumänien | 226 |
| Russland | 250 |
| Schweden | 240 |
| Schweiz | 228 |
| Slowakei | 231 |
| Slowenien | 293 |
| Spanien | 214 |
| Türkei | 286 |
| Tschechien | 230 |
| UK | 234 + 235 |
| Ukraine | 255 |
| Ungarn | 216 |
| Zypern | 280 |

**Nordamerika 3xx**

| | |
|---|---|
| Haiti | 372 |
| Kanada | 302 |
| Kuba | 368 |
| Mexiko | 334 |
| USA | 310-316 |

**Asien 4xx**

| | |
|---|---|
| Afghanistan | 412 |
| Bangladesch | 470 |
| Bahrain | 426 |
| China | 460 |
| Hongkong | 454 |
| Indien | 404 |
| Irak | 418 |
| Iran | 432 |
| Israel | 425 |
| Japan | 440-441 |
| Jemen | 421 |
| Jordanien | 416 |
| Laos | 457 |
| Libanon | 415 |
| Mongolei | 428 |
| Nepal | 429 |
| Nord-Korea | 467 |
| Oman | 422 |
| Pakistan | 410 |
| Saudi Arabien | 420 |
| Sri Lanka | 413 |
| Süd-Korea | 450 |
| Syrien | 417 |
| Taiwan | 466 |
| Vietnam | 452 |

**Ozeanien 5xx**

| | |
|---|---|
| Australien | 505 |
| Indonesien | 510 |
| Malaysia | 502 |
| Neuseeland | 530 |
| Philippinen | 515 |
| Singapur | 525 |
| Thailand | 520 |

**Afrika 6xx**

| | |
|---|---|
| Ägypten | 602 |
| Algerien | 603 |
| Angola | 631 |
| Äthiopien | 636 |
| Benin | 616 |
| Botsuana | 652 |
| Burundi | 642 |
| Ivorküste | 612 |
| Dschibuti | 638 |
| Eritrea | 636 |
| Gabun | 628 |
| Gambia | 607 |
| Ghana | 620 |
| Guinea | 611 |
| Kamerun | 624 |
| Kap Verde | 625 |
| Kenia | 639 |
| Kongo | 629 |
| Liberia | 618 |
| Libyen | 606 |
| Malawi | 650 |
| Mauritius | 617 |
| Mosambik | 643 |
| Namibia | 649 |
| Niger | 614 |
| Nigeria | 621 |
| Ruanda | 635 |
| Sambia | 645 |
| Senegal | 608 |
| Simbabwe | 648 |
| Somalia | 637 |
| Sudan | 634 |
| Südafrika | 655 |
| Swasiland | 653 |
| Tansania | 640 |
| Tunesien | 605 |
| Tschad | 622 |
| Uganda | 641 |

**Süd-Amerika 7xx**

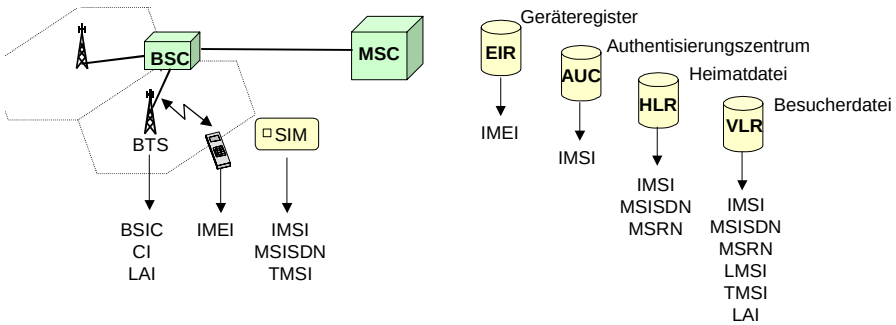
| | |
|---|---|
| Argentinien | 722 |
| Brasilien | 724 |
| Bolivien | 736 |
| Chile | 730 |
| Costa Rica | 712 |
| Ecuador | 740 |
| El Salvador | 706 |
| Guayana | 738 |
| Honduras | 708 |
| Kolumbien | 732 |
| Nicaragua | 710 |
| Panama | 714 |
| Pararguay | 744 |
| Peru | 716 |
| Surinam | 746 |
| Uruguay | 748 |
| Venezuela | 734 |

Bild: Mobilnetz-Ländervorwahl (E.212)

Die Mobilnetzvorwahlnummern werden nur zwischen Netzbetreibern verwendet. Sie haben für die Teilnehmer keine Bedeutung.

Als Vertreter für die Nummerierung und Adressierung in Mobilnetzen wird GSM (Global System for Mobile Communications) betrachtet. GSM besteht aus einem Zugangsnetz von Funkzellen mit Basisstationen (BTS, Base Station Transceiver), die über Controller (BSC, Base Station Controller) mit den Vermittlungsknoten (MSC, Mobile Switching Node) verbunden sind. Zur Realisation stehen vier Datenbanksysteme mit den Benutzerdaten zur Verfügung. Für die Adressierung hat jeder Mobilteilnehmer eine Telefonnummer sowie eine eindeutige, nicht öffentlichbekannte IMSI (International Mobile Subscriber Identity) auf der SIM-Karte. Die IMSI wird nur über das Netz geschickt, wenn beim Einbuchen ins Netz auf der SIM-Karte des Teilnehmers keine temporäre Nummer (TMSI, Temporary Mobile Subscriber Number) vorhanden ist. Diese Nummern sind zum Teil auch in den Heimat- und Besucherdateien zu finden.

In den Heimat- und Besucherdateien zu finden. Dort ist eine weitere wichtige Nummer zu finden. Die **Aufenthaltsrufnummer** (mobile station roaming number, MSRN) ist die Nummer, die einem Mobilteilnehmer vorübergehend zugeordnet wird und angibt, in welchem Netzteil sich dieser Teilnehmer momentan aufhält. Sie besteht aus Landeskennzahl, Netzkennzahl des besuchten Netzes und einer Teilnehmernummer innerhalb des besuchten Netzes. Sie wird von der Aufenthaltsdatei (visiting location register, VLR) vergeben.




| | |
|---|---|
| SIM | - Subscriber Identity Module |
| EIR | - Equipment Identification Register |
| AUC | - Authentication Centre |
| HLR | - Home Location Register |
| VLS | - Visitor Location Register |
| BSC | - Base Station Controller |
| BTS | - Base Transceiver Station |
| MSC | - Mobile Switching Centre |

| | |
|---|---|
| MSISDN | - Mobile Subscriber ISDN Number |
| TMSI | - Temporary Mobile Subscriber Identity |
| MSRN | - Mobile Station Roaming Number |
| LMSI | - Local Mobile Station Identity |
| IMEI | - International Mobile Equipment Identity |
| IMSI | - International Mobile Subscriber Identity |
| BSIC | - Base Transceiver Station Identity Code |
| CI | - Cell Identity |
| LAI | - Location Area Identity |

Bild: Nummern und Adressen in GSM

Die Identität des Mobilgerätes (International Mobile Equipment Identifier, IMEI) ist im Geräteregister abgelegt.

In einem Mobilnetz selbst müssen alle Netzelemente adressierbar sein. Dies sind unter anderen:

- Zellen (CI, Identifier),
- organisatorisch zusammengefasste Zellen für das Suchen eines Teilnehmers (LAI, Location Area Identifier),
- Basisstationen (Base Station Identification Code, BSIC).

Das Authentisierungszentrum bereitet die Informationsdaten vor, die zur Authentisierung eines Teilnehmers durch die Heimatdatei (HLR, Home Register Location) benötigt wird.

# Adressierung zwischen OSI-Protokollschichten (SAPs, Service Access Point)

| Services | SAP |
|---|---|
| Application | - |
| Presentation | P - SAP |
| Session | S - SAP |
| Transport | T - SAP |
| Network | N - SAP |
| DataLink | DL - SAP |
| PHysical | PH - SAP |

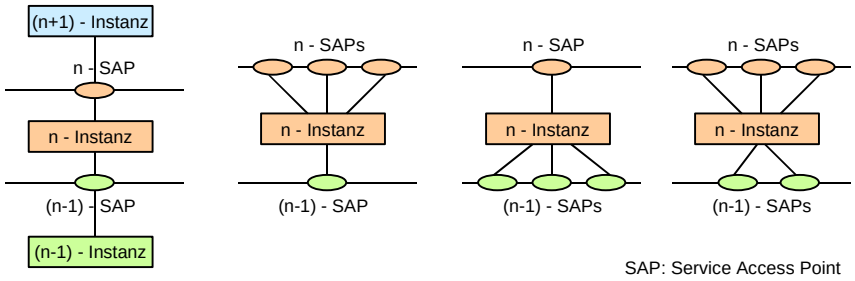
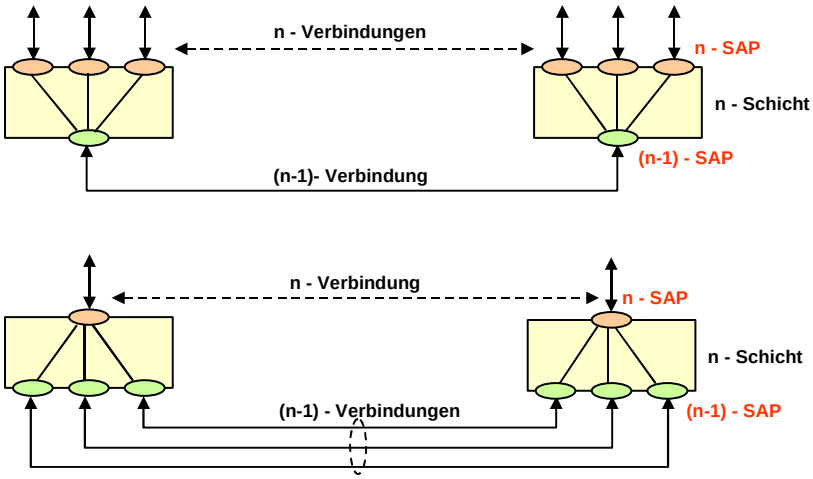



Bild: Service Access Points




Nnnnnnnn

Bild: Logische Verbindungen zwischen SAPs

# Adressierung zwischen Internet-Protokollschichten (Sockets)

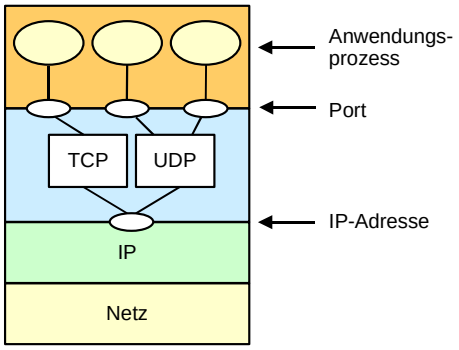



Bild: Transport-Adressen im Internet

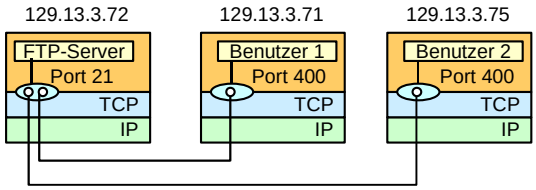



Bild: Adressierung in TCP (IP-Adresse + Port-Adresse)

| | | |
|---|---|---|
| 20 | FTP (Data), File Transfer Protocol | (TCP) |
| 21 | FTP (Control) | (TCP) |
| 23 | TELNET, Terminal Emulation | (TCP) |
| 25 | SMTP, Simple Mail Transfer Protocol | (TCP) |
| 53 | DOMAIN, Domain Name Server | (UDP) |
| 67 | BOOTPS, Bootstrap Protocol Server | (UDP) |
| 68 | BOOTPC, Bootstrap Protocol Client | (UDP) |
| 69 | TFTP, Trivial File Transfer Protocol | (UDP) |
| 80 | HTTP Hypertext Transfer Protocol (default port) | (TCP) |
| 111 | SUN RPC, Run Remote Procedure Call | (TCP) |
| 161 | SNMP, Simple Network Management Protocol | (UDP) |

Bild: Well Known Ports

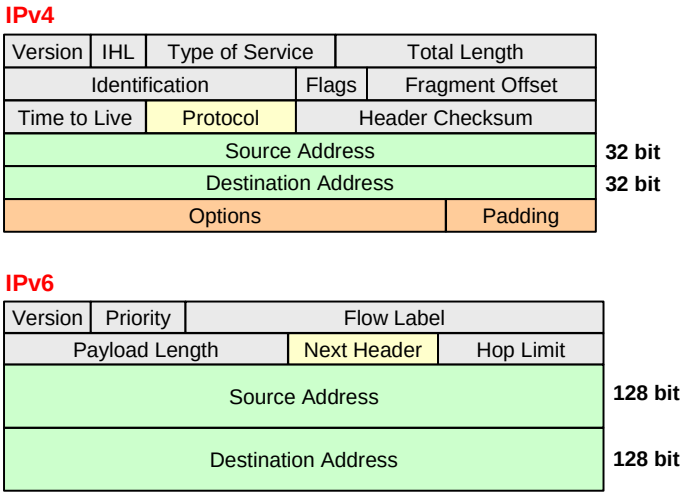



Bild: IPv4 und IPV6 Headers

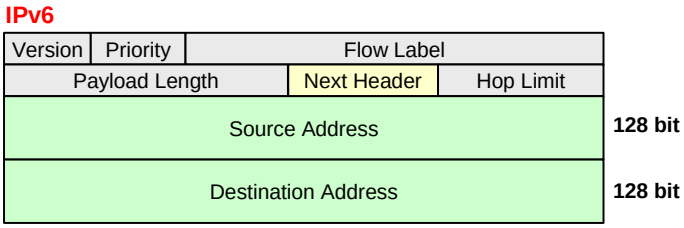



Bild: Protokoll

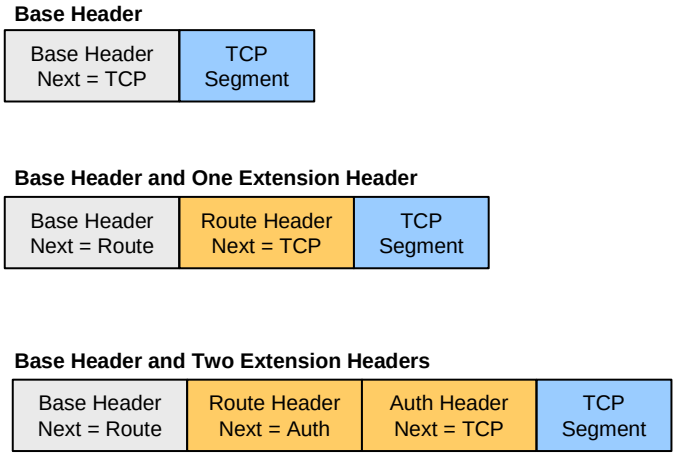
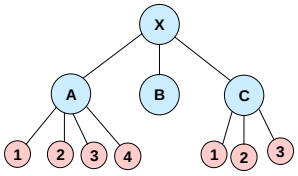
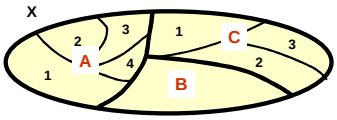



Bild: Extension Header in IPv6

# Adressierung in OSI-Systemen




Hierarchische Struktur




Netzaufteilung

**ISO-Adressierungsschema**

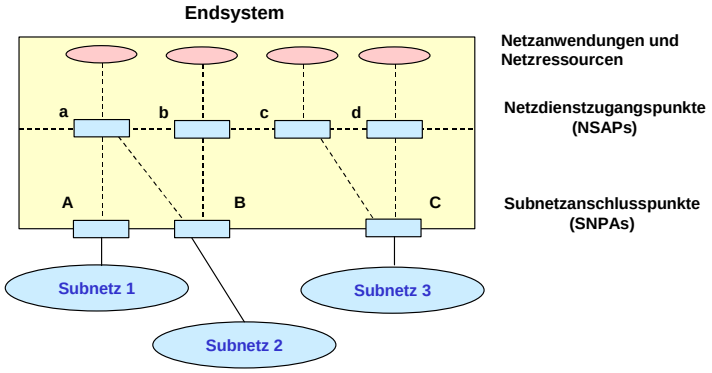
In ISO ist ein allgemeingültiges Adressierungsschema definiert, welches folgenden Forderungen genügt:

- Integration bestehender Adressierungsschemata (ITU, nationale Festlegungen),
- Strukturiertheit,
- Lokale Adressierungsmöglichkeit in abgegrenzten Teilbereichen.

**Merkmale:**

- Einteilung in mehrere Adressierungsbereiche (Adressierungsdomänen)
- Verfeinerung in Teildomänen möglich Adressierung innerhalb der Domänen durch eine Adressierungsverwaltung, welche verantwortlich ist für die weitere Unterteilung und Adressvergabe
- Codierung in Form von Dezimalziffern oder binär

Bild: OSI-Domänen und Subnetze




NSAP: Network Service Access Point
SNPA: Subnetwork Point of Attachment

Bild: OSI-Adressierungskonzept

Innerhalb dieses Adressierungsschemas können unterschieden werden:

- Netzadresse (network address)
  Kennzeichnung des Dienstzugangspunktes (SAP) der Vermittlungsschicht im OSI-Referenzmodell
- Quell-, Zieladresse (source/destination address)
  Adresse des Absenders/Empfängers von Nachrichten
- Gruppen-/Rundrufadresse (multicast/broadcast address)
  Adresse, unter der eine Gruppe oder alle Endeinrichtungen eines Netzbereiches angesprochen werden können

Die Adressen sind in einem **Adressverzeichnis** (directory) aufgeführt.

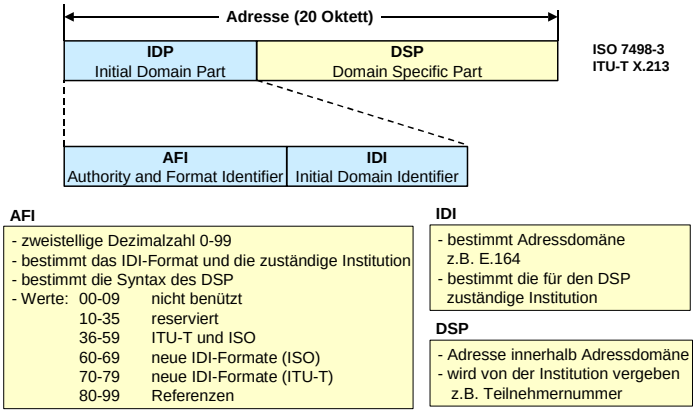
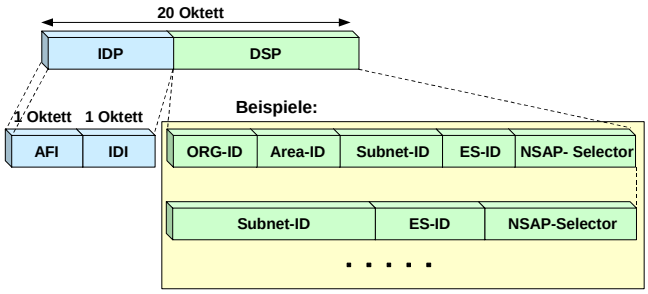



Bild: Adress-Struktur nach OSI

**Adressierung nach OSI**

Die verwendete Adressierung ist auch in X.213 festgelegt. Dort wird ein hierarchischer Aufbau der **NSAP-Adresse** (Network Service Access Point) beschrieben, der diese Felder enthält:

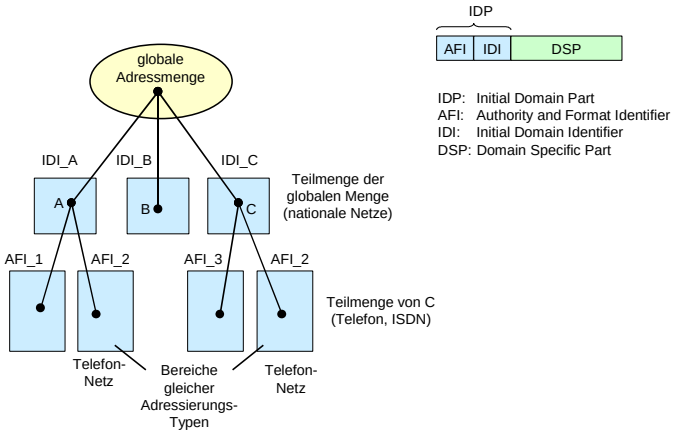
- IDP (Initial Domain Part), bestehend aus AFI und IDI.
- AFI (Authority Format Identifier) enthält eine zweistellige Dezimalzahl (0-99), die das IDI-Format und die dafür zuständige Institution sowie die Syntax des DSP bestimmt.
- IDI (Initial Doniain Identifier) gibt die Adressendomäne (beispielsweise DM ICD oder E.164 und die für den DSP zuständige Institution an. Die genaue Bedeutung des IDI folgt aus dem angegebenen AFI-Wert.




IDP: Initial Domain Part
DSP: Domain Specific Part
AFI: Authority and Format Identifier
IDI: Initial Domain Identifier

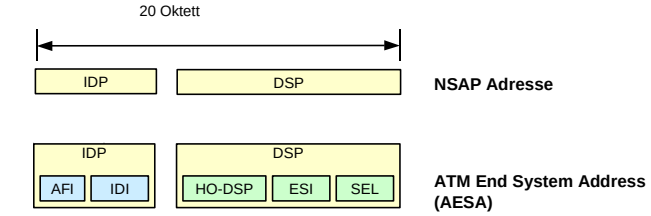
ES: End System
NSAP: Network Service Access Point

Bild: Network Service Access Point (NSAP)




IDP: Initial Domain Part
AFI: Authority and Format Identifier
IDI: Initial Domain Identifier
DSP: Domain Specific Part

Bild: Adressierungssystem




AFI: Authority and Format Identifier
IDI: Initial Domain Identifier
IDP: Initial Domain Part
DSP: Domain Specific Part

HO-DSP: Higher Order Domain Specific Part
ESI: End System Identifier
SEL: Selector

Bild: Schema der NSAP Adresse

DSP (Domain Specific Part), Adresse innerhalb der Adressendomäne. Diese wird von der dafür zuständigen Institution vergeben und kann die Adresse eines Teilnehmers sein.

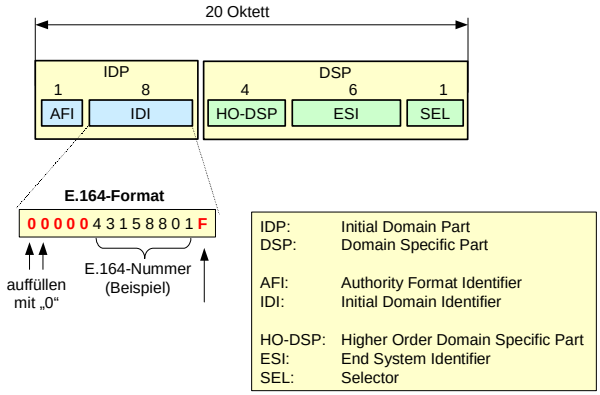



Bild: NSAP Adresse nach E.164

# Adressierung in ATM-Systemen

In ATM-Systemen bilden die Felder AFI und IDI zusammen den IDP (Initial Domain Part). Der DSP (Domain Specific Part) besteht aus HO-DSP, ESI und SEL. Der HO-DSP identifiziert einen Teil eines Adressraums, also ein Subnetz. Der ESI benennt ein bestimmtes Endsystem irrt Subnetz. Das SEL-Feld kann durch das Endsystem interpretiert und für die Auswahl eines bestimmten Anwendungsprozesses benutzt werden.

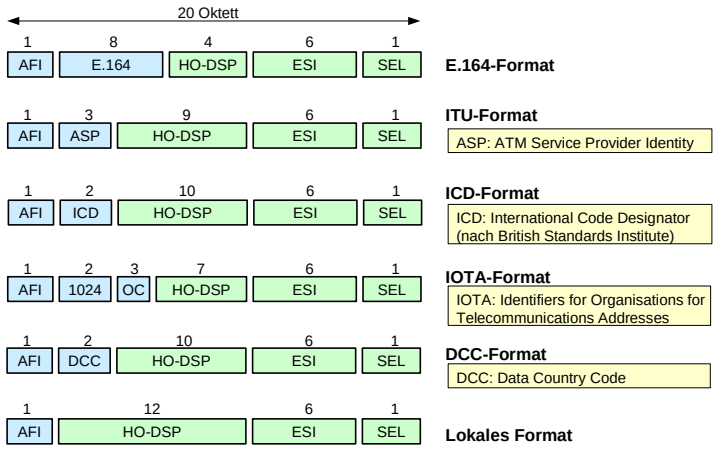



Bild: AESA: ATM End System Address

**ATM-Adressen** sind ein Beispiel für OSI-Adressen. Für die Realisierung weltweiter ATM-Netze wurden mehrere Adressformate vorgesehen. Das **DCC-Format** (Data Country Code) enthält Ländercodes. Das **ICD-Format** (International Code Designator) identifiziert im Feld ICD eine internationale Organisation eindeutig. Der Inhalt dieses Feldes wird vom BSI (British Standards Institute) zugeteilt. Das E.164-Format enthält im IDI-Feld eine E.164 Nummer. Diese besteht aus 15 Dezimalziffern, die eine Landeskennung und eine nationale Kennung (National Significant Number) repräsentieren. Bei Verwendung einer E.164-Nummer sind ATM-Systeme weltweit eindeutig adressierbar.

**X.121-Adressen**

Adressen nach der Empfehlung X.121 werden im Packet Level Protocol von X.25 zur Adressierung des Empfängers. Sie können ebenfalls in Frame Relay genutzt werden. Die Adresse besteht aus maximal 14 Dezimalziffern. Das Feld PSN erlaubt die Auswahl eines bestimmten Netzes (Netzbetreibers) in einem Land.

## Adressierung in IEEE LANs

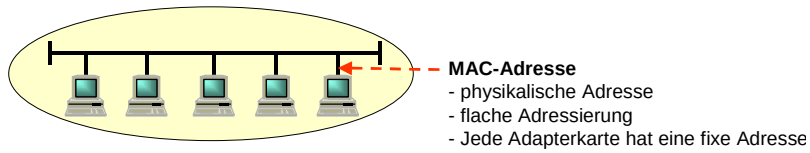



Bild: IEEE MAC-Adressen

**MAC-Adressen** sind **Hardwareadressen** (physikalische Adressen)**.** Sie sind der Hardware des Netzadapters in einem Netzknoten zugeordnet. Eine MAC-Adresse muss innerhalb eines Netzes, in dem Rahmen der Schicht 2 übertragen werden, eindeutig sein. Häufig werden MAC-Adressen jedoch global eindeutig vergeben, insbesondere dann, wenn - wie üblich - das Adressierungsschema nach IEEE 802 verwendet wird.

Wichtig ist, dass die MAC-Adressen keine Information darüber enthalten, wo sich die entsprechenden Stationen im LAN geographisch befinden.

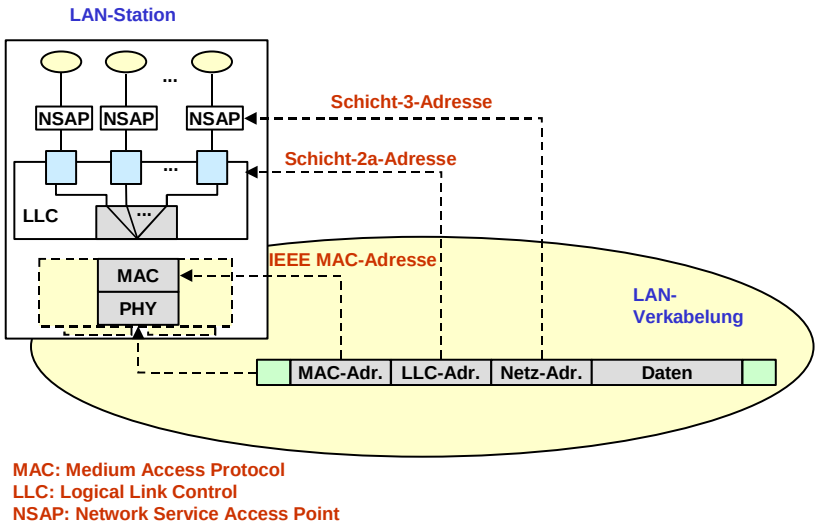



Bild: LAN-Adressierung

Logisch gesehen besteht die Kommunikation im LAN im Datenaustausch zwischen zwei Kommunikationspuffern innerhalb der LLC-Schicht. Dafür müssen die Datenrahmen zuerst zwischen entsprechenden LAN-Adapterkarten ausgetauscht werden.

Das prägnante Merkmal der MAC-Teilschicht ist die MAC-Adresse, mit der die entsprechende LAN-Adapterkarte addressiert wird. In jedem MAC-Rahmen muss sowohl eine MAC-Quelladresse als auch eine MAC-Zieladresse enthalten sein. Eine MAC-Adresse ist als eine physikalische LAN-Adresse zu interpretieren.

Um keinen Wildwuchs an unterschiedlichen MAC-Adressen aufkommen zu lassen, standardisierte das IEEE-Komitee 802 die physikalischen LAN-Adressen. Die erste Festlegung betraf hierbei die Länge des Adressfeldes im MAC-Header. Zuerst wurden sowohl 16- als auch 48-Bit Adressen vorgesehen (ausgenommen 802.6-Standard). Die Adressen mit 16 Bit Länge haben sich nicht durchgesetzt und wurden sogar aus dem Standard herausgenommen. Einzig beim Standard 802.6 besteht die Möglichkeit, mit 16-, 48- oder 64-Bit-Adressen zu arbeiten. Die größte Bedeutung kommt der MAC-Adresse mit 48 Bit Länge zu. Die 48-Bit-Adressen werden global eindeutig vergeben. Dazu teilt IEEE jedem Hersteller von Netzadaptern einen Block von herstellerspezifischen Adressteilen (OUI, Organisationally Unique Identifier) zu. Der Hersteller ergänzt diesen Teil für jeden hergestellten Adapter mit einer laufenden Nummer. IEEE hat für zukünftige Netze auch 64-Bit-Adressen unter der Bezeichnung EUI-64 definiert, die bisherigen 48-Bit-Adressen werden als EUI-48 bezeichnet.

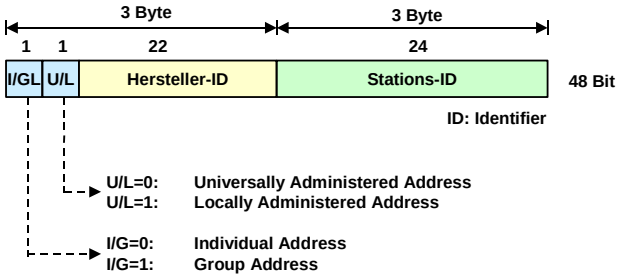



Bild: Struktur der IEEE MAC-Adresse

Ein LAN-Adapter-Hersteller muss eine von der IEEE einen Adressblock, bestehend aus mehreren Adressen, kaufen und hat dadurch die Gewissheit, dass die LAN-Adapterkarte, die er herstellt, weltweit eindeutig adressierbar ist. Die ersten drei Bytes der MAC-Adresse enthalten einen Festwert als Hersteller-Identifikator (ID), der den Hersteller weltweit eindeutig kennzeichnet. Diese Identifikator wird auch als OUI-Code (Organisationally Unique Identifier) bezeichnet. Die restlichen drei Bytes dienen als Stations-Identifikator und können von der Firma frei vergeben werden. Die Stations-ID ist also eine Art Kartennummer. Ein Hersteller kann damit bei einem festen Hersteller-ID bis zu 224 LAN-Adapterkarten mit unterschied-lichen Nummern (Adressen) versehen.

**Gruppenadresse**

In jedem LAN muss auch die Möglichkeit bestehen, einen MAC-Frame einmalig an mehrere Stationen zu verschicken. Dies setzt eine Gruppenadressierung voraus. Um eine derartige Adressierung zu unterstützen, haben in der MAC-Adresse die ersten zwei Bits eine besondere Bedeutung.

Das **I/G-Bit** legt fest, ob es sich um eine individuelle MAC-Adresse (I: Individuum) oder eine Gruppenadresse (G: Gruppe) handelt. Wird I/G=0 gesetzt, dann stellt die MAC-Adresse eine individuelle Adresse dar und deutet nur auf eine Station hin. Dagegen stellt im Fall I/G=1 die MAC-Adresse eine Gruppenadresse dar. Bei einer MAC-Ziel-Adresse als Gruppenadresse kann die Stations-ID eine Bitkombination enthalten, mit der eine logische Gruppe von Stationen gekennzeichnet wird. Ein Sonderfall ist eine Gruppe, die aus allen LAN-Stationen besteht. Dazu wird eine Sonder-Gruppenadresse verwendet, die als Multicast- oder Broadcast-Adresse bezeichnet wird, bei der sämtliche Bits der Stations-ID gleich 1 sind. Ein MAC-Frame mit einer Broadcast-Adresse wird von allen LAN-Adapterkarten aufgenommen.

Das **G/L-Bit** markiert, ob die gegebene MAC-Adresse eine globale (G) oder lokale (L) Bedeutung hat. Ist G/L=1, bedeutet dies, dass die Adresse durch IEEE vergeben wurde. In diesem Fall hat diese Adresse globale Bedeutung, d.h. sie ist weltweit

eindeutig. Ist G/L=0, besteht für den Hersteller einer LAN-Adapterkarte die Möglichkeit, die Adressen für die eigenen Karten unabhängig von den IEEE-Adressen selbst zu vergeben. Derartige Adressen haben nur lokale Bedeutung und können weltweit nicht eindeutig sein.

Ein Problem resultiert aus der Darstellung und die Übermittlung der Bits von MAC-Adressen bei den unterschiedlichen MAC-Zugriffsverfahren. So wird bei IEEE 802.3 (CSMA/CD) und IEEE 802.4 (Token Bus) das niederwertige Bit jedes Bytes zuerst übertragen, dagegen bei IEEE 802.5 (Token Ring) und FDDI wird das höchstwertige Bit zuerst übertragen. Dies kann durchaus dazu führen, dass bei einem Übergang von einem 802.3 LAN zu einem FDDI jede MAC-Adresse entsprechend umgestellt werden muss. Diese Situation ist vor allem in den Kopplungselementen zwischen zwei unterschiedlichen LANs zu beachten.

## Adressierung im Internet mit IPv4

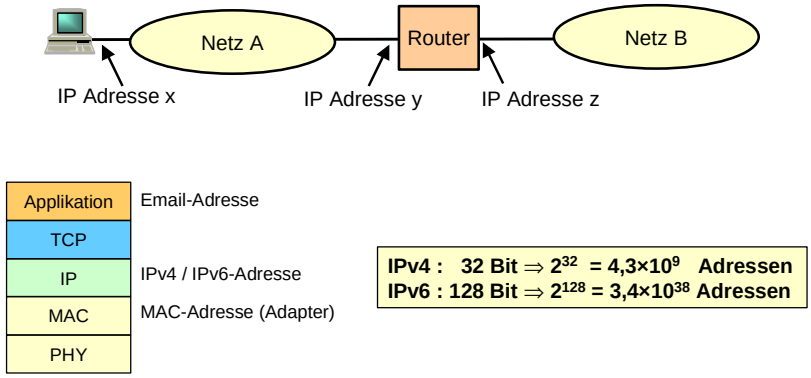
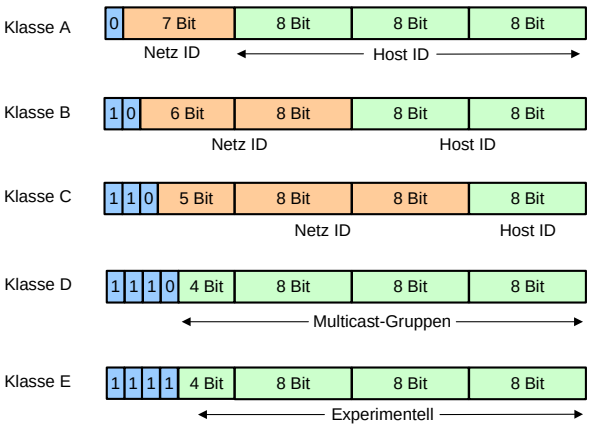
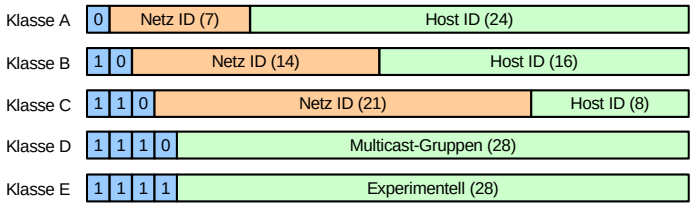



Bild: Verwendung von IP-Adressen

**Adressierung nach TCP/IP**
TCP/IP kennt IP-Adressen und Portnummern. **IP-Adressen** sind die Adressen der Netzschicht im TCP/IP-Protokollstapel. Sie bestehen aus 32 bit (4 Byte, in der IP-Version 4, kurz IPv4) bzw. 128 bit (16 Byte in IPv6). **Portnummern** werden von TCP und UDP zur Adressierung des darüber liegenden Dienstes benutzt. Sie sind also der OSI-Schicht 4 zuzuordnen. Im OSI-Referenzmodell ist der TSAP das Äquivalent zur Portnummer.

**Internet-Adressen**
Jedes Endsystem (Rechner, Router) im Netz wird beim Einsatz der Protokollfamilie TCP/IP durch eine logische IP-Adresse identifiziert. Für alle Endsysteme und Netzkomponenten, die unter Verwendung von TCP/IP kommunizieren, ist eine eindeutige IP-Adresse erforderlich. Jede IP-Adresse (sog. Unicast-Adresse) hat im allgemeinen folgende Struktur: Netz-ID , Host-ID (ID = Identifkation). Die Netz-ID (auch als Netz-ID bezeichnet) identifiziert sämtliche Systeme, die sich im gleichen Netz befinden. Alle Systeme im gleichen Netz müssen dieselbe Netz-ID tragen. Die Host-ID identifiziert ein beliebiges Endsystem (Arbeitsstation, Server, Router, ...) im Netz. Die Identifikation Host-ID muss für jedes einzelne Endsystern in einem Netz (d.h. für eine Netz-ID) eindeutig sein. Eine IP-Adresse bestimmt weltweit eindeutig einen Rechner. Es werden fünf Klassen von IP-Adressen definiert, um den Aufbau der Netze unterschiedlicher Größe zu ermöglichen. Die Adresse einer Klasse legt fest, welche Bits für die Netz-ID und welche für die Host-ID verwendet werden. Sie bestimmt ebenfalls die mögliche Anzahl der Netze und Endsysteme (Hosts).




| Klasse | Anzahl Netze | Anzahl Hosts | Adressbereich |
|---|---|---|---|
| A | 126 ($2^7 - 2$) | 16.777.214 ($2^{24} - 2$) | 1.0.0.0 – 126.0.0.0 |
| B | 16.384 ($2^{14}$) | 65.534 ($2^{16} - 2$) | 128.0.0.0 – 191.255.0.0 |
| C | 2 .097.152 ($2^{21}$) | 254 ($2^8 - 2$) | 192.0.0.0 – 223.255.255.0 |
| D | | | 224.0.0.0 – 239.255.255.255 |
| E | | | 240.0.0.0 – 255.255.255.254 |

Bild: IPv4-Adressklassen

- **Klasse A (Class A)**
  Die Adressen dieser Klasse werden Netzen mit einer sehr großen Anzahl von Endsystemen zugewiesen. Das höchstwertigste Bit einer Adresse der Klasse A ist immer auf 0 gesetzt. Die nächsten sieben Bits schließen die Netz-ID ab. Die rest-

lichen 24 Bits (d.h. die restlichen 3 Bytes) bilden die Host-ID. Dies ermöglicht, $2^7$ = 126 Netze und circa 17 Millionen von Endsystemen pro Netz zu identifizieren.

- **Klasse B (Class B)**
  Die Adressen dieser Klasse werden mittelgroßen und großen Netzen zugewiesen. Die zwei höchstwertigen Bits einer Adresse der Klasse B sind immer auf 10 gesetzt. Die weiteren 14 Bits (zur Vervollständigung der ersten beiden Bytes) stellen die Netz-ID dar. Die letzten 2 Bytes bilden die Host-ID. Dies ermöglicht, $2^{14}$ = 16 384 Netze und circa 65 000 Endsysteme pro Netz zu identifizieren.
- **Klasse C (Class C)**
  Die Adressen dieser Klasse C werden für kleine Netze (wie z.B. LANs) verwendet. Die 3 höchstwertigen Bits einer Adresse der Klasse C sind immer auf 110 gesetzt. Die weiteren 21 Bits (zur Vervollständigung der ersten 3 Bytes) stellen die Netz-ID dar. Das letzte Byte bildet die Host-ID. Dies ermöglicht, etwa 2 Millionen Netze und 254 Endsysteme pro Netz zu identifizieren.
- **Klasse D (Class D)**
  Die Adressen dieser Klasse D werden für den Einsatz bei Multicast-Gruppen (als geschlossene Benutzergruppen) verwendet. Eine Multicast-Adresse wird in der Regel mehreren Endsystemen zugeordnet. Die 4 höchstwertigen Bits einer Multicast-Adresse sind immer auf 1110 gesetzt. Die restlichen Bits bezeichnen eine Gruppe von Endsystemen. Die Multicast-Adressen enthalten keine Netz- bzw. Host-ID-Bits. Die IP-Pakete werden an eine ausgewählte Gruppe der Endsysteme in einem Netz weitergeleitet. Eine Multicast-Adresse repräsentiert im Grunde genommen bei der Multicast-Verteilung eine Tabelle mit "normalen" IP-Adressen einer Gruppe von Endsystemen.
- **Klasse E (Class E)**
  Die Klasse E stellt eine experimentelle Adresse dar und ist nicht für den normalen Gebrauch bestimmt.

**Beispiel: Klasse B**

| 1 | 0 | 00 0000 1111 0000 | 0000 0001 0110 1101 |
|---|---|---|---|
| | | Netz ID | Host ID |

**Notation**

**Binär:** 1000 0000 1111 0000 0000 0001 0110 1101
**Hexadezimal:** 80 F0 01 6D
**Gruppiert-dezimal** 128.240.1.109

Binäre Zahl: 1011 ⇒ $1•2^3 + 0•2^2 + 1•2^1 + 1•2^0 = 11$

| | | | | | |
|---|---|---|---|---|---|
| $2^0$ = | 1 | $2^3$ = | 8 | $2^6$ = | 64 |
| $2^1$ = | 2 | $2^4$ = | 16 | $2^7$ = | 128 |
| $2^2$ = | 4 | $2^5$ = | 32 | $2^8$ = | 256 |

| Hexa-dezimal | Binär | Dezimal |
|---|---|---|
| 0 | 0000 | 0 |
| 1 | 0001 | 1 |
| 2 | 0010 | 2 |
| 3 | 0011 | 3 |
| 4 | 0100 | 4 |
| 5 | 0101 | 5 |
| 6 | 0110 | 6 |
| 7 | 0111 | 7 |
| 8 | 1000 | 8 |
| 9 | 1001 | 9 |
| A | 1010 | 10 |
| B | 1011 | 11 |
| C | 1100 | 12 |
| D | 1101 | 13 |
| E | 1110 | 14 |
| F | 1111 | 15 |

### Darstellung von IP-Adressen

Jede IP-Adresse ist 32 Bit lang und besteht aus vier Feldern von je 8 Bit Länge, auch Bytes genannt. Die einzelnen Bytes werden durch Punkte voneinander getrennt. Ein Byte repräsentiert eine Dezimalzahl zwischen 0 und 255.

Bei dieser Adressvergabe unterscheidet man drei Klassen von Netzen. Je nach Anzahl der im Netz vorgesehenen TCP/IP-Hosts bekommt man eine Adresse einer entsprechenden Klasse zugeteilt. Über die Netzadresse wird, unter anderem, eine Unterteilung in verschiedene Anwendungen (Wissenschaft, Militär ..) und in Installationsorte (USA, Europa ... ) vorgenommen.

Bild: IPv4-Adresse

Es können weltweit maximal $2^7$-2 = 126 Netze der Klasse A existieren. Die IP-Adressen mit den Bit-Kombinationen "Alle Bits 0" und "Alle Bits l" sind ungültige IP-Adressen. Bei einem Netz der Klasse A können $2^{24}$ -2 Stationen adressiert werden. Bei einem Netz der Klasse B wird eine IP-Adresse vergeben, die die ersten 16 Bit (14 Bit) festlegt. Hier können nur noch $2^{16}$-2 IP-Adressen innerhalb eines Netzes vergeben werden. Einem Betreiber eines Klasse-C-Netzes bleiben genau 254 Adressen, die er seinen im Netz befindlichen Endsystemen (Hosts) zuordnen kann.

Neben dieser klassenbasierten Einteilung von IP-Adressen findet insbesondere bei ISPs eine bitweise Beschreibung des Netzschemas Verwendung, das Grundlage des Classless Inter-Domain Routings CIDR geworden ist.

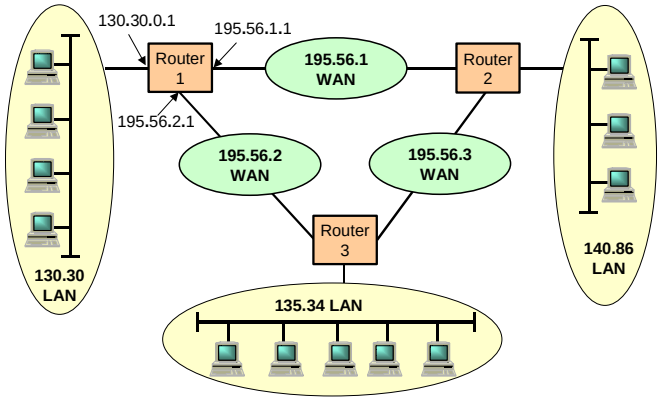



Bild: Router-Netz

Wie im Bild zu sehen ist, muss dem WAN auch eine Subnetz-ID zugeordnet werden, wenn die lokalen Netze mit Hilfe von Routern standortübergreifend über ein WAN verbunden sind. Zwischen diesen beiden Routern werden IP-Pakete über das WAN übermitttelt, so dass die Router-Ports seitens des WANs durch die eindeutigen IP-Adressen identifiziert werden. Da sich unterwegs zwischen den beiden Routern im WAN kein Router mehr befindet, muss das ganze WAN aus der Routing-Sicht als ein Subnetz gesehen werden. Damit muss dem WAN (formal!) eine Netz-ID zugeteilt werden. In diesem Fall stellt das WAN nur eine Verbindung für den Datenaustausch zwischen den Routern zur Verfügung.

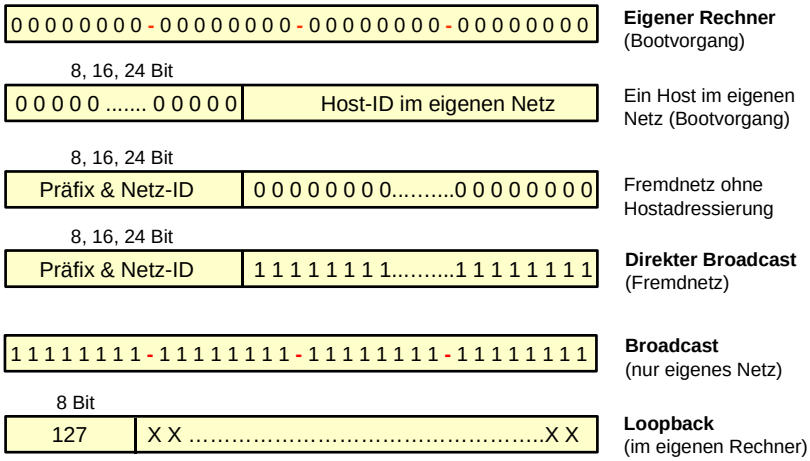



Bild: Spezielle IPv4-Adressen

### Vergabe von IP-Adressen

Bei der Vergabe von IP-Adressen muss vordringlich darauf geachtet werden, dass die Adressen aller in einem physikalischen Netz liegenden Endsysteme (Stationen) sich nur in dem Netz-ID-Teil unterscheiden und dass keine IP-Adresse doppelt vorkommt. Für die Nutzung des IP-Adressraums gelten darüber hinaus einige weitere Einschränkungen, auf die wir im folgenden kurz eingehen möchten. Diese betreffen die Verwendung bestimmter Netz-Adressbereiche sowie die Vergabe lokaler IP-Adressen als Host- bzw. Interface-ID. Generell können unterschieden werden:

- (lokale) IP-Netzadressen,
- (lokale) IP-Broadcastadressen,
- Loopback-Adresse sowie
- private IP-Adressbereiche.

Die lokale IP-Netzadresse, z.B. 135.167.0.0, darf nicht als Host-IP-Adresse verwendet werden. Falls alle Netz- und Host-ID-Bits auf 0 gesetzt sind, wird diese Adresse mit der Bedeutung "nur dieses Netz" interpretiert. Kritisch ist dieser Sachverhalt in Netzen mit gesetzten Subnetz-Masken. Bei benutzerdefinierten Subnet-Masken und eines Class-C-IP-Netzes kommt es vor, dass die IP-Subnetzadresse nicht auf den Wert „0“ endet. Ein Class-C-Netz mit der Subnetz-Maske *. 192 hat z. B. die Subnetz-Adressen *.0, *.64, *.128 sowie *.192.

Eine Host-ID darf nicht der Netz- bzw. Subnetz-Broadcastadresse entsprechen. Ein so eingerichteter Rechner würde neben den an ihn gerichteten Unicasts vom ganzen IP-Broadcast betroffen sein! Auch hier gilt, dass bei IP-Netzen mit nichttrivialen Subnetz-Masken besondere Aufmerksamkeit gefordert ist. Bei einem Class-C-IP-Netz mit Subnetz-Maske *.192 gelten auch die Adressen *.63, *.127 sowie *.191 als Subnetz-Broadcastadresse, die zusätzlich zum universellen Broadcast *.255 zu berücksichtigen sind. Auch ohne konfigurierte IP-Adresse hat jedes Interface eine eigene sog. Loopback-Adresse. Hierfür ist die Netznummer 127.0.0.* reserviert. Loopback-Adressen werden nach der Interface-Hierarchie vergeben. Das erste Interface hat somit die Loopback-Adresse 127. 0. 0. 1, das zweite Interface 127. 0. 0. 2 etc. Durch Ansprechen der Loopback-Adresse mittels der Kommandos ping und ifconfig (bzw ipconfig bei Windows) kann ein erster rudimentärer Test der Funktionsbereitschaft von IP erfolgen.

Zur Bildung privater IP-Netze innerhalb des Intemets sind gemäß RFC 1597/1918 folgende Adressbereiche vorgesehen:

- Class A: 10.0.0.0 ... 10.255.255.255
- Class B: 172.16.0.0 ... 172.31.255.255
- Class C: 192.168. 0. 0 ... 192.168.255.255

Diese Adressen können von mehreren Organisationen als Netz-ID gemeinsam benutzt werden, ohne dass Konflikte auftreten, da diese IP-Adressen weder im Internet vergeben noch ins Internet geroutet werden. In diesem Zusammenhang wird auch von einem Wiedergebrauch (reuse) von IP-Adressen gesprochen. Innerhalb der privaten IP-Adresssphäre lassen sich alle TCP/IP-Dienste (wie Domain Name Service) lokal ohne Einschränkungen aufbauen und benutzen. Für die Kommunikation mit dem öffentlichen Bereich des Internets gelten jedoch spezielle Verfahrensweisen, die in RFC 1631 als Network Adress Translation (NAT) beschrieben sind. Spezielle Anforderungen stellen sich z.B. im Hinblick auf das Weiterleiten von ICMP-

und SNMP-Mitteilungen sowie die Nutzung des Internet Domain Name Systems. Es ergibt sich eine asymmetrische Situation: Einerseits sollen für Client-Applikationen aus dem privaten IP-Netz heraus Server-Applikationen im Internet transparent verfügbar sein. Andererseits gilt, dass für Client-Anwendungen aus dem Internet heraus das private IP-Netz nicht sichtbar (wohl aber erreichbar!) sein darf.

Die Host-ID muss in einem Netz (bzw. einem Subnetz) eindeutig sein. Die Netz-ID identifiziert sämtliche Endsysteme, die sich im gleichen physikalischen Netz befinden. Allen Endsystemen eines physikalischen Netzes ist somit dieselbe Netz-ID zuzuteilen. Falls die Netze über Router miteinander verbunden sind, kann der Router als ein Multinetz-Endsystem gesehen werden, und pro Interface können mehrere IP-Adressen definiert sein. Jedem Port des Routers muss mindestens eine entsprechende IP-Adresse (die Interface-ID) zugewiesen werden. Systeme mit mehreren IP-Adressen (bzw. mehrere Interface-lDs) werden als Multi-Homed bezeichnet.

**Multicast-IP- und -MAC-Adressen**
Im reservierten Klass-D Adressraum für IP-Multicast-Zwecke werden zunächst noch einmal - ähnlich dem generellen IP-Adressraum – dedizierte Multicast-Adressen festgelegt (RFC 1700):

- lokales Multicasting: 224.0.0.0 bis 224.0.255, deren Adressen nicht geroutet werden
- Source-specific Multicasting: 232.0.0.0 bis 232.255.255.255 entsprechend IGMPv3 und
- All-Host-Group: 224.0.0.1 sowie
- All-Router-Group: 224.0.0.2 mit der Unterteilung
  - All DMVRP Routers 224.0.0.4
  - All OSPF Routers: 224.0.0.5
  - All OSPF Designated Routers: 224.0.0.6
  - All RIP2 Routers: 224.0.0.9
  - All PIM Routers: 224.0.0.13
  - All CBT Routers: 224.0.0.15
- Applikationsspezifische Multicasts (Auswahl):
  - NetworkTimeProtoco l(NTP) 224.0.1.1
  - Rhwo Daemon (RhwoD) 224.0.1.3
  - IETF-I-LOW-AUDIO: 224.0.1.10
  - JETF-1-AUDIO: 224.0.1.11
  - IETF- 1 –VIDEO: 224.0.1.12
  - IETF-2-LOW-AUDIO: 224.0.1.13
  - IETF-2-AUDIO: 224.0.1.14
  - IETF-2-VIDEO: 224.0.1.15

Alle anderen Multicast-Adressen werden temporär eingesetzt. Kennzeichnend für das IP-Multicasting ist, dass hierdurch einem IP-Interface zusätzlich zu seiner Unicast- mehrere Multicast-Adressen zugesprochen werden. Eine spezifische Multicast-Adresse steht hierbei für eine Anzahl von k Endsystemen, die der gleichen Multicast-Gruppe angehören. Zusätzlich gehören alle diese Systeme zur All-Host-Group.. Für die Endsysteme ist es wiederum leicht, ihren lokalen Multicast-Router zu ermitteln: Hierzu reicht eine IGMP-Request-Nachricht an die Adresse 224.0.0.2.

Würde sich IP-Multicasting nur auf IP-Adressen beziehen, müsste der M-Router zusätzlich eine k:1 Adresstabelle aller zu erreichenden Endsysteme pflegen, wobei hier k für die MAC-Adressen steht. Tatsächlich wird jedoch der umgekehrte Weg beschritten: Multicast-fähige Endsysteme verwalten neben ihrer MAC-Unicast-Adresse auch noch eine MAC-Multicast-Adresse, die aus der IP-Adresse abgeleitet wird.

Die 48 Bit MAC-Adresse wird unter Verwendung des G/L-Bits (Group/Local) als Multicast-Adresse gekennzeichnet. Der erste Teil der Adresse stellt den sog. Organisation Unique Identifier OUI dar, dessen Werte in RFC 1700 festgelegt sind. Dies gilt auch für das Bit 25 (in der hier gezeigten kanonischen Darstellung der MAC-Adresse), das den IP-Multicast-Typ festlegt. Es ist beachtenswert, dass durch diese Einschränkung lediglich 23 Bit zur Abbildung der IP-Adresse auf die MAC-Adresse verfügbar sind. Die höchstwertigen 5 Bit der IP-Adresse werden hierbei verworfen, so dass prinzipiell Adressüberschneidungen auftreten können.

| Klasse | Netzmaske | IP Adresse | Netz ID | Host ID | Host-Adressen |
|---|---|---|---|---|---|
| A | 255.0.0.0 | 34.63.1.132 | 34.0.0.0 | 0.63.1.132 | 0.0.1 -- 255.255.254 |
| B | 255.255.0.0 | 148.33.22.5 | 148.33.0.0 | 0.0.22.5 | 0.1 -- 255.254 |
| C | 255.255.255.0 | 195.1.1.34 | 195.1.1.0 | 0.0.0.34 | 1 -- 254 |

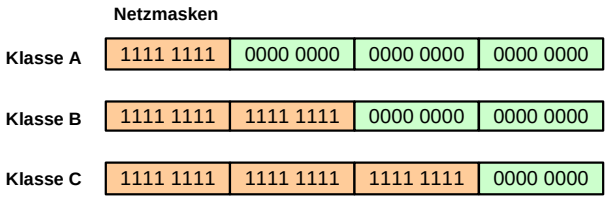



Bild: Netz und Host IPv4-Adressen

### Standard-Subnetz-Maske

Eine Subnetz-Maske (Subnet Mask) kann eine Standard-Subnetz-Maske (Default Subnet Mask) bzw. eine benutzerdefinierte Subnetz-Maske darstellen. Wird ein physikalisches Netz nicht auf die Subnetze (Teilnetze) aufgeteilt, so verwendet man in diesem Fall eine Standardmaske. Wird ein physikalisches Netz auf mehrere Subnetze (Teilnetze) aufgeteilt, so muss eine Subnetz-Maske vom Benutzer definiert werden. Auf diese Möglichkeit gehen wir später ein. Zunächst wird die Bedeutung einer Standardmaske näher erläutert.

Eine Standard-Subnetz-Maske ist eine 32-Bit-Kombination, die verwendet wird, um

- einen Teil der IP-Adresse auszublenden und auf diese Weise die Netz-ID von der Host-ID zu unterscheiden
- festzustellen, ob der Ziel-Host sich in demselben Netz oder einem anderen (Remote-) Netz befindet.

Jeder Host in einem TCP/IP-Netz benötigt eine Subnetz-Maske, d.h. entweder

- eine Standardmaske, falls keine Aufteilung des physikalischen Netzes vorgenommen wird, oder
- eine benutzerdefinierte Subnetz-Maske, falls das physikalische Netz auf mehrere Subnetze aufgeteilt wird.

Die Struktur der Standard-Subnetz-Maske ist von der Klasse der IP-Adresse abhängig. Wie hier ersichtlich ist, werden alle Bits, die zu einer Netz-ID gehören, auf 1 gesetzt. Der Dezimalwert jedes Bytes beträgt jeweils 255. Alle Bits, die zur Host-ID gehören, werden auf 0 gesetzt.

Um die Identifikation des Zielnetzes (d.h. Ziel-Netz-ID) aus einer IP-Adresse herauszufiltern, wird eine Operation Bitweise_AND für IP-Adresse und Subnetz-Maske ausgeführt. Die Operation Bitweise_AND besteht darin, dass jedes einzelne Bit der IP-Adresse mit dem entsprechenden Bit in der Subnetz-Maske verglichen wird. Wenn beide Bits 1 sind, ist das resultierende Bit ebenfalls 1. Wenn eine andere Kombination von Bits vorliegt, ist das resultierende Bit 0. Die Operation Bitweise_AND wird als ein rechnerinterner Prozeß durchgeführt, so dass der Benutzer keinen Einfluss auf dessen Durchführung hat.

**Bis 1992:**
- keine Zusammenhang zwischen Adressen und geographischen Bereichen
- dadurch große Routing-Tabellen

**Zuweisung der restlichen Klasse C Adressen**

| Region | Adressbereich |
|---|---|
| Multi-regional | 192.0.0.0 – 193.255.255.255 |
| Europa | 194.0.0.0 – 195.255.255.255 |
| Weitere geographische Bereiche | 196.0.0.0 – 197.255.255.255 |
| Nordamerika | 198.0.0.0 – 199.255.255.255 |
| Zentral- und Südamerika | 200.0.0.0 – 201.255.255.255 |
| Ozeanien | 202.0.0.0 – 203.255.255.255 |
| Weitere geographische Bereiche | 204.0.0.0 – 205.255.255.255 |
| Weitere geographische Bereiche | 206.0.0.0 – 207.255.255.255 |

Bild: Zusammenfassung von Klasse-C Adressen

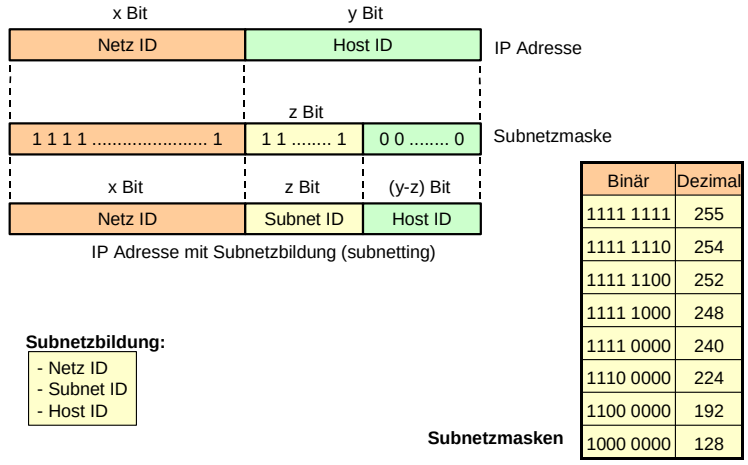



Bild: Subnetzbildung (Subnetting)

**Bildung von Subnetzen**

Ein Subnetz stellt eine geschlossene Gruppe der Endsysteme (Hosts) dar, und diese Gruppe wird mit einer Subnetz-ID identifiziert. Wird ein physikalisches Netz auf mehrere Teilnetze aufgeteilt, so bezeichnet man diese Teilnetze als Subnetze. Das ganze physikalische Netz kann auch als ein Sonder-Subnetz gesehen werden. Die Subnetze entstehen, wenn autonome Netze in mehrere physikalische oder logische Netze aufgeteilt werden. Zu einem Subnetz können auch mehrere physikalische Netze zusammengefasst werden. Dieser Gruppe von physikalischen Netzen muss eine gemeinsame Subnetz-ID zugewiesen werden.

Innerhalb von physikalischen LANs werden oft geschlossene Gruppen der Endsysteme gebildet. Diese Gruppen werden als virtuelle LANs (VLANs) bezeichnet. Ein virtuelles LAN kann als ein logisches Subnetz innerhalb eines physikalischen LANs interpretiert werden. Somit muss jedem virtuellen LAN auch eine Subnetz-ID zugewiesen werden.
Die großen TCP/IP-Netze müssen aus organisatorischen bzw. politischen Gründen oft auf kleinere Subnetze aufgeteilt werden, was man als Strukturierung bezeichnet. Diese Subnetze werden oft IP-Subnetze genannt. Für die Vernetzung von einzelnen IP-Subnetzen miteinander können IP-Router bzw. IP-Switches (d.h. Layer-3-Switches) eingesetzt werden.
Um ein Netz in Subnetze unterteilen zu können, muss jedes Subnetz eine andere Identifikation (ID) verwenden. Eine eindeutige Subnetz-ID wird geschaffen, indem man die Bits der Host-ID in zwei Bereiche aufteilt. Ein Bereich wird verwendet, um das Subnetz als eindeutige und selbständige Gruppe der Endsysteme zu identifizieren, der andere Bereich wird zur Identifizierung der Hosts in diesem Subnetz verwendet. Eine solche Aufteilung der Host-ID in der IP-Adresse wird auch als Subnetting oder Subnetworking bezeichnet.

- Jeder Abteilung (Organisation) kann ein getrenntes Subnetz zugeordnet werden.
- Unterschiedliche LAN-Technologien (beispielsweise Ethernet und Token-Ring) können als unterschiedliche Subnetze definiert und dementsprechend über Router verbunden werden.
- Die Belastung des Netzes kann reduziert werden, indem man den Verkehr zu den einzelnen Subnetzen einschränkt.

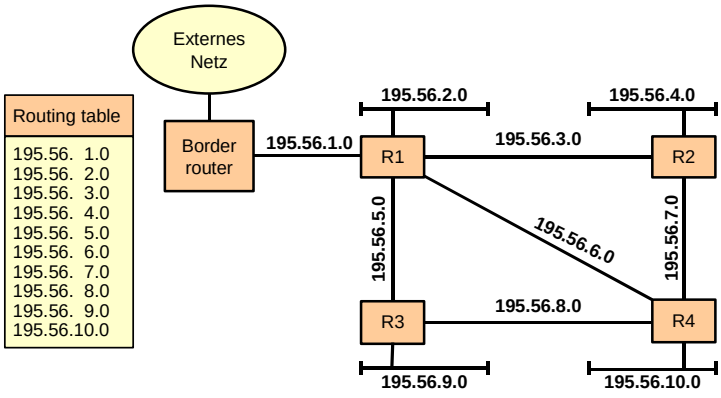



Bild: Netzklasse C ohne Subnetzbildung

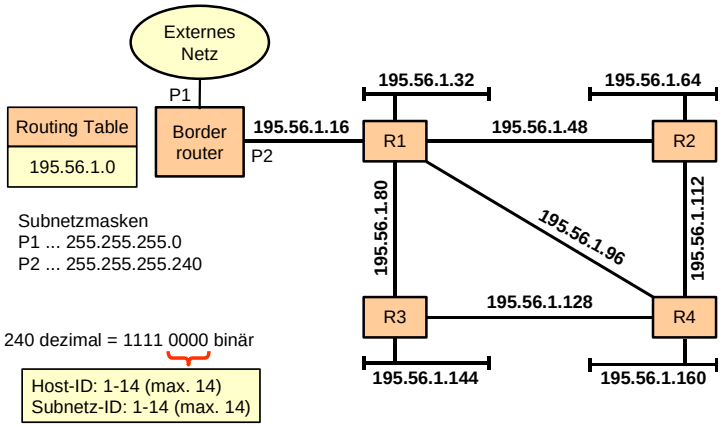



Bild: Netzklasse C mit Subnetzbildung

**Natürliche Subnetzmasken**

| | |
|---|---|
| Netzklasse A : | 255.0.0.0 |
| Netzklasse B : | 255.255.0.0 |
| Netzklasse C : | 255.255.255.0 |

**8-Bit Masken**

| Binär | Dezimal |
|---|---|
| 1111 1111 | 255 |
| 1111 1110 | 254 |
| 1111 1100 | 252 |
| 1111 1000 | 248 |
| 1111 0000 | 240 |
| 1110 0000 | 224 |
| 1100 0000 | 192 |
| 1000 0000 | 128 |

| | | |
|---|---|---|
| 0000 1001 0100 0011 0010 0110 0000 0001 | 9.67.38.1 | Klasse A Adresse |
| 1111 1111 1111 1111 1111 1111 11xx xxxx | 255.255.255.192 | Subnetzmaske |
| 0000 1001 0100 0011 0010 0110 00xx xxxx | 9.67.38.0 | Subnetzbasisadresse |
| xxxx xxxx 0100 0011 0010 0110 00xx xxxx | 68760 | Subnetznummer |

Klasse A ← Subnetz → Host

Bild: Subnetzmasken

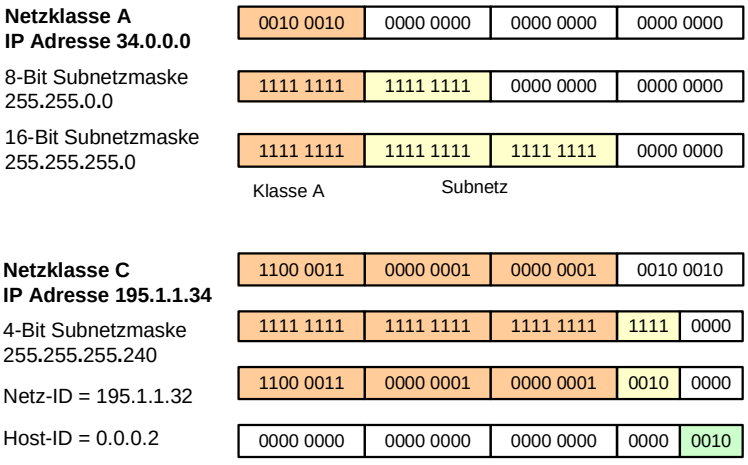



Bild: Subnetzbildung

### Benutzerdefinierte Subnetz-Maske

Die Festlegung einer benutzerdefinierten Subnetz-Maske ist erforderlich, wenn ein physikalisches Netz vom Benutzer in mehrere Subnetze aufgeteilt wird. Bevor eine Subnetz-Maske festgelegt wird, ermittelt man zuerst

- die Anzahl der Subnetze,
- die Anzahl der Hosts pro Subnetz.

Das Verfahren der IP-Subnetzbildung ist in RFC 950 beschrieben. Hierbei sind folgende Schritte zu unterscheiden:

1. Zunächst ist die Anzahl der Subnetze zu ermitteln und in das Binärformat zu konvertieren.
2. Die Anzahl der Bits, die für die Darstellung der Zahl der Subnetze im Binärformat erforderlich ist, bestimmt die Anzahl von Bits der Subnetz-ID. Werden beispielsweise 5 Subnetze benötigt, beträgt der Binärwert 101. Die Darstellung von "fünf" im Binärformat erfordert drei Bits.
3. Sind beispielsweise drei Bits für die Identifikation der Subnetze erforderlich, werden die ersten drei Bits der Host-ID durch die Subnet-ID belegt.
4. Der Dezimalwert für die binäre Kombination 11100000 beträgt 224. Die Subnetz-Maske (dezimal) ist somit 255.255.255.224.

**Bestimmen von Subnetz-lDs und Host-lDs**

Die Subnetz-II)s bestimmen diese Host-ID-Bits, über die sich die Subnetz-Maske erstreckt. Um eine Subnetz-ID zu bestimmen, werden zunächst die möglichen Bitkombinationen untersucht und dann in das Dezimalformat konvertiert.

Wie hier ersichtlich ist, sind dafür folgende Schritte nötig:

1. Alle möglichen Bitkombinationen der durch die Subnetz-Maske "belegten" Bits werden ermittelt.
2. Alle Bitkombinationen, die entweder nur 0 oder nur 1 enthalten, sind ungültig.
3. Die Bitkombinationen "Alle Bits 0" und "Alle Bits l" sind ungültige IP-Adressen. Die Kombination "Alle Bits C' ist reserviert und hat die Bedeutung "nur dieses Netz ". Mit der Kombination "Alle Bits l" wird eine Subnetz-Maske identifiziert.
4. Die restlichen Kombinationen (über das ganze Byte) werden in das Dezimalformat konvertiert. Jeder Dezimalwert stellt ein einzelnes Subnetz-ID dar.

Nach der Festlegung von Subnetz-lDs müssen die Host-II)s in den einzelnen Subnetzen bestimmt werden. Um Host-IDs innerhalb eines Subnetzes zu bestimmen, muss man zuerst berechnen, wie viele Bits für die Host-ID zur Verfügung stehen.

Subnetzmaske: 255.255.255.192 (1100 0000)
Subnetze : $2^2 - 2 = 2$
Hosts pro Subnetz : $2^6 - 2 = 62$

| | | | | |
|---|---|---|---|---|
| **Subnetz 1:** | 195.1.1 | 01 | 00 0000 | Netz ID = 195.1.1.64 |
| **Subnetz 2:** | | 10 | 00 0000 | Netz ID = 195.1.1.128 |

- Nicht erlaubt ist Subnetz 0 (Netz ID.0)
- Nicht erlaubt ist Subnetz-Broadcast (Netz ID.192)
- 124 von 254 Host-Adressen werden verwendet (48,8%)

Bild: Netzklasse C - Adresse 195.1.1.0 /26

Subnetzmaske: 255.255.255.224 (1110 0000)
Subnetze : $2^3 - 2 = 6$
Hosts pro Subnetz : $2^5 - 2 = 30$

| | | | | |
|---|---|---|---|---|
| **Subnetz 1:** | 195.1.1 | 001 | 0 0000 | Netz ID = 195.1.1.32 |
| **Subnetz 2:** | | 010 | 0 0000 | Netz ID = 195.1.1.64 |
| **Subnetz 3:** | | 011 | 0 0000 | Netz ID = 195.1.1.96 |
| **Subnetz 4:** | | 100 | 0 0000 | Netz ID = 195.1.1.128 |
| **Subnetz 5:** | | 101 | 0 0000 | Netz ID = 195.1.1.160 |
| **Subnetz 6:** | | 110 | 0 0000 | Netz ID = 195.1.1.192 |

- Nicht erlaubt ist Subnetz 0 (Netz ID .0)
- Nicht erlaubt ist Subnetzbroadcast (Netz ID .224)
- 180 von 254 Host-Adressen werden verwendet (70,8%)

Bild: Netzklasse C - Adresse 195.1.1.0 /27

Subnetzmaske: 255.255.255.240
(1111 0000)
Subnetze : $2^4 - 2 = 14$
Hosts pro Subnetz : $2^4 - 2 = 14$

- Nicht erlaubt ist
  Subnetz 0 (Netz ID .0)
  Subnetzbroadcast (Netz ID .240)
- 196 von 254 Host-Adressen
  werden verwendet (77,2%)

| Subnetz | Subnetz-ID | Subnetz-ID |
|---|---|---|
| 1 | 195.1.1. 0001 \| 0000 | 195.1.1.16 |
| 2 | 195.1.1. 0010 \| 0000 | 195.1.1.32 |
| 3 | 195.1.1. 0011 \| 0000 | 195.1.1.48 |
| 4 | 195.1.1. 0100 \| 0000 | 195.1.1.64 |
| 5 | 195.1.1. 0101 \| 0000 | 195.1.1.80 |
| 6 | 195.1.1. 0110 \| 0000 | 195.1.1.96 |
| 7 | 195.1.1. 0111 \| 0000 | 195.1.1.112 |
| 8 | 195.1.1. 1000 \| 0000 | 195.1.1.128 |
| 9 | 195.1.1. 1001 \| 0000 | 195.1.1.144 |
| 10 | 195.1.1. 1010 \| 0000 | 195.1.1.160 |
| 11 | 195.1.1. 1011 \| 0000 | 195.1.1.176 |
| 12 | 195.1.1. 1100 \| 0000 | 195.1.1.192 |
| 13 | 195.1.1. 1101 \| 0000 | 195.1.1.208 |
| 14 | 195.1.1. 1110 \| 0000 | 195.1.1.224 |
| | | |

Bild: Netzklasse C - Adresse 195.1.1.0 /28

Subnetzmaske: 255.255.255.248
(1111 1000)
Subnetze : $2^5$ - 2 = 30
Hosts pro Subnetz : $2^3$ - 2 = 6

14 • 2 Subnetze

| Subnetz | Subnetz-ID | Subnetz-ID |
|---|---|---|
| 1 | 195.1.1. 0000 1 \| 000 | 195.1.1.8 |
| 2 | 195.1.1. 0001 0 \| 000 | 195.1.1.16 |
| 3 | 195.1.1. 0001 1 \| 000 | 195.1.1.24 |
| 4 | 195.1.1. 0010 0 \| 000 | 195.1.1.32 |
| 5 | 195.1.1. 0010 1 \| 000 | 195.1.1.40 |
| 6 | 195.1.1. 0011 0 \| 000 | 195.1.1.48 |
| 7 | 195.1.1. 0011 1 \| 000 | 195.1.1.64 |
| | | |
| 24 | 195.1.1. 1100 0 \| 000 | 195.1.1.194 |
| 25 | 195.1.1. 1100 1 \| 000 | 195.1.1.202 |
| 26 | 195.1.1. 1101 0 \| 000 | 195.1.1.210 |
| 27 | 195.1.1. 1101 1 \| 000 | 195.1.1.216 |
| 28 | 195.1.1. 1110 0 \| 000 | 195.1.1.224 |
| 29 | 195.1.1. 1110 1 \| 000 | 195.1.1.232 |
| 30 | 195.1.1. 1111 0 \| 000 | 195.1.1.240 |

- Nicht erlaubt ist
  Subnetz 0 (Netz ID .0)
  Subnetzbroadcast (Netz ID .248)
- 180 von 254 Host-Adressen
  werden verwendet (70,8%)

2•1 +14•2 = 30 Subnetze

Bild: Netzklasse C - Adresse 195.1.1.0 /29

Subnetzmaske: 255.255.255.252
(1111 1100)
Subnetze : $2^6$ - 2 = 62
Hosts pro Subnetz : $2^2$ - 2 = 2

14 • 4 Subnetze

| Subnetz | Subnetz-ID | Subnetz-ID |
|---|---|---|
| 1 | 195.1.1. 0000 01 \| 00 | 195.1.1.4 |
| 2 | 195.1.1. 0000 10 \| 00 | 195.1.1.8 |
| 3 | 195.1.1. 0000 11 \| 00 | 195.1.1.12 |
| 4 | 195.1.1. 0001 00 \| 00 | 195.1.1.16 |
| 5 | 195.1.1. 0001 01 \| 00 | 195.1.1.20 |
| 6 | 195.1.1. 0001 10 \| 00 | 195.1.1.24 |
| 7 | 195.1.1. 0001 11 \| 00 | 195.1.1.28 |
| | | |
| 56 | 195.1.1. 1110 00 \| 00 | 195.1.1.224 |
| 57 | 195.1.1. 1110 01 \| 00 | 195.1.1.228 |
| 58 | 195.1.1. 1110 10 \| 00 | 195.1.1.232 |
| 59 | 195.1.1. 1110 11 \| 00 | 195.1.1.236 |
| 60 | 195.1.1. 1111 00 \| 00 | 195.1.1.240 |
| 61 | 195.1.1. 1111 01 \| 00 | 195.1.1.244 |
| 62 | 195.1.1. 1111 10 \| 00 | 195.1.1.248 |

- Nicht erlaubt ist
  Subnetz 0 (Netz ID .0)
  Subnetzbroadcast (Netz ID .252)
- 124 von 254 Host-Adressen
  werden verwendet (48,8%)

2•3 +14•4 = 62 Subnetze

Bild: Netzklasse C - Adresse 195.1.1.0 /30

Subnetzmaske: 255.255.255.240 (1111 0000)

Subnetze: $2^4$ - 2 = 14
Hosts pro Subnetz : $2^4$ - 2 = 14

**Subnetz 1**

| Host number | | |
|---|---|---|
| | 195.1.1. 0001 \| 0000 | Netz ID = 195.1.1.16 |
| Host 1 | 195.1.1. 0001 \| 0001 | Host ID = 195.1.1.17 |
| Host 2 | 195.1.1. 0001 \| 0010 | Host ID = 195.1.1.18 |
| ---------- | 195.1.1. 0001 \| ------- | ---------- |
| Host 14 | 195.1.1. 0001 \| 1110 | Host ID = 195.1.1.30 |
| Broadcast | 195.1.1. 0001 \| 1111 | Broadcast ID = 195.1.1.31 |

**Subnetz 2**

| Host number | | |
|---|---|---|
| | 195.1.1. 0010 \| 0000 | Netz ID = 195.1.1.32 |
| Host 1 | 195.1.1. 0010 \| 0001 | Host ID = 195.1.1.33 |
| Host 2 | 195.1.1. 0010 \| 0010 | Host ID = 195.1.1.34 |
| ---------- | 195.1.1. 0010 \| ------- | ---------- |
| Host 14 | 195.1.1. 0010 \| 1110 | Host ID = 195.1.1.46 |
| Broadcast | 195.1.1. 0010 \| 1111 | Broadcast ID = 195.1.1.47 |

**4-Bit Subnetzmaske**

Subnetzmaske: 255.255.255.240 (1111 0000)
Subnetze : $2^4$ - 2 = 14
Hosts pro Subnetz : $2^4$ - 2 = 14

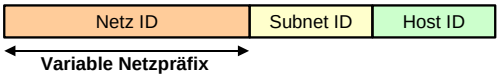
| | |
|---|---|
| 195.1.1.0 | **Subnetz 0** (Ungültige Host-Adressen) |
| 195.1.1.1 | |
| 195.1.1.2 | |
| -------- | |
| 195.1.1.15 | |

| | |
|---|---|
| 195.1.1.16 | (Ungültige Host-Adressen) **Subnetz 1** |
| 195.1.1.32 | **Subnetz 2** |
| 195.1.1.48 | **Subnetz 3** |
| -------- | -------- |
| 195.1.1.224 | **Subnetz 14** |

| | |
|---|---|
| 195.1.1.31 | **Broadcast** (Ungültige Host-Adressen) **in Subnetz 1** |
| 195.1.1.47 | **in Subnetz 2** |
| 195.1.1.63 | **in Subnetz 3** |
| -------- | -------- |
| 195.1.1.239 | **in Subnetz 14** |

| | |
|---|---|
| 195.1.1.240 | (Ungültige Host-Adressen) |
| 195.1.1.241 | |
| -------- | |
| 195.1.1.254 | |
| 195.1.1.255 | **Broadcast in allen Subnetzen** |

Bild: Netzklasse C - Adresse 195.1.1.0 /28




Ersetzen der festen Netzklassen durch Netz-Präfixe variabler Länge (13 bis 27 Bit)

**Beispiel: 129.24.12.0/14**
Die ersten 14 Bit der IP-Adresse werden für die Netz-Identifikation verwendet

Einsatz in Verbindung mit hierarchischem Routing
- Backbone-Router betrachtet nur z.B. die ersten 13 Bit (kleine Routing-Tabellen, wenig Rechenaufwand)
- Router eines angeschlossenen Providers z.B. die ersten 15 Bit
- Router in einem Firmennetz mit 128 Hosts betrachtet 25 Bit

Durch geschickte Adressvergabe können mehrere ursprüngliche Netze der Klasse C durch ein einziges Präfix zusammengefasst werden

Wiederholte Zusammenfassung führt zu kürzeren Präfixes der IP-Adressen

**Vorteil:** Reduzierung der Grösse von Routingtabellen
Auffinden des „Longest Matching Prefix“

Class C ist auch nach dem geographischem Vorkommen unterteilt
Europa: 194.0.0.0 – 195.255.255.255

**CIDR und Subnetze**

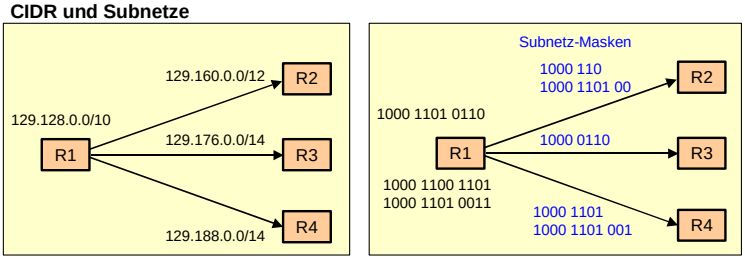



Bild: CIDR: Classless Inter-Domain Routing

### Zielbestimmung eines IP-Pakets beim Quellrechner

Beim Absenden jedes IP-Pakets muss im Quellrechner festgelegt werden, ob das Paket für einen Zielrechner in demselben Subnetz oder in einem anderen "Remote"-Subnetz bestimmt ist. Falls der Zielrechner sich in einem anderen Subnetz befindet, wird das IP-Paket an einen Router (Gateway) abgeschickt. Im allgemeinen besteht die Funktion eines Routers (genauer ge-

sagt: eines IP-Routers) darin, die einzelnen Subnetze miteinander logisch so zu vernetzen, dass die Kommunikation zwischen zwei Rechnern, die zu unterschiedlichen Subnetzen gehören, ermöglicht werden kann. An dieser Stelle ist hervorzuheben, dass die primäre Funktion eines IP-Routers darin besteht, mehrere (IP-)Subnetze miteinander zu vernetzen.

Falls eine Aufteilung des physikalischen Netzes vorgenommen wurde, setzt sich das physikalische Netz aus einer Anzahl von Subnetzen zusammen. Da es sich nun um eine Vernetzung von Subnetzen handelt, ist dies beim Absenden jedes Pakets zu berücksichtigen. In diesem Fall muss zuerst bestimmt werden, ob der Zielrechner zum gleichen Subnetz gehört. Es muss hierfür das Paar (Ziel-Netz-ID, Ziel-Subnetz-ID) mit dem Paar (Quell-Netz-ID, Quell-Subnetz-ID) bitweise verglichen werden.

Falls kein Subnetting verwendet wird, handelt es sich um eine Standard-Subnetz-Maske (genauer gesagt: Netzmaske). Beim Subnetting wird die Subnetz-Maske vom Benutzer definiert. In beiden Fällen kann die im Bild dargestellten Operation Bitweise-AND verwendet werden. Diese Operation wird vor dem Versand eines IP-Pakets sowohl für die Zieladresse als auch für die Quelladresse mit derselben Subnetz-Maske des Quellrechners ausgeführt. Wenn die Ergebnisse identisch sind, weiß man, dass der Zielrechner sich in demselben Netz befindet. In diesem Fall wird das IP-Paket direkt zum Zielrechner geschickt. Wenn die Ergebnisse der Operation Bitweise - AND unterschiedlich sind, gehört der Zielrechner zu einem anderen Netz und das IP-Paket wird zuerst an den Router (oft auch Default Gateway genannt) gesendet.

**Adressierungsaspekte**

Im folgenden wird auf einige Aspekte der Adressierung beim Versand der IP-Pakete näher eingegangen. Hierbei wird unter dem Begriff Subnetz sowohl ein logisches Subnetz als auch ein ganzes physikalisches Netz verstanden, falls dieses Netz auf die Teilnetze (Subnetze) nicht aufgeteilt wird. Wenn der Zielrechner sich im gleichen Subnetz befindet, wird das IP-Paket direkt an den Zielrechner abgeschickt, sonst an einen Router (Gateway) übergeben.

Im allgemeinen sind zwei Fälle zu unterscheiden:

- Das Subnetz ( stellt ein herkömmliches Shared Medium LAN dar, d.h. ein verbindungsloses Netz, das nach dem Broadcast-Prinzip funktioniert. In diesem Fall wird das IP-Paket in einen MAC-Frame des LANs eingebettet, und dieser MAC-Fraine enthält die MAC-Adresse des Ziel-Endsystems.
- Das Subnetz stellt ein leitungsvermittelndes Netz dar, wie z. B. ein WAN (ISDN, X.25-, ATM- bzw. Frame-Relay-Netz). In diesem Fall muss eine Verbindung zum Ziel-Endsystem für die Übermittlung des IP-Paketes aufgebaut werden.

Im allgemeinen ist eine IP-Adresse eines Rechners einem Kommunikationspuffer in diesem Rechner zuzuordnen. Dieser Kommunikationspuffer kann als Zugangsport zu der IP-Protokollinstanz im Rechner gesehen werden. Somit befindet sich dieser Kommunikationspuffer an der Grenze zwischen den Protokollen TCP und IP, nämlich an der Grenze zwischen den Schichten 3 und 4 im logischen Schichtenmodell des Endsystems.. Im allgemeinen ist der Transport eines IP-Pakets vom Rechner A mit der IP-Adresse x zum Rechner B mit der IP-Adresse y als Übermittlung dieses Pakets vom Kommunikationspuffer x im Rechner A zum Kommunikationspuffer y im Rechner B zu interpretieren.

Es besteht die IP-Kommunikation in der Übergabe eines IP-Pakets von Kommunikationspuffer x im Quellrechner mit der MAC-Adresse a zum Kommunikationspuffer y im Zielrechner mit der MAC-Adresse b. Diese Kommunikationspuffer repräsentieren entsprechend Quell- und Ziel-IP-Adressen. Der Quellrechner muss die MAC-Adresse, d.h. die physikalische LAN-Adresse des Zielrechners, im zu sendenden MAC-Frame setzen. Hierfür muss eine Tabelle mit folgenden Zuordnungen vorhanden sein: IP-Adresse zu MAC-Adresse Die Pflege dieser Tabelle gehört zur Aufgabe des Protokolls ARP (Address Resolution Protocol). Das ARP-Protokoll bietet somit einen dynamischen Mechanismus zur Ermittlung der MAC-Adresse des IP-Peerpartners. Wenn ein Übermittlungsnetz verbindungsorientiert ist (z.B. X.25-, Frame-Adressen Relay-, ATM-Netz oder ISDN), muss der Quellrechner die physikalische Adresse des Zielrechners auch kennen, um die gewünschte Verbindung aufzubauen. Hierfür muss eine Tabelle mit den folgenden Zuordnungen vorhanden sein: IP-Adresse zu Netzadresse (z. B. ATM-, X.25-Adresse)

Die Bestimmung von physikalischen Adressen in verbindungsorientierten Netzen muss anders als in verbindungslosen LANs gelöst werden. Da das Protokoll ARP aus der TPC/IP-Protokollfamilie als APR-Request einen MAC-Broadcast generiert, kann es in verbindungsorientierten Netzen nicht eingesetzt werden. Um dieses Problem zu lösen, wird oft eine Tabelle mit den Zuordnungen von physikalischen Adressen zu IP-Adressen in einem zentralen Server zur Verfügung gestellt. Ein solcher Server wird für die Adressauflösung oft als ARP-Server bezeichnet.
Liegt ein IP-Paket in einem Rechner an einem verbindungsorientierten Netz zum Senden vor, so kann dieser Quellrechner die gesuchte physikalische Zieladresse beim ARP-Server abfragen und für die weitere zukünftige Verwendung bei sich speichern. In großen verbindungsorientierten Netzen werden in der Regel mehrere ARP-Server implementiert. Die einzelnen ARP-Server müssen miteinander u.a. die Zuordnungen IP-Adresse zu Netzadresse nach einem Protokoll austauschen können. Die Kommunikation zwischen den einzelnen ARP-Servern erfolgt nach dem Protokoll NHRP (Next Hop Resolution Protocol).

Wenn sich der Zielrechner in einem anderen Subnetz befindet, wird das IP-Paket an den Router zur Weiterleitung abgegeben. Wir betrachten die Übermittlung eines IP-Pakets in verbundenen verbindungsorientierten Subnetzen. In diesem Fall wird zunächst eine Verbindung über das erste Subnetz zum Router aufgebaut; anschließend baut der Router eine Verbindung über das zweite Subnetz zum Zielrechner auf.
Die hier dargestellten verbindungsorientierten Subnetze können zwei Teile eines physikalischen Netzes (z.B. eines ATM-Netzes) darstellen. Werden mehrere verbindungsorientierte Subnetze miteinander vernetzt, so können sich mehrere Router auf dem Datenpfad zwischen den kommunizierenden Rechnern, die zu unterschiedlichen Subnetzen gehören, befinden. In einem solchen Fall entstehen große Verzögerungen auf den Ende-zu-Ende-Verbindungen. Da jedes verbindungsorientierte Netz die Switching-Funktion (Vermittlungsfunktion) enthält, versucht man, um dieses Problem in den Griff zu bekommen, Switching und Routing in einem Netz entsprechend zu integrieren. Ein solcher Einsatz in ATM-Netzen ist unter dem Begriff MPOA (Multi-Protocol over ATM) bekannt

**Network Address Translation (NAT)**

Häufig besteht die Notwendigkeit, aus Sicherheitsgründen ein Intranet komplett vom Internet abzuschotten, so dass die innere Struktur des Intranets nicht nach außen bekannt gegeben wird. Dieses Verhalten wird als Network Address Translation bzw. Private Address Translation (NAT/PAT) bezeichnet und ist auch unter dem Begriff IP-Masquerading bekannt. NAT/PAT kann interpretiert werden als eine semi-permeable Verbindung zwischen Intranet und Internet.

Zwei Fälle sind zu unterscheiden:

- Intranet zu Internet:
  Der NAT-Router zwischen beiden Netzen nimmt eine Umsetzung der IPAdressen in den Paketen (bzw. auch in den ICMP- und ggf. SNMP-Mitteilungen) vor. Dies bedingt zusätzlich eine Neuberechung der IP-Header Checksumme. In der Regel lassen sich hierdurch nur Dienste, die über eine feste (Well-Known) Portnummer verfügen, zwischen Intranet und Internet abwickeln, wie z. B. FTP, TELNET und HTTP.
- Internet zu Intranet:
  Das Intranet tritt lediglich durch den NAT-Router auf. IP-Ziel und Dienste im Intranet lassen sich daher nur durch den Einsatz geeigneter Applikations-Gateways erreichen.

Der Router verwaltet eine NAT-Tabelle, in der die Zuweisung von privaten und öffentlichen IP-Adressen abgespeichert ist. Diese Tabellen können statisch oder dynamisch sein. In einer statischen Tabelle wird jeder internen IP-Adresse eine öffentliche fest zugeordnet. Dagegen wird in einer statischen Tabelle eine öffentliche IP-Adresse aus einem Pool bei Bedarf einer internen Adresse zugewiesen.

Je nach dem, wie viele öffentliche IP-Adressen dem ganzen IP-Netz zur Verfügung stehen, sind in der Regel folgende Systemlösungen zu unterscheiden:

- **Systemlösungen n:m**
  In diesem Fall stehen m öffentliche IP-Adressen dem privaten IP-Netz mit n Rechnern zur Verfügung, so dass bis zu m Kommunikationsvorgänge nach außen gleichzeitig unterstützt werden können. Dies ist die ähnliche Situation, die bei den privaten Telefonanlagen mit m Amtsleitungen vorkommt, wo nur m Verbindungen nach außen gleichzeitig möglich sind.
- **Systemlösungen n:1**
  Dem privaten IP-Netz steht nur eine öffentliche IP-Adresse zur Verfügung. Hier muss der Router also alle privaten IP-Adressen auf eine einzige, öffentliche IP-Adresse abbilden. Um dies zu erreichen, werden die nach außen abgehenden Kommunikationsvorgänge mit Hilfe der Nummer des Quell-Ports identifiziert.

Die Nummer des Zielports bestimmt normalerweise den Dienst auf dem Zielrechner und wird weltweit eindeutig festgelegt (Well-Known Port). Dagegen ist die Nummer des Quell-Ports frei wählbar und bestimmt den Port, an den die Antwort zurückgeliefert werden soll. Die Nummer des Quell-Ports wird vom Router neu vergeben und dient anschließend zur Identifikation der "abgehenden" Kommunikationsvorgänge. Für diese spezielle Form von NAT hat sich ein fester Begriff etabliert. Viele Hersteller sprechen davon, dass sie NAT mit dem sogenannten Single User Account Feature (SUA) unterstützen.

## Adressierung im Internet mit IPv6

**Adressstruktur von IPv6**

Bereits Anfang der 90er Jahre war festzustellen, dass der auf dem Protokoll IPv4 basierende Adressraum bei dem weiteren rapiden Internet-Wachstum bald zu knapp sein würde. Einer der Hauptgründe, ein neues IP-Protokoll zu entwickeln, war die Erweiterung der Adressierung. Die Adresslänge in IPv6 wird auf das Vielfache - jeweils 128 Bits für Quell- und Zieladresse - im Vergleich zu der Adresslänge 32 Bits beim IP4 erweitert. Somit sind $2^{32}$ Adressen beim IPv6 verfügbar. Dies bedeutet die Vergrößerung des Adressraums um den Faktor 2 Ähnlich wie beim Protokoll IP4 identifiziert eine IP-Adresse nicht eine ganze Station, sondern deren Interface als ein physikalischer Port (Netzanschluss). Beispielsweise werden einer Station, die an zwei Netzen (DualHoming) "angeschlossen" ist, zwei IP-Adressen zugeteilt.

Im allgemeinen wird zwischen folgenden Kategorien von IPv6-Adressen unterschieden:

- Unicast
- Multicast
- Anycast

Die Unicast-Adressen werden für die Unterstützung von Punkt-zu-Punkt-Verbindungen verwendet. Somit repräsentiert dieser Typ die häufigste Adressierungsart, bei der ein Quellsystem die Daten an ein direkt angegebenes Zielsystem sendet. Eine Unicast-Adresse identifiziert einen Interface in einer Station.

Eine Multicast-Adresse identifiziert eine Gruppe von Interfaces. Ein Paket mit einer Multicast-Adresse wird an die Interfaces aller Stationen einer Gruppe direkt übermittelt.

Eine Anycast-Adresse identifiziert ebenfalls eine Gruppe von Stationen, genauer gesagt eine Gruppe von Prozessen. Der Unterschied zwischen Multicast- und Anycast-Adressen besteht in der Übermittlung von Paketen. Die Anycast-Adressen ermöglichen den Versand von Paketen über eine festgelegte Stelle an alle Stationen aus einer Gruppe. Ein Paket mit einer AnycastAdresse wird zuerst an eine Station aus der Gruppe (z.B. einen speziellen dedizierten -Router) übergeben, die im nächsten Schritt das empfangene Paket an die weiteren Stationen aus dieser Gruppe verteilt. Die AnycastAdressen unterstützen also eine Art der Verteilung der Pakete und erlauben, unterschiedliche Rechner zu einer funktionellen Gruppe zusammenzufassen.

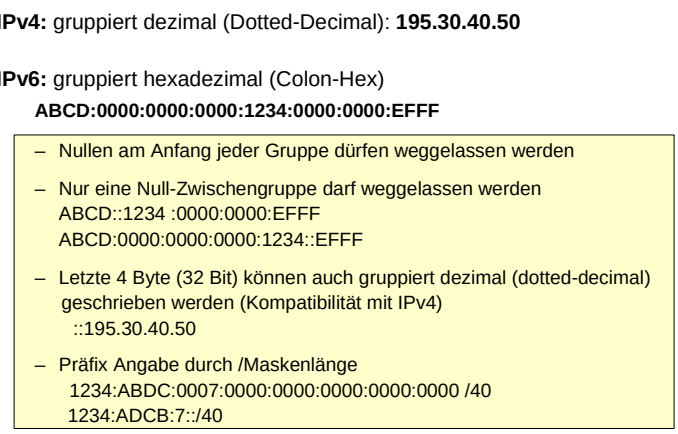



Bild: IP-Adressendarstellung

**Darstellung von IPv6-Adressen**

Die IPv6-Adressen haben im allgemeinen folgende Form:
X:X:X:X:X:X:X:X
wobei jedes X-Zeichen einen 16-Bit-Wert in hexadezimaler Schreibweise darstellt. Eine IPv6-Adresse kann also folgendermaßen aussehen
ADCF:0005:0000:0000:0000:0000:0600:FEDC
Die führenden Nullen können weggelassen werden. Somit ist es erlaubt, z.B.
0 statt 0000 5 statt 0005 600 statt 0600
zu schreiben. Hierdurch lässt sich die bereits erwähnte Adresse nun in der gekürzten Form
ADCF:5:0:0:0:0:600:FEDC
darstellen.

Ebenso können mehrere aufeinanderfolgende Null-Werte unterdrückt und durch "::" abgekürzt werden. Eine korrekte Schreibweise für die eben gezeigte Adresse wäre damit auch:
ADCF:5::600:FEDC

**Volle Darstellung**
ADCF:BA56:600:FEDC:0:0:0:0
0:0:0:0:ADCF:BA56:600:FEDC
0:0:0:ADCF:BA56:0:0:0

**Vereinfachte Darstellung**
ADCF:BA56:600:FEDC::
::ADCF:BA56:600:FEDC
::ADCF:BA56:0:0:0 oder
0:0:0:ADCF:BA56::

Das Symbol "::" darf nur an einer Seite der Adresse verwendet werden. Die Darstellung

::ADCF:BA56:: als 0:0:0:ADCF:BA56:0:0:0

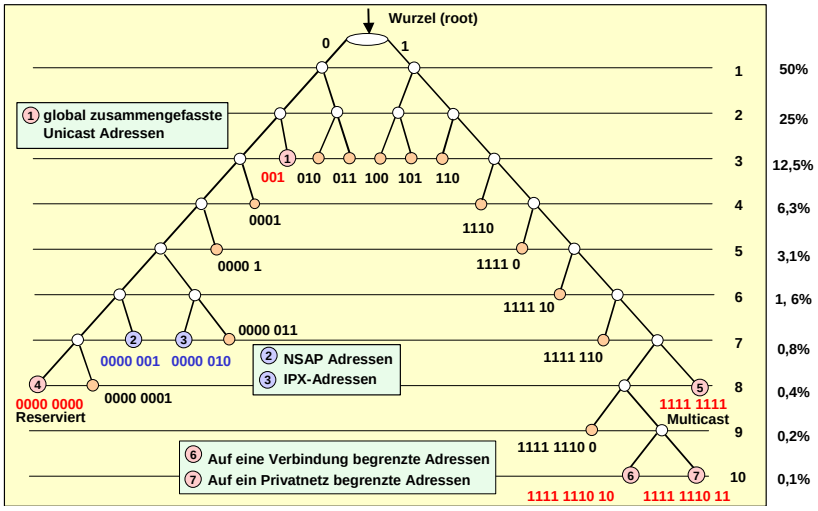
ist nicht eindeutig.

- **128 Bit (feste Länge)**
- $2^{128}$ = 3.4×$10^{38}$ Adressen ⇒ 665*$10^{21}$ Adressen pro $m^2$ der Erdoberfläche
- 128 Bit anstatt 32 Bit
  ⇒ 340 282 366 920 938 463 463 374 607 431 768 211 456 (3*$10^{38}$) Hosts
  ⇒ 665 570 793 348 866 943 898 599 Hosts pro $m^2$ der Erdoberfläche
- Bei einer Adresszuweisungsrate von $10^6$ /µs, würde es 20 Jahre dauern

- 32 Bit ⇒ 4×$10^9$ Hosts (durch die Klasseneinteilung sind nicht alle Adressen vorhanden)
- Hierarchische Zuweisung ⇒ verschnitt wie in der Telefonie
- Erwartete Ausnutzungsgrad von 8*$10^{17}$ bis 2*$10^{33}$ Adressen
- 8*$10^{17}$ ⇒ 1 564 Adressen pro $m^2$ der Erdoberfläche
- 85% noch nicht zugeordnet

- mehrere Schnittstellen (Interfaces) pro Host und mehrere Adressen pro Schnittstelle
- Unicast, Multicast, Anycast
- Adressenzuweisung: Provider-basierend, lokal pro Netzbereich, lokal pro Anschluss

Bild: Anzahl IPv6-Adressen




Im Gegensatz zur einfachen Unterteilung von Adressen nach Klassen A bis E in Netzen beim IPv4-Einsatz ist die Unterscheidung von Adresstypen beim Protokoll IPv6 sehr flexibel und somit aufwendiger. Um welchen Adresstyp es sich handelt, bestimmt ein sogenannter Formatpräfix, der eine variable Länge besitzt und durch die ersten (von links gelesen) Bits bestimmt wird. Durch den Präfix-Einsatz kann der ganze Adressraum auf bestimmte Adressklassen aufgeteilt werden.

Bild: IPv6: Binäre Präfixwerten

### Autfteilung des IPv6-Adressraums

Während IPv4-Adressen in verschiedene Netzklassen A, B, C etc. unterteilt werden, gibt es bei IPv6-Adressen eine derartige statische Trennung von Netz- und Host-ID nicht. Das Protokoll IPv6 nutzt flexiblere Adresstypen. Um welchen Adresstyp es sich handelt, wird in den führenden Bits der Adresse als Format Präfix hinterlegt. Mit dessen Hilfe lassen sich bestimmte Spezialadressen kennzeichnen, wie z.B. Multicast, Aggregatable Global, Link Local Use, Site Local Use etc. Die allgemeine Architektur der Adressierung im Protokoll IPv6 ist in RFC 2373 fest-, gelegt.

Beim Protokoll IPv6 ist im allgemeinen zwischen

- Unicast-Adressen und
- Multicast-Adressen

zu unterscheiden. Zwei Unicast-Adressen legen eine Punkt-zu-Punkt Verbindung fest, so dass dieser Typ von Adressen am häufigsten verwendet wird. Eine Unicast-Adresse identifiziert eindeutig einen physikalischen Anschlussport (Interface) in einer Station. Ist eine Systemkomponente (z.B. ein Server bzw. ein Router) über mehrere Netze erreichbar, d.h. wird sie an mehreren Netzen angeschlossen, muss jedem Anschlussport eine Unicast-Adresse zugeteilt werden. Enthält eine Systemkomponente zwei Adressen, wird sie als Dual-Homing bezeichnet.

Es werden auch einige Adressformate reserviert, um die anderen bekannten Adressen in die IPv6-Adressen einbetten zu können. Hierzu gehören die IPv6-Adressen für die Übertragung:

- von NSAP-Adressen, d.h. OSI-Adressen (Prefix 0000 001),
- von IPX-Adressen (Prefix 0000 010).

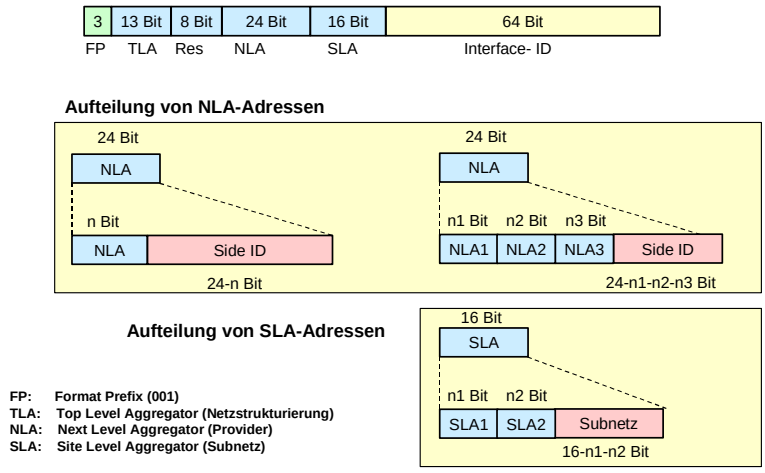



Bild: IPv6-Adressstruktur

**Unicast-Adressen von IPv6**

Unter den Unicast-Adressen sind wiederum folgende Klassen zu unterscheiden:

- Provider Based Global Unicast Addresses: Diese Klasse von Adressen werden für normale Punkt-zu-Punkt-Kommunikation verwendet und unterscheidet sich von anderen Adressen durch das Präfix 010. Ein Achtel des Adressraums wird für diese Klasse eingeräumt und dem Präfix nur 3 Bits zugeordnet. Die Struktur dieser Klassen von Unicast-Adressen wird im Dokument RFC 2078 festgelegt.
- Aggregatable Global Unicast Addresses: Diese aggregierbaren globalen Unicast-Adressen unterscheiden sich von anderen Adressen durch das Präfix 001 und sind auch für normale Punktzu-Punkt-Verbindungen vorgesehen. Diese Klasse von Adressen wird in RFC 2374 beschrieben.
- Adressen von lokaler Bedeutung: Hierbei werden zwei Arten definiert:
  - Link Local Use Unicast Addresses,
  - Site Local Use Unicast Addresses.

Diese Adressen können nur ohne Internet-Anbindung verwendet werden.

- Spezielle Unicast-Adressen: Zu dieser Klasse gehören vor allem:
  - IPv4-kompatible IPv6-Adressen und
  - IPv4-mapped IPv6-Adressen.

Diese Adressen werden für die Kommunikation zwischen den Endsystemen mit dem klassischen Protokoll IP4 und den Endsystemen mit dem neuen Protokoll IPv6 verwendet. Diese speziellen Adressen sind von großer Bedeutung bei der Migration zum IPv6-Einsatz, insbesondere wenn die beiden Protokolle in einem Netz implementiert werden.

Die einzelnen Typen von Unicast-Adressen werden nun näher dargestellt.

**Provider-basierte globale Unicast-Adressen**

Eines der größten Probleme beim Protokoll IPv4 ist der Umfang von Routing-Tabellen in großen Netzen und die damit verbundenen Leistungseinbußen. Dies ergibt sich aus der klassenbasierten Aufteilung der InternetAdressen nach dem Protokoll IPv4, was durch die Einführung des Classless Inter Domain Routing (CIDR) jedoch abgemildert werden konnte. Bei diesen Adressen wird der ganze Adressraum direkt auf die einzelnen Netze aufgeteilt, ohne irgendwelche Verweise auf die Lokation der Netze auf der Erdkugel zu geben.

Die IPv4-Adressen haben den Nachteil, dass sie keine Hierarchie in dem Hierarchien Sinne bilden, dass es möglich wäre, auf die Lokation eines Netzes auf der Erdkugel zu verweisen. Durch eine mehrstufige Strukturierung von Adressen und Bildung einer Hierarchie von Subnetzen lässt sich das Wachsen von Routing-Tabellen noch in akzeptierten Grenzen halten und damit auch die Verzögerung der Pakete in Routern.

Dem eben geschilderten Problem versucht man im Protokoll IPv6 durch eine hierarchische Strukturierung von Adressen entgegenzukommen. In diesem Zusammenhang wurden zuerst sogenannte Provider-basierte (Anbieter-basierte) Unicast-Adressen (Provider Based Unicast Addresses) im RFC 2073 definiert.

Die Provider-basierten Unicast-Adressen werden von anderen Klassen von Adressen durch das Präfix 010 unterschieden. Diese Adressen werden in erster Linie von den jeweiligen internationalen Organisationen verwaltet. Registry-ID (kurz Reg-ID) bezieht sich auf die internationale "Registrierungs"-Organisation, bei der diese Adresse registriert wird.

Beispielsweise gelten zur Zeit. folgende Reg-ID-Zuweisungen:

- Reg-ID = 10000: ICAN (Internet Corporation for Assigned Names and Numbers - http://www.icann.org/),
- Reg-ID = 01000: RIPE (Reseau IP European, Regional Internet Registryfor Europe - http://www.ripe.net/),
- Reg-ID = 11000: InterNIC (Internet Information Center),
- Reg-ID = 00 100: APNIC (Asia Pacific Internet Information Center).

Durch die n-Bit-Angabe im Feld Provider-ID wird der Anbieter der Internet-Dienste identifiziert. Die Länge der Provider-ID kann variabel sein. Dadurch kann jede der bereits erwähnten internationalen Organisationen Provider-IDs von beliebiger Länge zulassen und auf diese Art und Weise verschiedene Klassen von Anbietern bilden. Wird eine kurze Provider-ID (n klein) einem großen weltweit agierenden Anbieter zugewiesen, so kann er eine große Anzahl von Netzbetreibern mit Subscriber-ID (56-n Bits) definieren. Eine Subscriber-ID stellt die Identifikation des Betreibers eines privaten Netzes dar und ist mit der Netz-ID bei der IPv4-Adresse zu vergleichen.

Eine internationale Organisation für die Registrierung von IPv6-Adressen kann mehrere nationale Organisationen mit den Adressen versorgen. Eine internationale Organisation kann mehrere nationale Organisationen für die Vergabe von Adressen koordinieren. Diese nationalen Organisationen werden mit National-Registry-ID) identifiziert.

Die letzten 64 Bits jeder Adresse werden als Intra-Subscriber bezeichnet und definieren die interne Netzstraktur bei einem Netzbetreiber. Für die Identifikation der Subnetze dient Subnet-ID. Die letzten 48-Bits als Interface-ID ermöglichen es, die Endsysteme in einem Subnetz zu identifizieren.

An dieser Stelle ist darauf hinzuweisen, dass man beim Protokoll IPv6 von Interface-ID statt Host-ID spricht. Die Interface-ID in der IPv6-Adresse entspricht vollkommen der Host-ID in der IPv4-Adresse. Ist ein Endsystem an unterschiedliche Netze (WANs bzw. LANs) angeschlossen, so hat es mehrere physikalische Ports und somit auch mehrere Interface-lDs. Ein Interface-ID ist somit als eine physikalische Netzadresse zu interpretieren.

Die öffentliche Struktur der Adresse beschreiben die Teile: Registry-ID, National Registry-ID und Provider-ID. Diese Angaben ermöglichen, im Gegensatz zur IPv4-Adresse, eine Provider-basierte globale IPv6-Adresse auf der Erdkugel Jast" zu lokalisieren. Durch die Lokalisierung von Adressen ist u.a. das weltweit hierarchische Routing möglich, so dass die IPv6-Pakete oft über die von vornherein bekannten internationalen Routen transportiert werden können.

An dieser Stelle ist eine Besonderheit von IPv4-Adressen hervorzuheben: Die Interface-ID repräsentiert eine Netzadresse eines Ports im Endsystem und enthält 48 Bits. Jede physikalische Adresse in Shared Medium LANs (d.h. jede MAC-Adresse) ist ebenfalls 48 Bits lang. Im Feld Interface-ID kann eine MAC-Adresse eingebettet werden.

Somit weist jede IPv6-Adresse zwei wichtige Besonderheiten auf

- sie ist weltweit eindeutig,
- sie enthält die physikalische Netzadresse des Endsystems.

Im Gegensatz zu den IPv4-Adressen ist in den IPv6-Adressen die Zuordnung IPv6-Adresse zu MAC-Adresse enthalten - der große Vorteil von IPv6-Adressen (möglicherweise aber auch ihr größter Nachteil). Aus diesem Grund ist das Hilfsprotokoll ARP beim Protokoll IPv6 nicht notwendig, was auch bestimmte Auswirkungen auf die Funktionsweise von IPv6-Routem hat.

Da IPv6-Adressen die physikalische Netzadresse bereits enthalten, ist eine automatische Adresskonfiguration (sog. Stateless Autoconfiguration) möglich.

**Aggregierbare globale Unicast-Adressen**

Eine zweite Klasse von IPv6-Adressen für die Punkt-zu-Punkt-Kommunikation bilden sogenannte aggregierbare globale Unicast-Adressen (Aggregatable Global Unicast Addresses). Diese Adressen werden im Internet-Standard RFC 2374 festgelegt und sollten die Provider-basierten globalen Adressen ersetzen. Im folgenden werden sie kurz AG-Unicast-Adressen (AG: Aggregierbar Global) genannt..

Beim Entwurf von AG-Unicast-Adressen wurde davon ausgegangen, dass die gesamte Internet-Welt organisatorisch gesehen eine hierarchische Aggregation Struktur aufweist. An der Spitze dieser Hierarchie (Top Level) stehen internationale und nationale Organisationen wie z.B. Anbieter der Netz- bzw. Internet-Dienste. Der ganze Raum von AG-Unicast-Adressen wird zunächst auf jene Top-Level-Organisationen aufgeteilt, die als internationale Verwaltungen von IPv6-Adressen fungieren. Hierfür dient die Angabe TLA-ID (Top Level Aggregation Identifier) in den AG-Unicast-Adressen. Die TLA-ID in den AG-Unicast-Adressen entsprechen vollkommen der Registry-ID in den Provider-basierten Unicast-Adressen.

Die nächste Stufe (Next Level) in dieser Hierarchie bilden weitere Organisationen, die einerseits als Verwaltungen von IPv6-Adressen bzw. als Anbieter der Netz- und Internet-Dienste fungieren können. Diese Organisationen können ebenfalls in einer Hierarchie zueinander stehen. Auf der letzten Stufe stehen individuelle Institutionen als "Endbenutzer" der Internetdienste. Die eben geschilderte Hierarchie im Bereich der Internet-"Welt" findet in den AG-Unicast-Adressen ihre Berücksichtigung.

Die einzelnen Angaben in den AG-Unicast-Adressen haben hier folgende Bedeutung:

- Format Präfix: Die Bitkombination 001 dient den AG-Unicast-Adressen als Identifikation und ermöglicht, diesen Adresstyp von anderen Adresstypen zu unterscheiden.
- NLA-ID (Next Level Aggregation Identifier): Eine Top-Level-Organisation mit einem Identifikator TLA-ID kann ihren Adressraum an die weiteren Organisationen der "nächsten" Hierarchiestufe mit Hilfe des Identifikators NLA-ID aufteilen. Der NLA-ID kann weiter strukturiert werden, so dass sich die hierarchische Struktur zwischen den einzelnen Organisationen in den Adressen abbilden lässt. Diese Struktur stellt quasi eine öffentliche Struktur innerhalb der Internet-Welt dar.
- SLA-ID (Site Level Aggregation Identifier): An dieser Stelle wird die Identifikation einer individuellen Organisation (eines Kunden) als Endbenutzer angegeben. Der SLA-ID-Inhalt kann weiter hierarchisch strukturiert, um eine Subnetz-Hierarchie innerhalb eines physikalischen großen Netzes adressieren zu können. Man kann hier von einer privaten Struktur sprechen.
- Interface-ID (Interface Identifier): Dieses Feld enthält den Identifikator eines physikalischen Ports in einem Endsystem, einen Router etc. Im allgemeinen ist die Interface-ID als eine physikalische (auch sog. Link-) Netzadresse eines Ports in einem Endsystem zu interpretieren.

Der Adressraum einer Top-Level-Organisation TLA-ID kann mit dem Identifikator TLA-ID auf Teil-Adressräume von weiteren (z.B. nationalen) Organisationen aufgeteilt werden. Mit einem Identifikator NLA-ID kann entweder eine Organisation oder eine hierarchische Struktur von Organisationen identifiziert werden. Im allgemeinen können die Angaben NLA-ID und SLA-ID weiter strukturiert werden. Durch die Strukturierung der N-LA-ID lässt sich eine weitgehende Hierarchie innerhalb der öffentlichen Struktur aufstellen. Durch die weitere Strukturierung der SLA-ID lässt sich die Netzstruktur eines Netzbetreibers hierarchisch strukturieren.

Der NLA-ID kann als einen Adressraum mit der Länge von 24 Bits weiter strukturiert werden, um eine hierarchische Struktur von Organisationen in Adressen zu berücksichtigen. Aufgrund der so strukturierten globalen Adressen lässt sich Routing in großen Level-Netzen vereinfachen.

Hat eine Next-Level-Organisation $A_i$ (z.B. eine nationale Organisation) von der Top-Level-Organisation mit TLA-ID eine Identifikation NLA-ID erhalten, so kann diese Organisation $A_i$ für sich die ersten m Bits vom NLA-ID als eigener Identifikator NLADI-ID reservieren. Das restliche 24-m Bits lange Feld, Site-ID, stellt einen Adressraum dar, der wiederum aufgeteilt werden kann. Somit können weitere Organisationen (Institutionen, Provider) $B_j$, j = l, 2, .... sich den (24-m)-Bit-langen Adressraum teilen. Jede dieser Organisationen kann wiederum einen Identifikator NLA2-ID mit n Bits für sich festlegen und die restlichen 24-m-n Bits als Adressraum an weitere Organisationen $C_k$, k = l, 2, ... zur Verfügung stellen. Diese Organisation $C_k$ kann einen o Bits langen Identifikator NLA2-ID) als eigene "Vorwahl" nutzen und die restlichen 24-m-n-o Bits als Adressraum für individuelle Organisationen bzw. Unternehmen nutzen.

Es lässt sich auf die gleiche Weise auch das Feld NLA-ID strukturieren. Private Netzstrukturen können somit auf Grundlage der Identifikator Site-ID im Feld NLA-ID gekennzeichnet und hierarchisch adressiert werden.

Eine Organisation in ihrer weltweit verteilten Netzstruktur kann die Komponenten effektiv adressieren. Hierfür nutzt sie das Feld SLA-ID als einen eigenen Adressraum. Mit dem Identifikator SLA1-ID kann sie die Standorte auf den einzelnen Kontinenten kennzeichnen. Der Rest als Subnet-ID kann wiederum in SLA2-ID) und Subnet-ID aufgeteilt werden. Der Identifikator SLA2-ID) kann dem Standort innerhalb eines Landes zugeteilt werden. Das Feld Subnet-ID ermöglicht es, die einzelnen Subnetze innerhalb eines Landes zu identifizieren.

Man kann sich auch andere Beispiele für die SLA-ID-Aufteilung vorstellen. Handelt es sich um eine Netzstruktur innerhalb eines Standortes, wie dies häufig der Fall sein wird, so setzt sich diese Netzstruktur aus den Teilnetzen innerhalb einzelner Gebäude zusammen. Ein Teilnetz in einem Gebäude enthält einige Subnetze, wie z.B. Etagennetze bzw. virtuelle LANs. Um die Komponenten innerhalb einer solchen Netzstruktur effektiv zu identifizieren, kann das Feld NLA-ID einer Adresse ähnlich aufgeteilt werden. Dies würde weitgehend der Subnetzbildung beim Protokoll IPv4 entsprechen.

Wie hier geschildert wurde, lässt sich jede AG-Unicast-Adresse mehrstufig strukturieren. Dadurch lassen sich sowohl große als auch kleine Organisationen bzw. Anbieter der Internet-Dienste definieren.

**Globale Unicast IPv6-Adressen und MAC-Adressen in LANs**

Beim Routing von IPv6-Pakete in IPv4-Netze ist folgendes Problem zu lösen: Der letzte Router auf einem Datenpfad erhält ein IP-Paket, das zu einem Endsystem im LAN weitergeleitet werden soll, aber im IP-Paket ist nur Ziel-IP-Adresse enthalten. Der Router (als der letzte unterwegs) muss ins LAN den vollständigen MAC-Frarne mit der Ziel-MAC-Adresse abschikken. Um die richtige Ziel-MAC-Adresse (d.h. physikalische Host-Adresse) zu ermitteln, nutzt der Router das Hilfsprotokoll ARP (Address Resolution Protocol). Dieses Protokoll hat die Aufgabe, die Zuordnung: Ziel-IP-Adresse zu Ziel-MAC-Adresse zu bestimmen.

Auf die Funktion des Hilfsprotokolls ARP könnte man verzichten, wenn eine Protokolladresse den Bezug zur entsprechenden physikalischen Adresse hätte. Dieser Ansatz wird bei den globalen Unicast-IPv6-Adressen verfolgt. Hier wird eine MAC-

Adresse im Feld Interface-ID eingebettet. Damit lässt sich die MAC-Adresse als physikalische LAN-Adresse aus der IPv6-Protokolladresse direkt ableiten, so dass man auf das Protokoll ARP beim IPv6 vollkommen verzichten kann.

Beim Einkapseln ins Feld Interface-ID wird die MAC-Adresse aufgeteilt. Der erste Teil Hersteller-ID (Company-ID) wird direkt nach dem Feld SLA-ID untergebracht danach folgen zwei Füll-Bytes mit den Bitkombinationen x'FF' und x'FE', und anschließend wird die Manufacturer-Selected Extension ID eingetragen.

**Unicast-Adressen von lokaler Bedeutung**

Wie bereits erwähnt, werden zwei Arten von Unicast-Adressen für lokale Nutzung definiert:
- Link Local Use Unicast Addresses
- Site Local Use Unicast Addresses

Es handelt sich bei Link Local Use Unicast Addresse (kurz LLU-Unicast-Adresse) um eine unstrukturierte Adresse. Da die LLU-Unicast-Adressen keine Identifikation von Subnetzen enthalten, können sie nur innerhalb isolierter IPv6-Subnetze verwendet werden. Die LLU-Unicast-Adressen dürfen von Routern nicht weitergeleitet werden, z.B. können sie nicht ins Internet geschickt werden.

Site Local Use Unicast Addresses (kurz SLU-Unicast-Adressen) sind strukturiert. Da die SLU-Unicast-Adressen keine weitere Identifikation höherer Hierarchie als Subnetz-IDs enthalten, können sie nur innerhalb einer Gruppe von IPv6-Subnetzen innerhalb eines isolierten Standorts (Site) verwendet werden. Die SLU-Unicast-Adressen ermöglichen, innerhalb einer nicht an das globale Internet angeschlossenen Organisation eindeutige Adressen zu vergeben, ohne dafür global eindeutige Adressen verwenden zu müssen. Die SLU-UnicastAdressen sind nur innerhalb einer Organisation eindeutig und dürfen von Routern nach außen (z.B. ins Internet) nicht weitergeleitet werden.

**Spezielle Unicast-Adressen von IPv6**

Beim IPv6 werden einige spezielle Unicast-Adressen eingeführt. Es handelt sich hierbei um:
- unspezifizierte Adressen (Unspecified Addresses),
- Loopback-Addressen,
- IPv6-Adressen mit eingekapselten IPv4-Adressen.

Diese unspezifizierte Adresse ist 0:0:0:0:0:0:0:0 (oder einfach "::") und kann z.B. als Absenderadresse eines Endsystems verwendet werden, dem die Adresse(n) noch nicht zugeteilt wurde(n). Dies ist z.B. der Fall, wenn ein Endsystem ein IP-Paket sendet, damit es die eigene IP-Adresse erfährt.

Die Loopback-Adresse ist 0:0:0:0:0:0:0:1 (oder einfach "::1") und wird in IP-Paketen genutzt, die zwischen den Programmen innerhalb eines Rechner (z.B. beim Testen) ausgetauscht werden. Diese Adresse kann weder Quell- noch Zieladresse von Paketen sein, die ein Endsystem bzw. einen Router verlassen.

Es werden zwei Arten von IPv6-Adressen mit eingekapselten IPv4- Adressen unterschieden:
- IPv4-kompatible IPv6-Adressen
- IPv4-mapped IPv6-Adressen

Diese Unicast-Adressen werden als IPv4-basierte Adressen bezeichnet.

Wie hier zu sehen ist, ergänzen die beiden Adresstypen eine 32-Bit-lange alte" IPv4-Adresse zu der vollen Länge der IPv6-Adresse. Diese Adresstypen werden mit Hilfe des 80-Bit-langen Präfixes 000 ... 0 identifiziert. Die nächsten 16-Bits ermöglichen es, diese beiden Adresstypen voneinander zu unterscheiden. Diese IPv4-basierten IPv6-Adressen werden bei der Migration zum IPv6-Einsatz verwenden, d.h. in Netzen, in denen die Systemkomponenten mit dem Protokoll entweder IPv4 oder IM bzw. mit den beiden Protokollen IP4 und IPv6 betrieben werden.

**Multicast- und Anycast-Adressen**

Eine Multicast-Adresse identifiziert eine Gruppe von Systemen. Ein Paket, das an eine Multicast-Adresse gesendet werden soll, wird normalerweise an alle Systeme der Gruppe gesendet. Beim IPv6 gibt es keine BroadcastAdressen. Diese Funktion wird durch Multicast-Adressen erfüllt. Die Broadcast-Adresse entspricht somit der "All-Nodes"-Multicast-Adresse.

Die einzelnen Angaben haben hier folgende Bedeutung:
- Präfix: Die Bitkombination 1111 1111 deutet auf eine Multicast-Adresse hin.
- Flags: Die ersten drei Bits sind zur Zeit reserviert und müssen auf 0 gesetzt werden. Das Bit T hat folgende Bedeutung:
  - T = 0: eine ständig zugeordnete (d.h. well-known) Multicast-Adresse,
  - T = 0: eine temporär zugeordnete Multicast-Adresse.
- Scope (Gültigkeitsbereich): Hier wird der Gültigkeitsbereich eines Multicast-Paketes angegeben.
- Group-ID (Gruppen-ID): Dieses Feld kennzeichnet unabhängig vom Scope-Wert ob es sich bei der Multicast-Adresse um eine permanente oder um eine nur vorübergehend gültige Adresse handelt.

Multicast-Adressen dürfen nicht als Quell-Adressen erscheinen.

## Adressierung im Internet (Email-Adresse, Adressauflösung, DNS, URL)

**Adressauflösung**
Da im Ablauf eines Kommunikationsvorgangs mehrere OSI-Schichten beteiligt sind, werden auch die Adressen dieser Schichten benötigt. Beim Übergang zwischen Schichten müssen demzufolge Adressen ineinander abgebildet werden, dieser Vorgang wird als **Adressauflösung** (address resolution) bezeichnet. Auf den höheren Schichten wird dies durch Verzeichnisdienste geleistet. Die Abbildung von Netzadressen in Hardwareadressen wird durch ARP (Address Resolution Protocol realisiert.

**Adresszuweisung**
Die einem Endsystem zugewiesene Adresse muss diesem mitgeteilt werden. Dafür gibt es grundsätzlich drei Möglichkeiten:

- Die Adresse wird **im Endsystem gespeichert.** Dies kann per Hardware (Schalter, PROM) oder Software (Festplatte) geschehen. Im einfachsten Fall erfolgt die Zuweisung lokal und manuell.
- Die Adresse wird in einem LAN-Server gespeichert und dem Endsystem auf Anfrage bzw. beim Booten mitgeteilt. Dies ist bei Endsystemen ohne permanente Speicher (Festplatte) sinnvoll, aber auch für die zentrale Konfiguration der Adressen (und weiterer kommunikationsrelevanter Informationen) über ein LAN. Hierfür sind BOOTP und DHCP verwendbar. PPP ermöglicht ebenfalls eine Adresszuweisung.
- Die Adresse muss nicht explizit mitgeteilt werden. Damit kann ein beliebiges Endgerät an das Netz angeschlossen und sofort genutzt werden (plug and play). Dies trifft für die MAC-Adresse von Ethernet-Adaptern zu, die nach IEEE 802 eindeutig einem bestimmten Adapter zugeordnet ist. Vorstellbar ist auch ein Verfahren, das eine noch nicht benutzte Adresse ermittelt und einem neuen Endsystem zuweist.

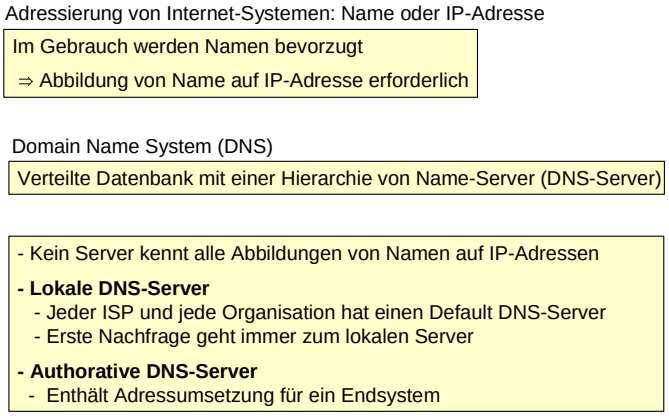



Bild: Namensdienst: Domain Name System (DNS)

**Domain Name System**

Bei der bisherigen Darstellung der Kommunikationsprinzipien in TCP/IP-Netzen wurde unterstellt, dass die IP-Adresse des Partners gegeben ist. Dies ist aber normalerweise nicht der Fall. Beim Aufruf einer WWW-Seite wird diese in Form eines sog. Uniform Resource Locators (URL) angesprochen. Teil dieser URL-Adresse ist der Name des Rechners (und der Domäne), der als WWW-Server dient. Um Rechnernamen in IP-Adressen zu konvertieren, wurde das Domain Name System (DNS) entwickelt, das ein weltweit verteiltes Verzeichnis von Internet-Namen darstellt.

Das DNS ist so ausgelegt, dass sich die Benutzer die IP-Adressen von Rechnern nicht merken müssen, sondern statt dessen deren Namen verwenden können, um entfernte Rechner in TCP/IP-Netzen zu lokalisieren und um diese Verbindungen herzustellen. Obwohl das DNS eigentlich für das Internet entwickelt wurde, lässt es sich auch in privaten TCP/IP-basierten Netzen einsetzen, wobei auch eine Ankoppelung an das Internet möglich ist.

Vor der Implementation von DNS wurde die Zuordnung von IP-Adressen zu den Namen in einer zentralen Host-Tabelle (auch Host-Datei genannt) abgespeichert. Jede Host-Tabelle enthält eine Liste mit Host-Namen (Namen von Rechnern bzw. von anderen TCP/IP-Endsystemen) mit deren IP-Adressen. Mit dem ständigen Zuwachs an Rechnern in einem Netz und durch Integration einer immer größeren Zahl von Netzen in größeren Netzen wurde deutlich, dass die Errnittlung von IP-Adressen über zentrale Host-Tabellen keine richtige Lösung mehr ist. In einem großen Netz kann die Namensvergabe nicht den Entscheidungen der einzelnen Benutzer überlassen werden. Ein großes Netz wäre dann kaum noch zu verwalten. Das

primäre DNS-Ziel war es, die Host-Tabellen durch eine verteilte und vernetzte Datenbank zu ersetzen. Mit der DNS-Hilfe ist es möglich, die Host-Namen - im gesamten Internet sowie in den privaten TCP/IP-basierten Netzen - so zu verwalten, dass sie weltweit eindeutig sind.

**Ermittlung von Ziel-IP-Adressen**

Ein DNS-System wird durch die Interaktion von zwei Komponenten implementiert:

- Resolver und
- Name-Server.

Das DNS funktioniert nach dem Client/Server-Prinzip. Der Resolver ist die Client-Software auf dem Rechner eines Benutzers, die DNS-Server abfragt, um Rechnernamen in IP-Adressen zu übersetzen. Der DNS-Server ist ein Programm in einem dedizierten Rechner, das auf eine Datei mit Host-Namen und ihren zugehörigen IP-Adressen zugreift, um die entsprechenden Anfragen des Resolvers zu beantworten. Somit sind Resolver Clients, die auf Name-Server zugreifen.

Mittels Name-Server Referrals ermittelt der Resolve einer Ziel-IP-Adresse über folgende Schritte:

1. Die Anwendung im Quellrechner (hier z.B. WVW- Browser) leitet eine Abfrage (Query) an den Resolver.
2. Der Resolver leitet die Abfrage an den lokalen Name-Server 1 weiter.

   Jeder Name-Server verfügt über eine Datenbank, in der u.a. die Zuordnungen Host-Name zu IP-Adresse enthalten sind. Es handelt sich hierbei nur um die Zuordnungen vom Host in einer Domain (Domäne), für die dieser Name-Server autorisiert ist. Ein Server kann ebenfalls über einen Cache verfügen, in dem er u.a. auch die Zuordnungen Host-Name zu IP-Adresse über eine festgelegte Zeit (z.B. 2 Tage) speichert. Diese Zuordnungen betreffen aber die "fremden" Hosts, die sich außerhalb seiner Domain befinden. Diese Zuordnungen repräsentieren einfach die Ergebnisse von früheren Abfragen. Antworten aus seinem Cache kennzeichnet der Name-Server als "not-authoritive Answer".

   a) Der lokale Name-Server findet die gesuchte Zuordnung Host-Name zu IP-Adresse weder in seiner eigenen Datenbank noch im Cache, so dass er diese Abfrage an einen übergeordneten Name-Server 2 weiterleitet.
   b) Name-Server 2 verweist den Name-Server 1 auf andere Name-Server, hier auf den Name-Server 3 im Zielnetz 2.
   c) Der lokale Name-Server 1 richtet die Abfrage an Name-Server 3 im Zielnetz.
   d) Name-Server 3 sendet die gesuchte Zuordnung.
3. Der lokale Name-Server 1 sendet die gesuchte Zuordnung an den Resolver im Rechner X. Der Resolver speichert diese Information in seinem Cache für eine eventuelle zukünftigen Nachfrage ab.
4. In diesem Schritt wird die gesuchte IP-Adresse der Anwendung übergeben.

In der Literatur wird diese Resolver-Variante auch als Full Resolver bezeichnet und steht W.R. als separates Programm mit dem Namen nslookup zur Verfügung. Die Resolver-Funktion ist allerdings heute meist in der Anwendung integriert. Sämtliche Namen, die in unterschiedlichen und weltweit verteilten Name Servern gespeichert sind, bilden einen sogenannten DNS-Namensraum. Nun wollen wir die Strukturierung dieses weltweit verteilten Namensraums darstellen.

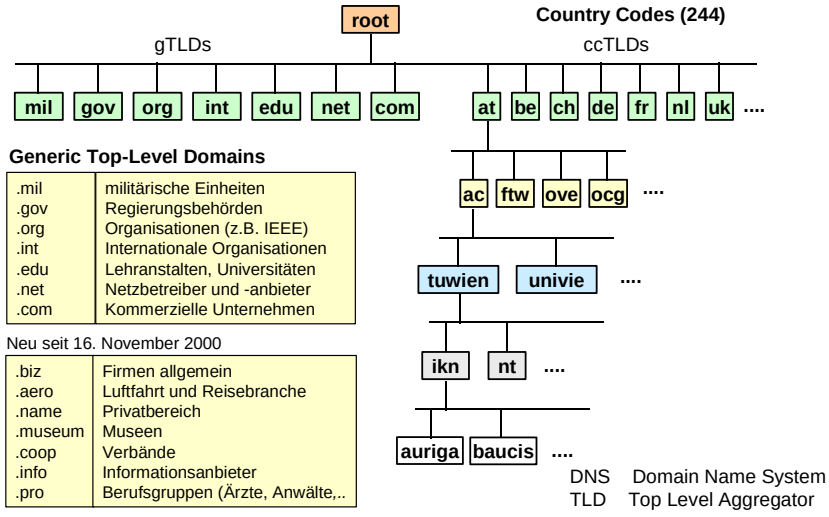



Bild: DNS hierarchische Namenstruktur

**Aufbau des DNS-Namensraums**

Bei DNS handelt es sich um eine baumförmige weltweite Vernetzung einzelner Name-Server, die eine weltweit verteilte Datenbank bilden. Sie wird auch als DNS-Datenbank bezeichnet. Jedes Datenelement in einer verteilten DNS-Datenbank ist über einen Namen indiziert. Diese Namen sind im Grunde genommen nur Pfade in einem großen Baum. Dieser Baum besitzt ganz oben eine einzige Wurzel (Root), die man einfach "Root" nennt. Genau wie bei jedem anderen Dateisystem kann der DNS-Baum mehrere Abzweigungen haben, die als Knoten (nodes) dargestellt werden.

Jeder Knoten des Baumes repräsentiert eine Domain (Domäne) und stellt einen Teil der gesamten Datenbank dar, also wie ein Verzeichnis in einem Dateisystem. Jede Domain (sowie jedes Verzeichnis) kann in weitere Teile untergliedert werden. Diese Teile werden im DNS als Subdomains bezeichnet und entsprechen den Unterverzeichnissen eines Dateisystems. Eine Subdomain wird, genau wie ein Unterverzeichnis, als Unterknoten (Sohn) des übergeordneten Knotens (Vater) interpretiert. Jeder Knoten des Baumes wird mit einem einfachen Namen versehen. Dieser Name kann bis zu 63 Zeichen lang sein. Dabei ist für die Root der Name „.“ reserviert.

Der vollständige Domain-Name im Baum (Full Qualified Domain Name) FQDN besteht aus den Namen einzelner Knoten bis zur Root. Dies bedeutet, dass der Name eines Knoten sich aus den einzelnen Namen im Pfad zusammensetzt, wobei diese einzelnen Namen durch einen Punkt voneinander getrennt werden. Z.B. setzt sich der Domain-Name Ih-fulda.de aus den Namen fh-fulda und de zusammen. Der FQDN eines Knotens kann so interpretiert werden, dass er drei Bestandteile beinhaltet:

- den Hostnamen (bzw. dessen Alias-Namen),
- den Domain-Namen (einschließlich evtl. Subdomänen) und
- das Domain-Suffix.

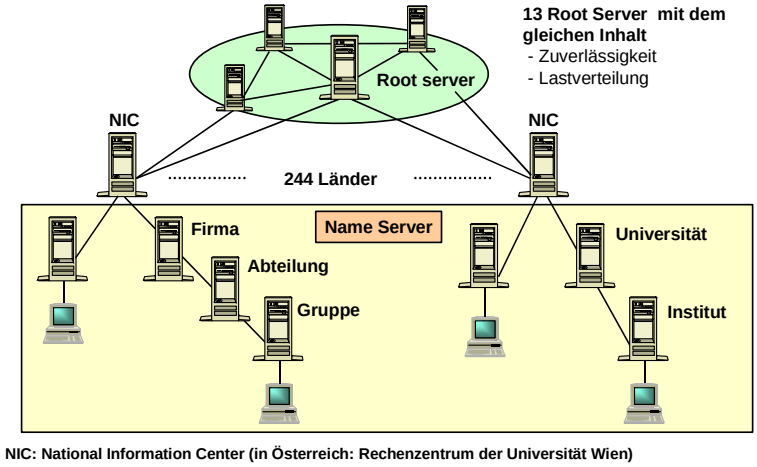



Bild: Domain Server System Hierarchie

Eines der Hauptziele beim Entwurf von DNS war die Dezentralisierung der Administration. Dieses Ziel wird durch sogenannte Delegierung erreicht. Das Delegieren von Domains funktioniert so ähnlich wie das Delegieren in der Arbeit. Ein Projektleiter kann ein großes Projekt in kleinere Aufgaben unterteilen und die Verantwortung für jede dieser Teilaufgaben an verschiedene Mitarbeiter übergeben (delegieren). Auf die gleiche Weise -kann eine Organisation, die eine Domain administriert, diese in Subdomains aufteilen. Jede dieser Subdomains kann an andere Organisationen delegiert werden. Dies bedeutet, dass die Organisation, der die Verantwortung dieser Domain übertragen wurde, für die Pflege aller Daten der Subdomain verantwortlich ist. Die Daten der Subdomain können unabhängig geändert und sogar in weitere Subdomains aufgeteilt werden, die sich dann wieder weiterdelegieren lassen. Die übergeordnete Domain enthält nur Zeiger auf die Quellen mit den Daten der Subdomain, so dass Anfragen entsprechend weitergeleitet werden können.

Die oberste Ebene des DNS-Namensraums wird vom InterNIC (Internet Network Information Center) verwaltet. Das InterNIC übergibt die Verantwortung sowohl an öffentliche Organisationen als auch an private Unternehmen für die Verwaltung von deren Domains im DNS-Namensraum. Die Organisationen und Unternehmen setzen DNS-Server zum Verwalten der Namenzuordnungen zu IP-Adressen von Rechnern und anderen Endsystemen in deren Domains ein.

Die oberste Ebene des Domain-Namensraums wird in drei Hauptgruppen unterteilt:

- Domains von Organisationen: dreistelliger Name, der die Hauptfunktion bzw. -Aktivität der Organisation in der Domain angibt. Die meisten Organisationen in den USA sind in einer solchen Domain vertreten.
- Geographische Domains Durch ISO 3166 festgelegte zweistellige Länderkennzeichen.
- arpa-Domain, eine besondere Domain mit dem Namen in-addr.arpa wurde für die Zuordnung von IP-Adressen zu Rechnernamen eingerichtet.

Die Organisationen und Unternehmen, denen das InterNIC einen Bereich des Domain-Namensraums zugewiesen hat, sind für das Benennen der Rechner und anderer Endsysteme in der ihnen zugeteilten Domain verantwortlich.

**Primary Name Server (Master)**
Datenbank mit authorisierten Daten
Datenbank Eintragungen

**Secondary Name Server (Slave)**
Datenbank mit authorisierten Daten
Aktualisierungen vom Master

**Caching Server**
Keine authorisierte Daten
Entfernung von Daten: time-to-live field (32 Bit)

Bild: DNS Server Typen

Um die Administration der Netze zu vereinfachen und sowohl Datensicherheit als auch Betriebssicherheit zu gewährleisten, können zwei Arten von Name-Server Name-Servern in einer NDS-Zone zur Verfügung gestellt werden, nämlich:

- Primäre (primary) Name-Server und
- sekundäre (secondary) Name-Server.

Ein primärer Name-Server erhält die Daten für die Zonen, über die er die Autorität besitzt, aus Dateien, die auf dem Host liegen, auf dem der Server läuft. Die Dateien, aus denen der primäre Name-Server seine Zonendaten liest, werden Zonendateien genannt. Bei Änderungen an den Zonendaten, z.B. durch Hinzufügen von Hosts zur Zone, müssen diese Änderungen auf dem primären Name-Server vorgenommen werden, so dass die neuen Daten in die lokale Zonendatei eingetragen werden.

Ein sekundärer Name-Server erhält seine Zonendaten von einem primären Name-Server. Beim Start stellt der sekundäre Name-Server den Kontakt mit dem primären Name-Server her, um seine Zonendaten zu aktualisieren. Dieser Vorgang wird als Zonentransfer bezeichnet. Während eines Zonentransfers sendet der primäre Name-Server eine Kopie der Zonendatei an den sekundären Name-Server.

Generell sollte man den primären und den sekundären Name-Server in verschiedenen Subnetzen installieren, damit die DNS-Namensabfragen auch dann unterstützt werden können, wenn ein Subnetz ausfällt.

Aufbau

- Hierarchie von Name-Server, dadurch Skalierbarkeit gegeben
- Kein Name-Server verfügt über die kompletten Daten

Typen von Name-Server

- **Lokale Name-Server**
  z.B. ISP, Universität, Firma etc. besitzt lokalen Name-Server
- **Root-Server**
  einige wenige solche Server existieren weltweit
- **Authorisierte Name-Server**
  Jedes System ist bei einem solchen Server registriert
  Oft geographisch mit lokalen Name-Server zusammen

Für jede Hierarchiestufe (= Domäne) gilt

- Sie besitzt die Authorität zur Namensvergabe innerhalb dieser Domäne
- Sie verfügt über Name-Server, die für die nächst tiefere Ebene zuständig sind
- Ein Root-Server ist bekannt

Bild: Name-Server

Root Server enthalten nur Einträge für TLDs
(generische und Länder TLDs)

**Allgemein:**

- jeder Nameserver enthält nur die Einträge für die er verantwortlich ist (authorative)
- darüberhinaus auch noch zwischengespeicherte Einträge von vorhergehenden Anfragen
- Timeout legt fest wie lange Einträge zwischengespeichert werden (typisch mehrere Tage)

Bild: Root Server and Registrierung von TLDs

Lokation der DNS Root-Server
http://www.wia.org/

Weltweit gibt es 13 Root-Server

**Aufgaben**

- Kontaktiert Authorative Name Server, falls Adressumsetzung unbekannt
- Gibt Adressumsetzung dem lokalen Name- Server bekannt

Bild: Verteiltes Netz von DNS Root-Server

ARIN
American Registry for Internet Numbers
Chantilly, VA, USA

RIPE
Réseaux IP Européens
Amsterdam, The Netherlands

APNIC
Asia Pacific Network Information Centre
Milton, Brisbane, Australia

Bild: Registrierung von NLAs

**DNS-Zonen und Name-Server**

Ein Name-Server stellt einen dedizierten Rechner dar, in dem die Informationen (als Ressource Records) über den Domain-Namensraum gespeichert werden. Ganz allgemein enthalten Name-Server vollständige Informationen über einen Teil des Domain-Namensraums. Dieser Teil wird Zone genannt und man sagt, dass der Name-Server "die Autorität" über die Zone besitzt. Die Name-Server können auch die Autorität über mehrere Zonen besitzen.

Der Unterschied zwischen einer Zone und einer Domain besteht darin, dass der Name-Server einer Zone nur solche Namen und Daten einer Domain enthält, die in ihre Subdomains nicht delegiert wurden. Somit handelt es sich bei einer Zone nur um einen Bereich einer DNS-Domain. In kleinen Unternehmen kann eine Zone die gesamte Domain umfassen. Die DNS-Server können in der (Root)-Domain, der Zone und den Subdomains eines TCP/IP-Netzs installiert werden, also überall dort, wo ein DNS-Server zum Verwalten der DNS-Daten sowie des Datenverkehrs aufgrund von DNS-Namensabfragen benötigt wird.

Das Aufteilen einer Domain in Zonen und Subdomains hat den Vorteil, Verwaltungsaufgaben den verschiedenen organisatorischen Gruppen zuordnen zu können. Bei der DNS-Server-Datenbank handelt es sich um einen Satz von Dateien, die die Zuordnungen der Host-Namen zu den IP-Adressen sowie andere DNS-Informationsdaten für die Rechner in einem TCP/IP-Netz enthalten.

**Prinzip der Namensauflösung**

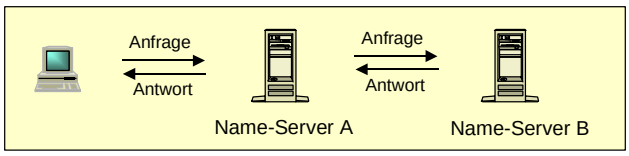
Die Name-Server gehen bei der Gewinnung von Daten aus dem DNS-Namensraum äußerst geschickt vor. Sie können nicht nur die notwendigen Informationen aus Zonen liefern, über die sie, die Autorität besitzen, sondern auch den DNS-Namensraum nach Daten absuchen, für die sie nicht verantwortlich sind. Dieser Prozeß wird als Namensauflösung (name resolution) oder einfach nur als Auflösung (resolution) bezeichnet.

Weil der Namensraum wie ein auf den Kopf gestellter Baum strukturiert ist, kann ein Name-Server eine Abfrage nach jedem beliebigen Namen im NDS-Namensraum an einen Root-Name-Server richten, der ihm dann den Weg weisen wird.

Der Root-Name-Server weiß, wo die einzelnen Top-Level-Domains Name-Server zu finden sind. Für jede Abfrage auf einen beliebigen DomainNamen hin kann der Root-Name-Server zumindest die Namen und Adressen des Naine-Servers zurückgeben, der für die Top-Level-Domain die Verantwortung trägt, in der dieser Domain-Name liegt. Diese Top-Level-NameServer können eine Liste von Name-Servern zurückgeben, die für die Second-Level-Domain verantwortlich sind. Jeder abgefragte Name-Server liefert genaue Angaben darüber, wie man der gesuchten Information näher kommt**,** oder erteilt selbst die gewünschte Antwort.

Die Root-Name-Server sind für die Auflösung sehr wichtig. Würden alle Root-Name-Server im Internet für eine längere Zeit nicht erreichbar sein, wäre auch jegliche Auflösung von Namen unmöglich. Um sich hiervor zu schützen, besitzt das Internet mehrere Root-Narne-Server die über verschiedene Teile des Netzes weltweit verteilt sind.

**Rekursive Anfrage**




**Iterative Anfrage**

Kann in jeder Stufe der Abfragekette angewandt werden

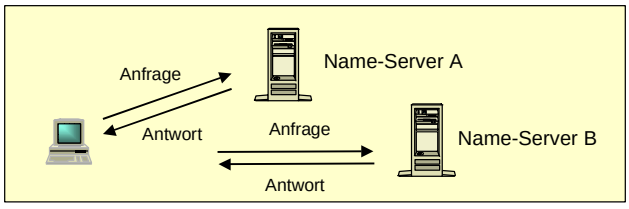



Bild: Typen von DNS-Anfragen

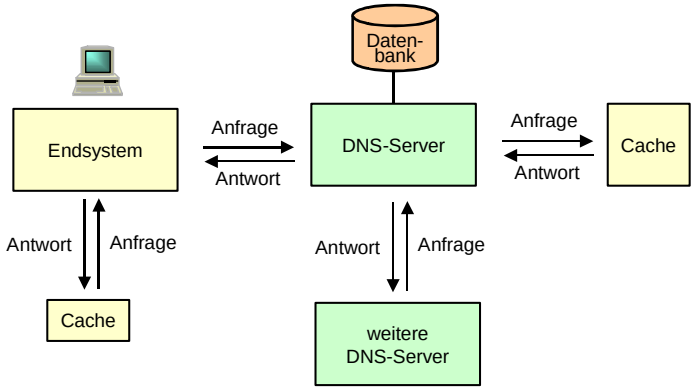



Bild: Domain Server System Abfrage

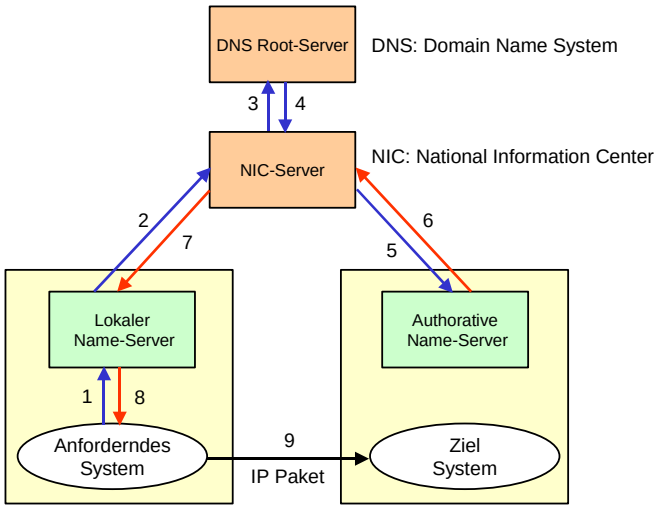



Bild: Allgemeiner Ablauf einer DNS-Abfrage

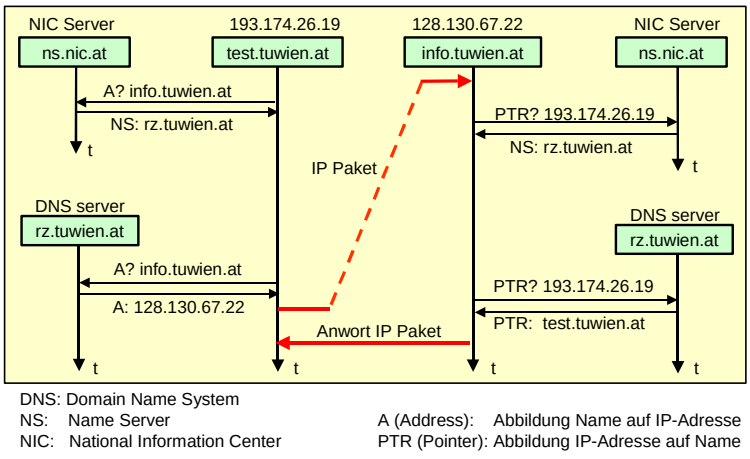



Bild: Beispiel einer DNS Anfrage

**Struktur von DNS-Nachrichten**

Bei den "normalen" Abfragen verwendet das DNS das verbindungslose Protokoll UDP. Für die Datenübermittlung zwischen einem primären und einem sekundären Name-Server in einer Domain (Zonentransfer) wird eine TCP-Verbindung aufgebaut.

Anschließend werden die DNS-Nachrichten als TCP-Segmente transportiert. Bei den beiden Protokollen UDP und TCP wird dem DNS die Port-Nummer 67 zugeordnet.

Jede DNS-Nachricht setzt sich aus einigen Teilen, die als Sektionen (Sections) bezeichnet werden, zusammen. Die einzelnen Teile umfassen:

- Header Section: Dieser Teil stellt den eigentlichen Header der Nachricht dar. Er enthält 12 Bytes (3 * 4 Bytes).
- Question Section (Abfrage-Sektion): Diese Sektion enthält Felder, die eine Abfrage an den Name-Server spezifizieren, d.h. dieser Teil gibt an, was gesucht wird.
- Answer Section (Antwort-Sektion): Dieser Teil enthält die Antwort eines Name-Servers in Form sogenannter RRs (Ressourcen-Einträgen, Resource Records).
- Authority Section (Autoritäts-Sektion): Diese Sektion enthält RRs eines autorisierten Servers.
- Additional Information Section (Zusätzliche Informationen): Dieser Teil enthält zusätzliche Angaben, die irgendwie zu einer Abfrage bzw. Antwort gehören.

Der Header ist immer vorhanden. Er enthält Felder, die angeben, welche anderen Sektionen vorhanden sind, und legt auch fest, wie eine DNS-Nachricht zu interpretieren ist. Die einzelnen Angaben im Header einer DNSNachricht haben folgende Bedeutung:

- Identifikation (2 Bytes): Hier wird die Identifikation der Anwendung angegeben, die diese Abfrage (Query) initiiert hat. Diese Angabe wird beim Name-Server in dessen Antwort kopiert, so dass der Resolver (Full Resolver) die empfangene Antwort der "richtigen" Anwendung zuordnen kann.
- Parameters: Hier wird u.a. angegeben, ob eine DNS-Nachricht eine Abfrage oder eine Antwort darstellt. Zusätzlich wird auch angegeben, ob es sich um eine normale Abfrage oder eine inverse Abfrage handelt. Eine inverse Abfrage bedeutet die Suche nach der Zuordnung IP-Adresse zu Host-Name? In diesem Fall ist die IP-Adresse bekannt, und es wird nach dem Host Namen gefragt.
- QDcount: Anzahl der Einträge (d.h. der RRs) in der Question Section.
- ANcount: Anzahl der RRs in der Answer Section.
- NScount: Anzahl der Naine-Server RRs in der Authority Section.
- ARcount: Anzahl der RRs in der Additional Information Section.

Die Struktur von DNS-Nachrichten ist in den RFCs 1035 und 1036 beschrieben.

**Auflösung von IP-Adressen auf Host-Namen**

Oft kommt es vor, dass ein Benutzer nur über die IP-Adresse eines Rechners verfügt, jedoch den der entsprechenden IP-Adresse zugeordneten HostNamen benötigt. In diesem Fall wird nach der Zuordnung IP-Adresse zu Host-Name gefragt. Die Abbildung von Adressen auf Namen wird benutzt, um Ausgaben zu erzeugen, die für den Anwender einfacher zu lesen und zu interpretieren sind (beispielsweise in Logdateien). Darüber hinaus wird dieses Verfahren auch bei der Fehlerbehebung in TCP/IP-Netzen angewendet.

Zur Verwaltung der Zuordnungen von IP-Adressen zu Host-Namen durch DNS-Server wurde eine besondere Domain in-addr.arpa durch InterNIC eingerichtet. Beim Eintragen der Zuordnungen von IP-Adressen zu Host-Namen werden diese Knotennummern entsprechend belegt. Da die Hierarchien von IP-Adressen und Host-Namen "umgekehrt" sind, muss dies die Organisation der Domain in-addr.arpa berücksichtigen.

Die Knoten der Domain in-addr.arpa sind nach den Zahlen in der für IP-Adressen übliche Repräsentation benannt. Die Domain in-addr.arpa kann beispielsweise bis zu 256 Subdomains besitzen, von denen jede einzelne einem möglichen Wert des letzten Bytes einer IP-Adresse entspricht. Jede dieser Subdomains kann wiederum 256 Subdomains aufweisen, die jeweils wiederum mit jedem möglichen Wert des zweiten (von rechts) Byte von IP-Adressen übereinstimmen. Schließlich werden - auf der vierten Unterteilungsstufe - den Knoten die entsprechenden Resource Records zugeteilt, die den vollen Host-Namen (FQDN) der jeweiligen IP-Adresse aufweisen.

Wenn ein lokales Netz an das Internet angeschlossen wird, so sollte man dieses Netz in der Domain in-addr.arpa eintragen lassen, um die Abbildung von IP-Adressen auf Host-Namen zu ermöglichen. Hierfür ist ein Forrnular nötig, das per E-mail (hostmaster@iniernic.net) von InterNIC angefordert werden kann.

**Name-Server und Internet-Anbindung**

Heutzutage werden private Netze oft mit dem Internet verbunden, um auf die externen Ressourcen im globalen Netz zuzugreifen (z.B. WWW-Anwendungen). Dies verlangt jedoch eine sorgfältige Planung, um potentielle Sicherheitsrisiken zu vermeiden, die durch das Öffnen des privaten Netzes für "fremde" Benutzer entstehen können.

Eine häufige Schutzmaßnahme ist daher der Einsatz eines als *Firewall* bezeichneten Rechners. Unter einer Firewall versteht man einen Rechner, der nur die Ausführung bestimmter Operationen oder Programme über das Internet erlaubt. Eine Firewall-Konfiguration kann, je nach den besonderen Anforderungen des jeweiligen Unternehmens, sehr einfach oder extrem komplex sein. Hier wird versucht, zu zeigen, dass das Konzept für den DNS-Einsatz mit dem Firewall-Konzept eng zusammenhängt.

Bei einer Lösung eines Unternehmensnetzes wird das Netz in zwei logischen Teilen aufgeteilt wurde:
- interner Netzteil,
- externer Netzteil.

Der interne Netzteil enthält einen internen DNS-Server, der hauptsächlich durch die interne Kommunikation in Anspruch genommen wird. Der externe DNS-Server wird bei der Kommunikation über das Internet verwendet.

Wie hier zu sehen ist, schützt die Firewall den internen Netzteil gegen Zugriffe durch die "fremden" Benutzer vom Internet, wobei den Rechnern im internen Netzteil der Zugriff auf Ressourcen im Internet gewährt wird. Die externen Server erlauben den Rechnern außerhalb des internen Netzteils, auf durch öffentliche Dienste zur Verfügung gestellte Ressourcen zuzugreifen.
Diese externen Server müssen jedoch genau überwacht und gesichert werden, da sie direkt mit dem Internet verbunden sind und keine Zugriffskontrolle durch die Firewall ausüben. Der "Eingangs-" Router kann speziell erweitert (=> Filterfunktion für IP-Pakete) und zur Überwachung des Zugriffs von außen auf die externen Server eingesetzt werden.

Die DNS-Dienste für die externen und internen Netze sollten vollständig voneinander getrennt sein, damit die Rechner außerhalb des internen Netzteils daran gehindert werden, die Namen und IP-Adressen von im internen Netzteil befindlichen Ressourcen ausfindig zu machen. Dadurch wird sichergestellt, dass die einzigen extern verfügbaren Informationen die Namen und IP-Adressen der extemen Server (DNS- und WWW-Server) sind, die für die Bereitstellung öffentlicher Dienste des Unternehmens konfiguriert wurden.

Den Rechnern aus dem internen Netzteil, die die Ermittlung von IP-Adressen auf den Internet-Zugriff fordern, müssen normalerweise die notwendigen Interaktionen mit den DNS-Servern im öffentlichen Internet ermöglicht werden. Aus diesem Grund sollte die Fähigkeit zum Datenaustausch außerhalb des internen Unternehmensnetzes nur bestimmten DNS-Servern eingeräumt werden. Ein DNS-Server, der zur Auswertung einer DNS-Abfrage außerhalb des privaten Netzes nach entsprechenden Daten sucht, wird als Forwarder bezeichnet.

Nachdem ein externer DNS-Server als Forwarder eingerichtet wurde, sollten alle anderen DNS-Server im Netz für die Verwendung der Forwarder zur Auswertung von fremden Namen außerhalb des internen Netzes konfiguriert werden. Wenn ein Name-Server, der für die Verwendung eines Forwarders konfiguriert wurde, eine Abfrage erhält und diese anhand seiner Zonendateien nicht beantworten kann, gibt er die Abfrage an den Forwarder zurück. Daraufhin übernimmt der Forwarder die notwendigen Schritte, die zur Antwort auf diese Abfrage führen. In diesem Fall richtet er die Abfrage an einen übergeordneten Name-Server im Internet und gibt die erhaltene Antwort an den richtigen Name-Server im internen Netzteil zurück.

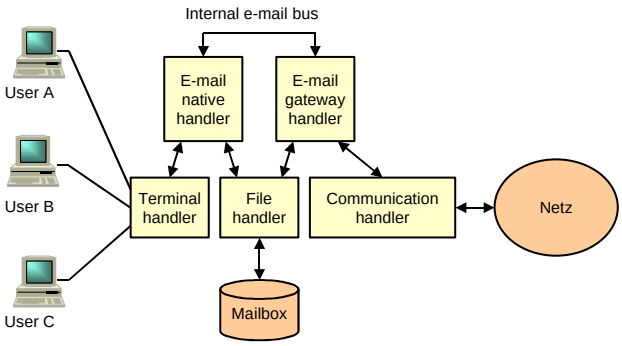



Bild: E-mail System Modell für ein Netz

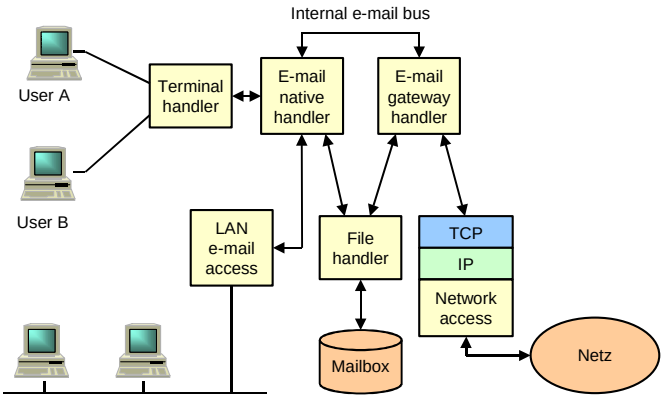



Bild: E-mail System Modell für den LAN Zugang

**Dynamische Vergabe und Ermittlung von IP-Adressen**

Durch die Vergabe von IP-Adressen können Rechner in IP-Netzen und speziell im Internet angesprochen werden. Im intuitiven Umgang sind IP-Adressen jedoch nicht sprechend genug. Es ist sinnvoll, statt einer IP-Adresse einen Rechner über seinen Namen zu adressieren. Dies kann im Prinzip durch eine statische Tabelle - die Host-Datei - erfolgen; sobald aber eine Vielzahl Rechner in entfernten IP-Netzen, d.h. speziell im Internet, erreicht werden sollen, wird die Pflege der Host-Dateien schnell unhandlich.

Um das Problem der dynamischen Namensauflösung im Internet zu lösen, wurde das Domain Name System (DNS) geschaffen. Das Domain Name System stellt eine verteilte Datenbank dar, die im Grunde genommen mit ihrem Informationsgehalt das Internet abbildet..

Entsprechend der Bedeutung des DNS für das Internet hat sich die Vergabe dynamischer IP-Adressen im Intranet entwickelt. Über das Dynamic Host Configuration Protocol (DHCP) kann eine dynamische und konsistente Vergabe von IP-Adressen und anderen wichtigen IP-Informationen für Rechner im Intranet erreicht werden. Dies wird im folgenden Abschnitt erläutert.