History of TCP/IP

1964 First book on packet networks (Kleinrock)

1968 US Department of Defence (DoD) funds the Arpanet = Advanced Research Projects Agency Network

1969 Arpanet connects 4 hosts, 50 kb/s

1972 First public Arpanet demonstration at Internat. Computer Communications Conference ICCC in Washington

1973 Ethernet

1976 The network protocol was split into TCP and IP.
Address space for 128 different networks (there were only three networks at the time)

1978 First OSI document

1982 Novell demonstrates of the first networked PC LAN at the National Computer Conference in Huston

1984 1000 internet hosts

1985 Prelude, a ATM-like cell switching system is developed at CNET
(16 byte cells, 1 byte header)

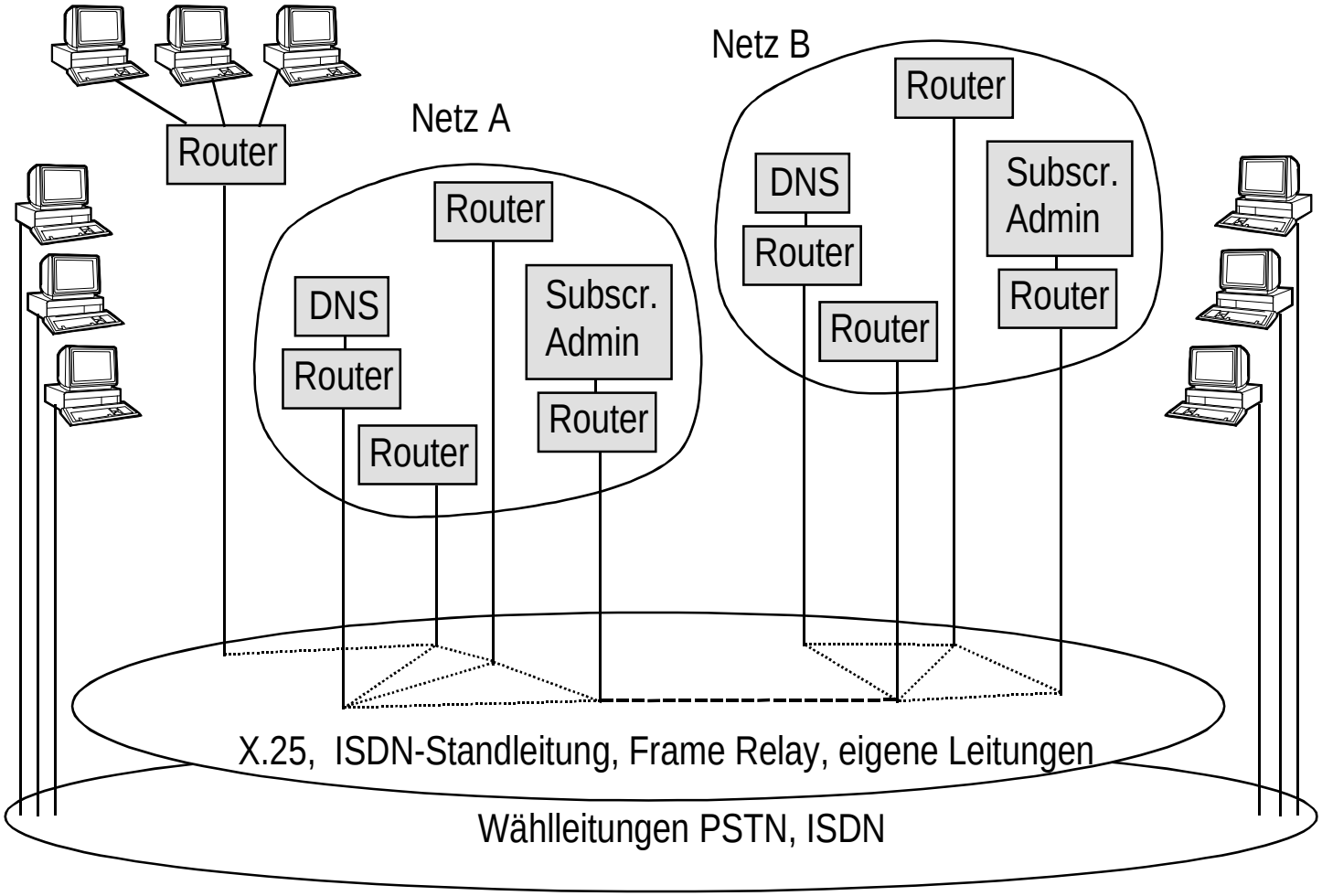
1987 Start of ATM specification in ITU-T (CCITT)

1990 first proposal for www

1992 commercial start of ATM

hosts: doubling every year (since 1989) web servers doubling every ½ year (since 1993)

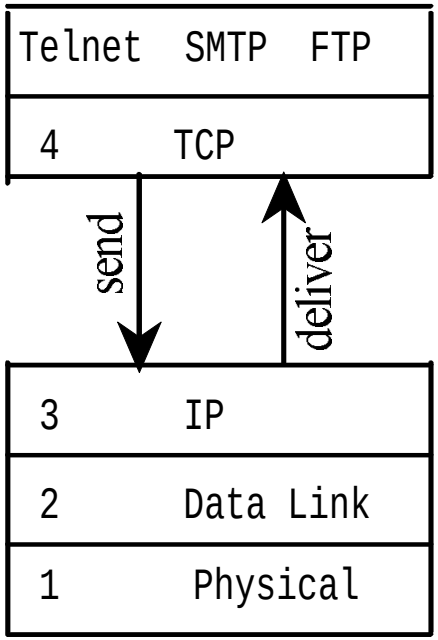
TCP/IP


Netz A
Netz B
Router
Router
DNS
Router
Subscr.
Admin
Router
Router
Router
DNS
Router
Subscr.
Admin
Router
Router
X.25, ISDN-Standleitung, Frame Relay, eigene Leitungen
Wählleitungen PSTN, ISDN

TCP/IP und OSI

Application	7	Telnet SMTP FTP
Presentation	6	
Session	5	
Transport	4	UDP TCP
Network	3	IP
Data Link	2	not defined (PPP, 802.x, X.25, FR, ATM,.HPPI,...)
Physical	1	not defined

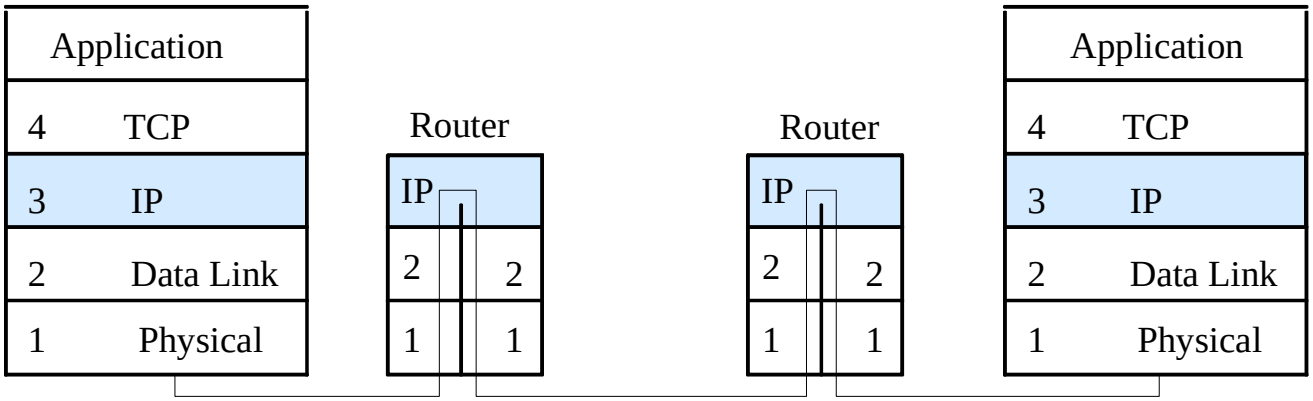
Internet Protocol IP



- Adressierungsmechanismen
- Wegewahl zwischen den Netzen
- Fehlererkennung und Statusinformation (Überlast, Paketlebenszeit)
- Definition von Übertragungsparametern (Priorität, erhöhte Sicherheit)
- Zugriffsmechanismen für niedrigere Schichten (X.25, Ethernet, FDDI, ...)

Services provided by IP:

- "Best effort delivery" datagram service
- Forwarding packets hop by hop, based on routing tables
- Fragmentation and reassembly
- No mechanisms for dealing with: lost packets, packets out of order, duplicate copies of packets



IP v4 -Protokollkopf

0 1 2 3	4 5 6 7	8 15	16 18	19 23	24 31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
TTL		Protocol	Header Checksum		
Source Address					
Destination Address					
Options (0 – 40 Bytes)					Padding

Version: die IP-Protokollversion, derzeit 4, z.T. auch schon 6

IHL: **I**nternet **H**eader **L**ength in 32-Bit-Worten; mindestens 5 Worte; kann durch Optionsfelder vergrößern werden,

Type of Service: z.B. Priorität oder Wartezeit.

Total Length: Gesamtlänge des Datagramms in Bytes; max. 64 kByte.

Identification: (z.B. ein Zähler); kennzeichnet zusammengehörige Fragmente einer Meldung

Flags: DF ("don´t fragment") und MF ("more fragments") steuern die Fragmentierung.

Fragment Offset: die Lage des Paketes relativ zum Beginn der Gesamtnachricht.

TTL (Time-to-live): jeder Netzknoten vermindert dieses Feld um mindestens 1.

Protocol: Identifikation des Transportprotokolls beim Empfänger; TCP=6, ICMP=1

Header Checksum: Kopfprüfsumme nur über den IP-Header; einfache Längsparität

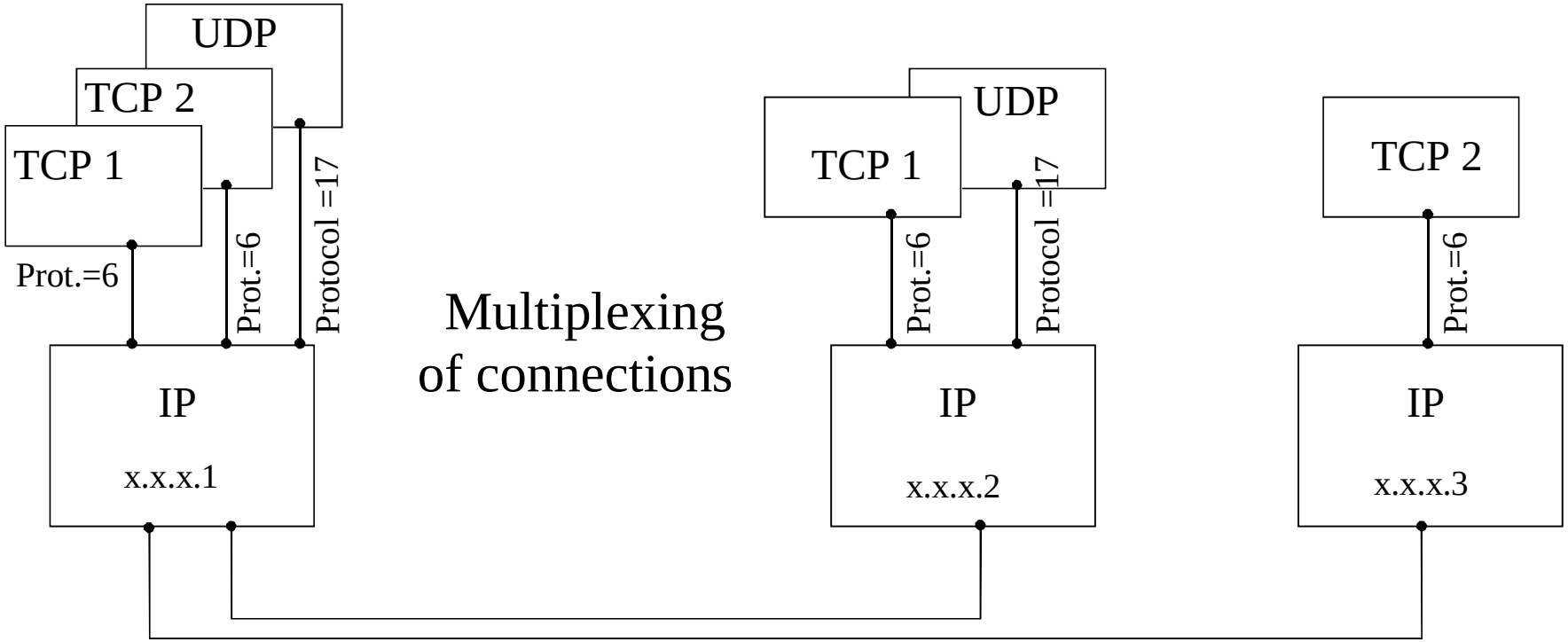
Source Address: Internet-Adresse des Quellknotens

Destination Address: Internet-Adresse des Zielknotens

Options: Für Netzwerkmanagement oder Sicherheit wird der IP-Kopf um Optionen erweitert.

Padding: Füllzeichen, damit die Länge des IP-Kopfs immer ein Vielfaches von 32 Bit ist.

Multiplexing of Connections

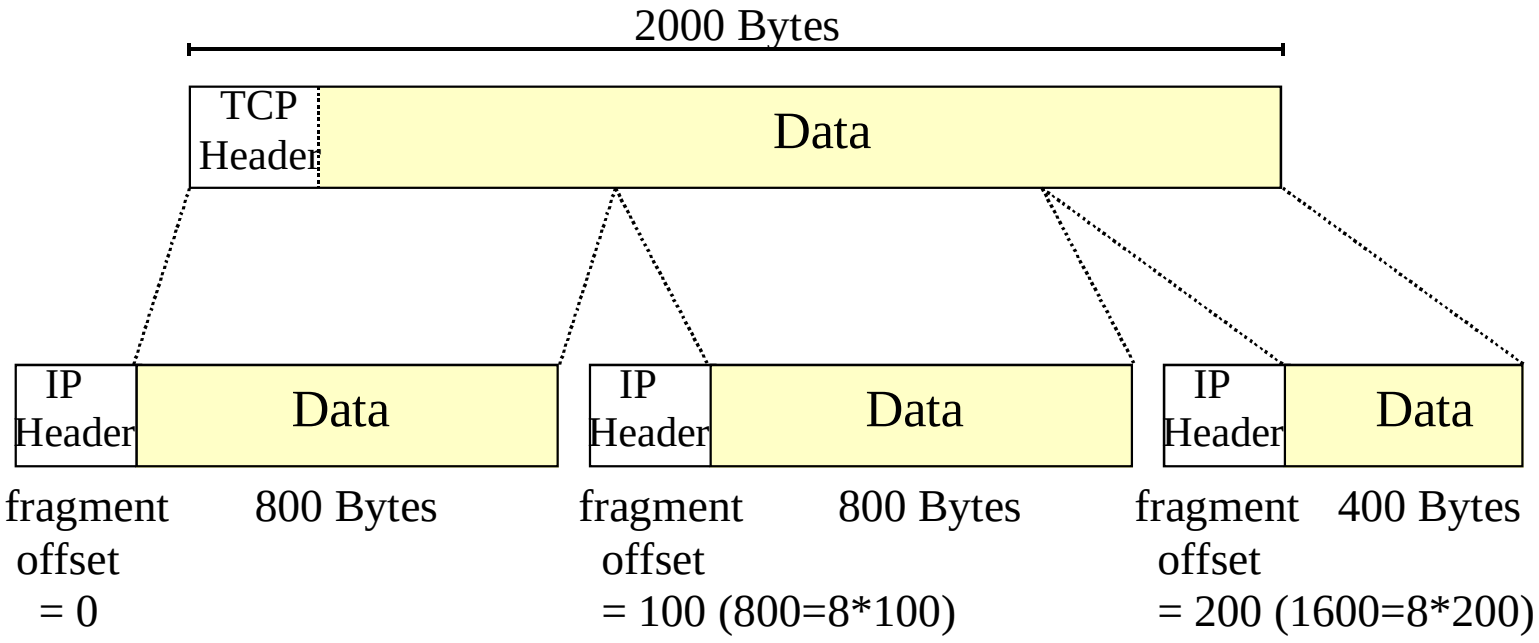


Das Feld *Protocol* unterscheidet die verschiedenen Anwendungen

1 = ICMP Internet Control Message Protocol
6 = TCP Transmission Control Protocol
17 = UDP User Datagran Protocol
2 = IGMP Internet Group Management Protocol
8 = EGP Exterior Gateway Protocol
9 = IGP any private Interior Gateway Protocol

Läuft eine Anwendung (z.B. TCP) mehrfach, dann wird die *Source Address* (IP) mit zur Unterscheidung verwendet.

Fragmentation (Segmentation / Reassembly)



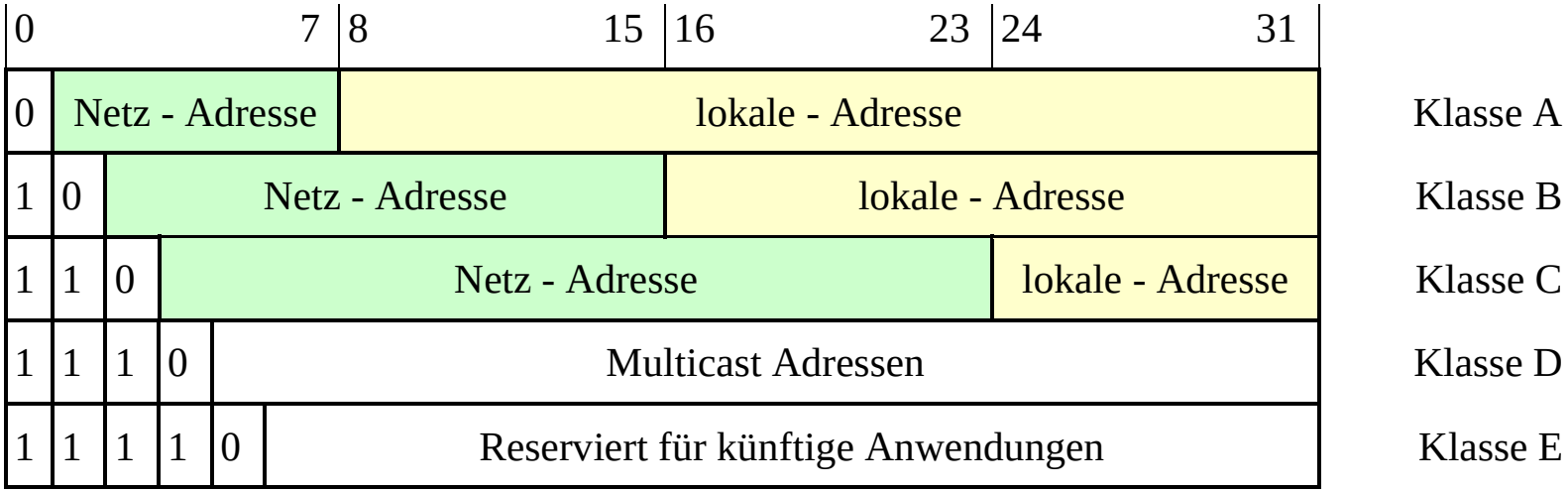
In diesem Beispiel fragmentiert IP die Daten in drei Teile: 2000 Bytes = 800 Bytes + 800 Bytes + 400 Bytes

Problems with fragmentation: Host cannot reuse an identifier for at least TTL period
- with 2 min. TTL, at most 546 packets/s may be transmitted

Adressierung

L5,6,7	Von Anwendung abhängig	
L4	Port (socket)	
L3	Protocol	Internet-Adresse
L2	DSAP, SSAP	
MAC	z.B. Type field	MAC-Adresse z.B. Ethernetadresse

IP-Adressen



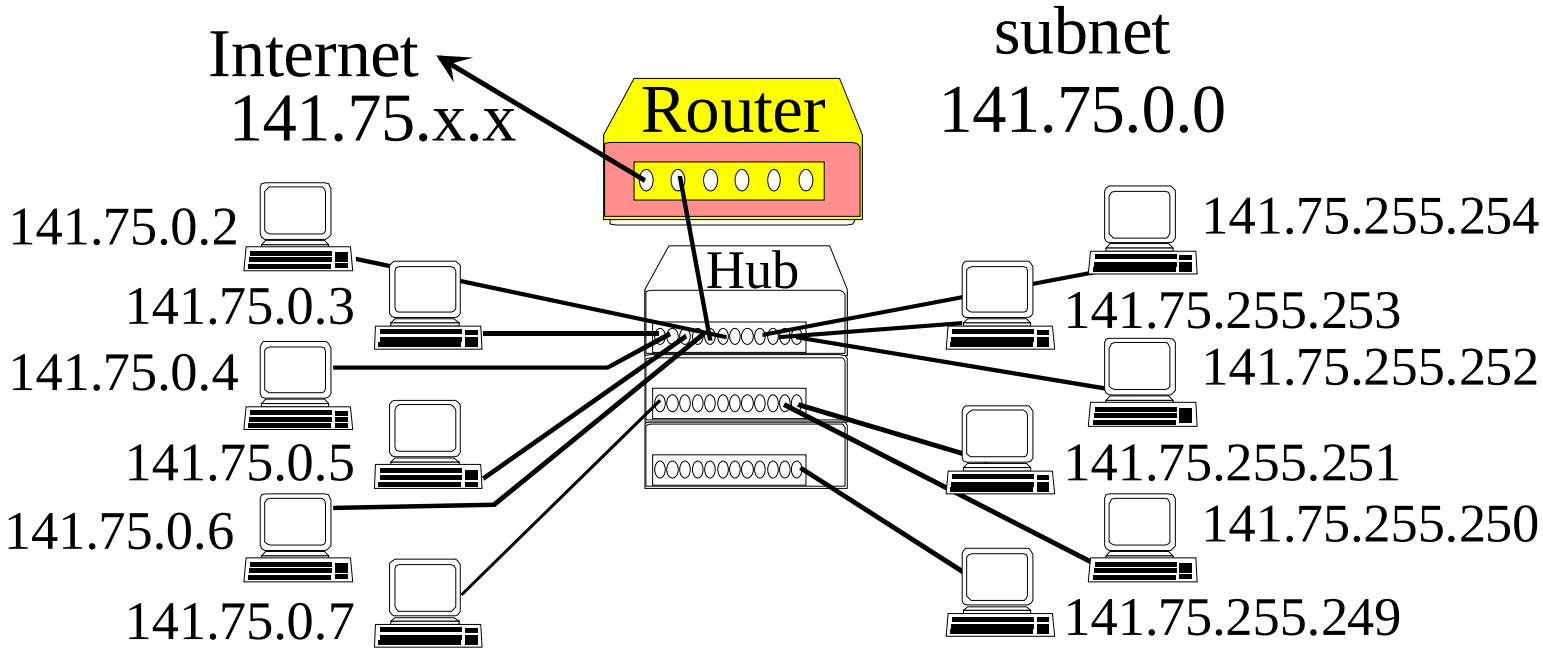
Netz-Adresse: netid lokale Adresse: hostid

Adressvergabe: nur **ein** großes Netz

1	0	Netz - Adresse	lokale - Adresse	Klasse B

Netz-Id = Adresse der Organisation, z.B. 141.75.x.x

141.75.0.0	Netzadresse der Organisation
141.75.0.1	Adresse für den Router zum Internet (nicht zwingend)
141.75.0.2 ... 141.75.255.254	65533 mögliche Host- und Router-Adressen
141.75.255.255	Broadcast-Adresse



Adressvergabe mit Subnetzen

1	0	Netz – Adresse net id	Subnetz subnet id	Host host id

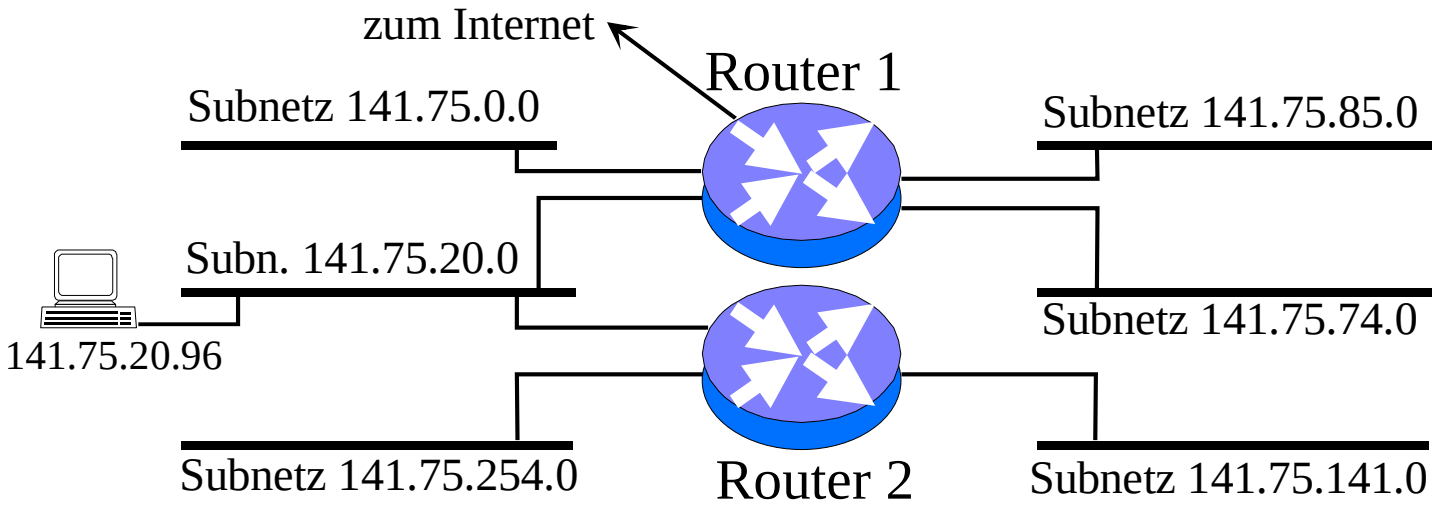
Klasse B

Beispiel für class B Netz

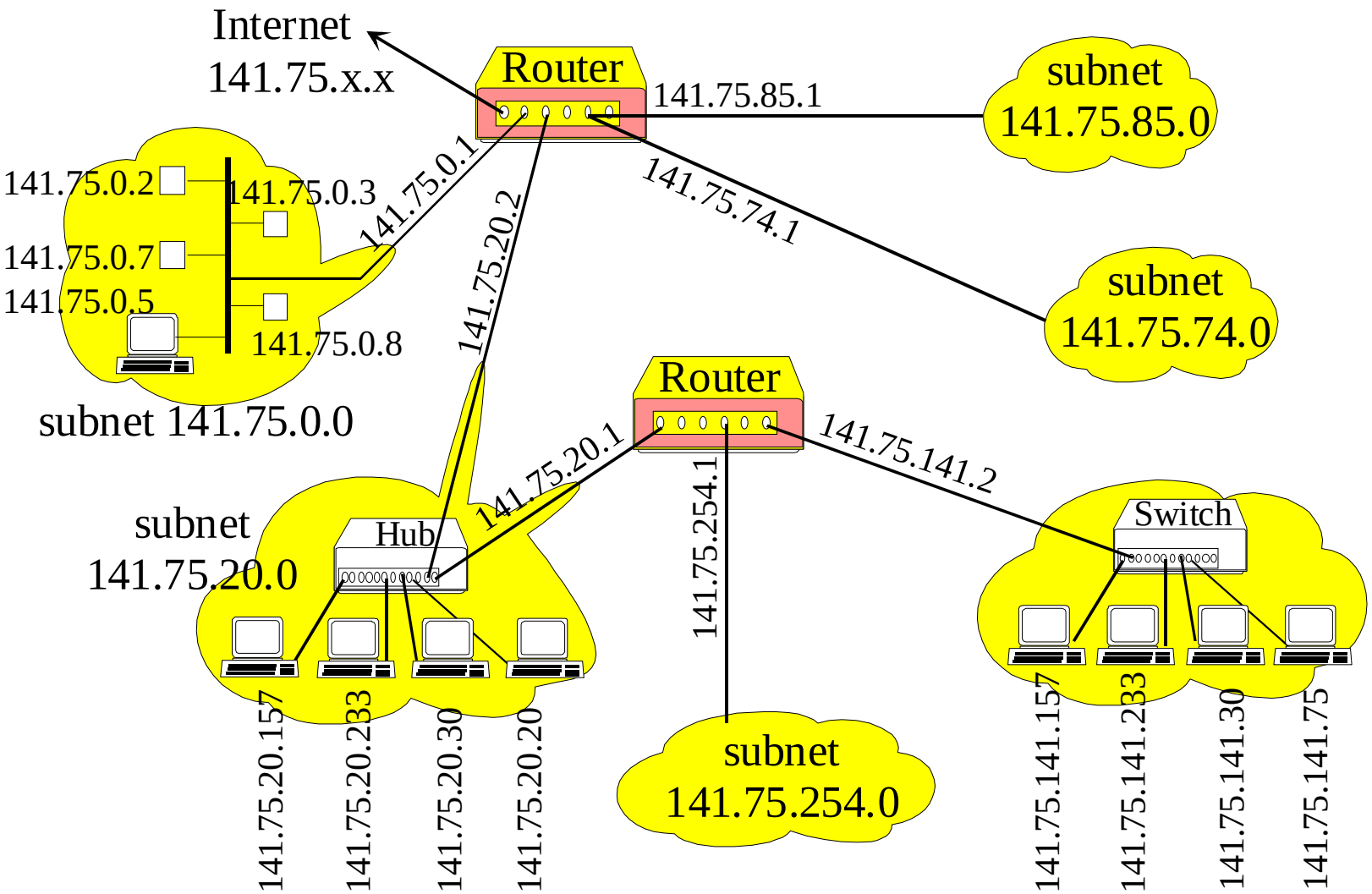
	14 bit z.B. 141.75	8 bit z.B. 20	8 bit

Netz-Id = Adresse der Organisation, z.B. 141.75.x.x

Subnetze mit je 255 Adressen



Adressvergabe mit Subnetzen



das gleiche Netz wie im Bild vorher in anderer Darstellung

Special Addresses

Net Id	Subnet Id	Host Id		
0		x	Host x on this network,	only as source address
-1		-1	Limited broadcast on this subnet,	only as destination address
n		-1	Directed broadcast to n,	only as destination address
n	s	-1	Directed broadcast to subnet s of network n	only as destination address
n	-1	-1	Directed broadcast to all hosts on all subnets of network n	only as destination address
127			Internal host loopback test	only inside host

Addresses for internal use:

1 class A Address : **10.x.x.x**, (16 Mio. Host-Adressen von 10.0.0.1 bis 10.255.255.254)

16 class B Addresses : **172.16.0.0. to 172.31.0.0**

256 class C Addresses : **192.168.0.0 to 192.168.255.0**

Subnetz - Größe

1	0	net id	subnet id	host id

Klasse B

Beispiel für class B Netz 14 bit 12 bit ←→ 4 bit

Netzwerkmaske: 11111111 11111111 11111111 1111 0000 255.255.255.240

1	0	net id	subnet id	host id

Klasse B

Beispiel für class B Netz 14 bit 8 bit ←→ 8 bit

Netzwerkmaske: 11111111 11111111 11111111 00000000 255.255.255.0

1	0	net id	subnet id	host id

Klasse B

Beispiel für class B Netz 14 bit 4 bit ←→ 12 bit

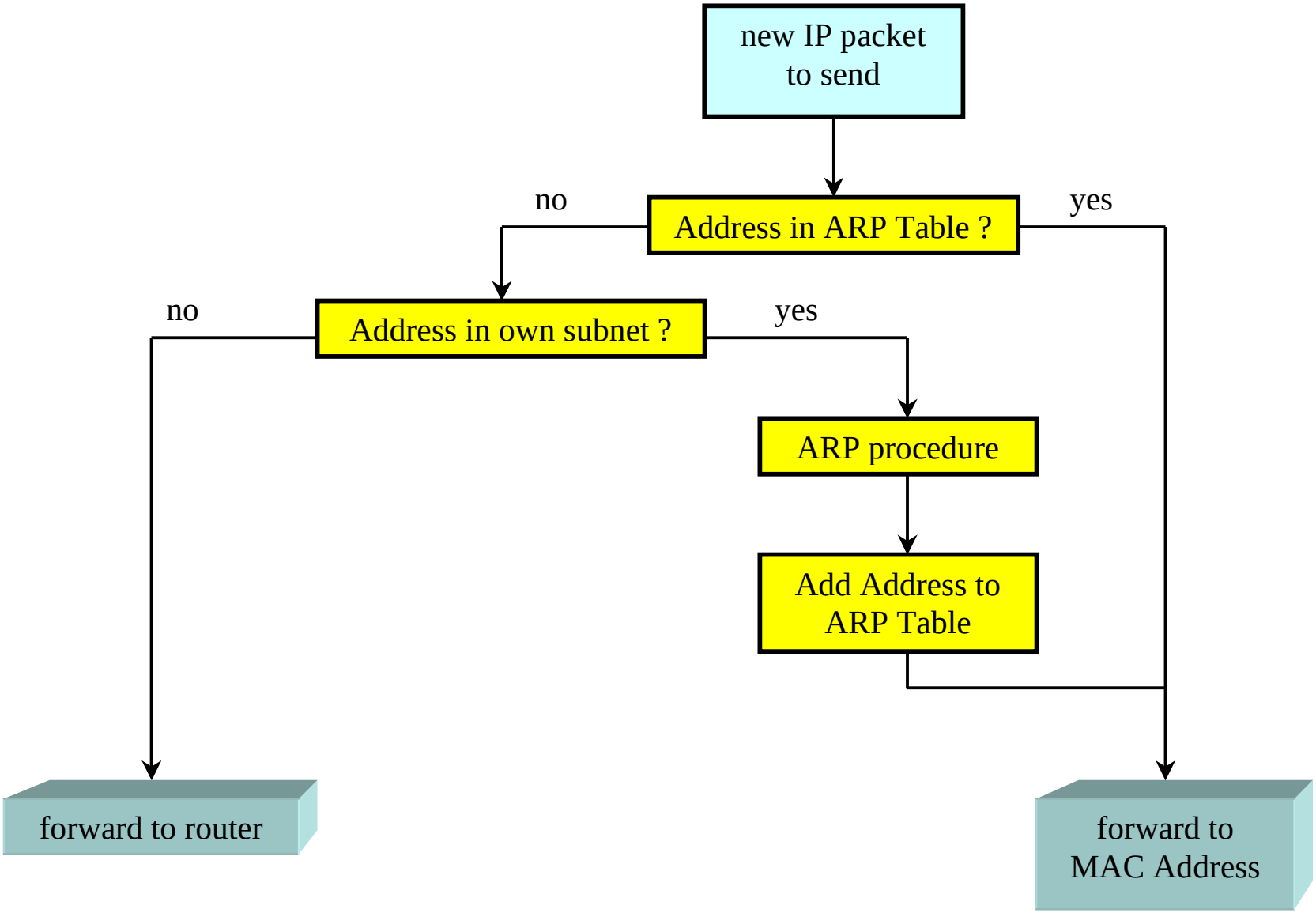
Netzwerkmaske: 11111111 11111111 1111 000000000000 255.255.240.0

Decimal	Binary	Number of Subnets $2^n - 2$	Number of '1'	Number of '0'
255	1111 1111 (Eight 1's, n=8)	$2^8 – 2 = 254$	8	0
254	1111 1110 (Seven 1's, n=7)	$2^7 – 2 = 126$	7	1
252	1111 1100 (Six 1's, n=6)	$2^6 – 2 = 62$	6	2
248	1111 1000 (Five 1's, n=5)	$2^5 – 2 = 30$	5	3
240	1111 0000 (Four 1's, n=4)	$2^4 – 2 = 14$	4	4
224	1110 0000 (Three 1's, n=3)	$2^3 – 2 = 6$	3	5
192	1100 0000 (Two 1's, n=2)	$2^2 – 2 = 2$	2	6

Routing

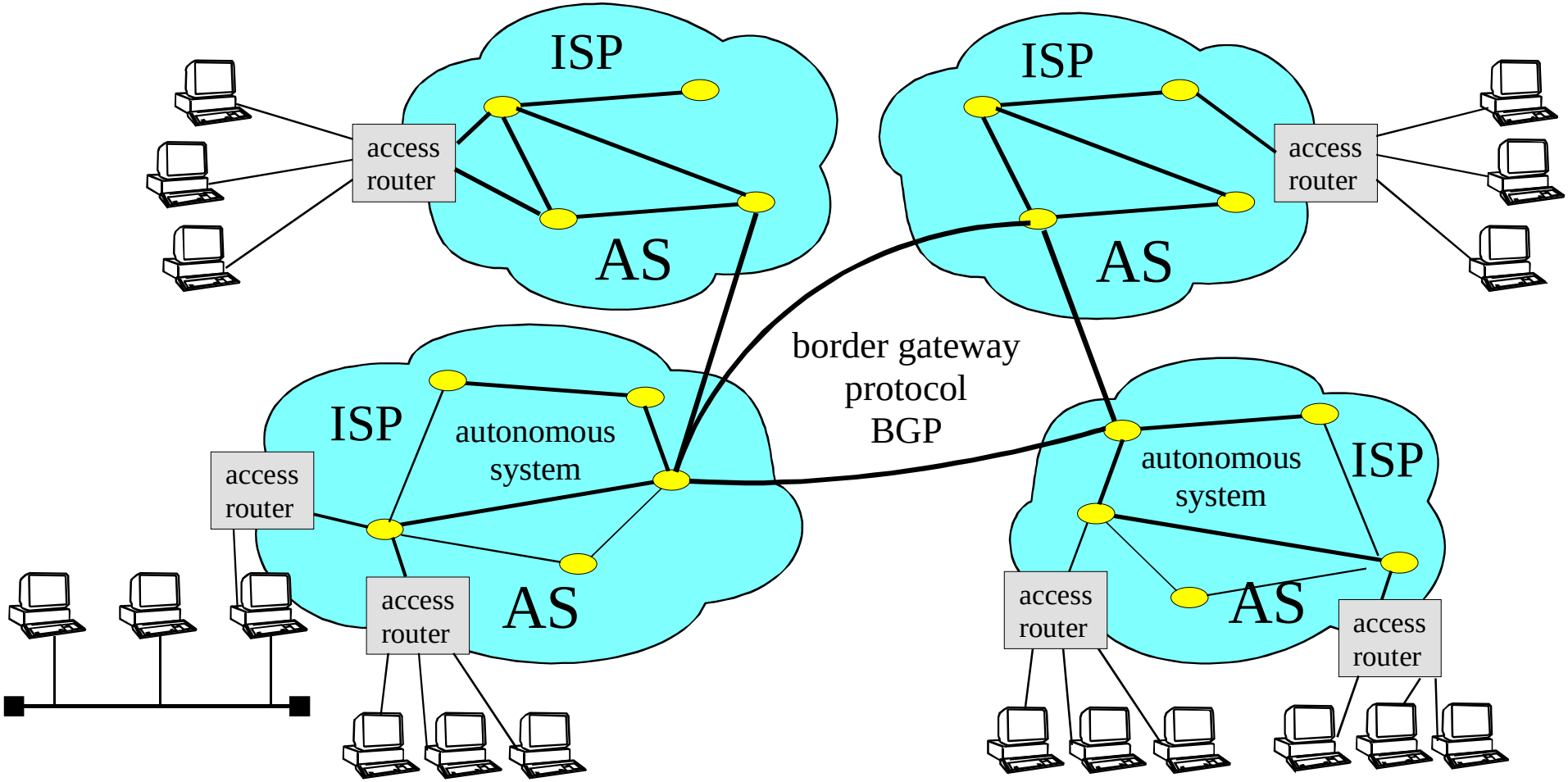
Indirect Routing	Normalfall; Router bestimmt den nächsten Knoten aus der Routingtabelle.
Source Routing:	Absender gibt Weg zum Ziel explizit vor.
Direct Routing:	Absender und Ziel liegen im gleichen (Sub)Netz. Routing ist nicht nötig,
Default Routing:	Wenn für Ziel kein Eintrag in der Routingtabelle , wird Datagramm an *Default-Router* gesendet. Dieser muß explizit spezifiziert werden.
Statisches Routing:	Routingtabelle wird manuell vom Netzwerkmanager erstellt.
Dynamisches Routing:	Hosts und Router tauschen *Routing Information* Pakete aus. Durch *Interior Gateway* Protokolle IPG lernen Router die Pfade zwischen Datennetzen kennen

Host Routing



Das Internet ist eine Sammlung von einzelnen Netzen (autonomous network AS)

Internet



Routing on the Internet Backbone

- ISPs are connected with one another at network access points (NAPs).
- NAP routers have to know about every network on the Internet (they are the default gateways)
- NAP routers have to be configured, when a new network is added to the network

CIDR : Classless inter-domain routing

CIDR (RFCs 1517 through 1520)

NAP routers have to know only about ranges of IP addresses

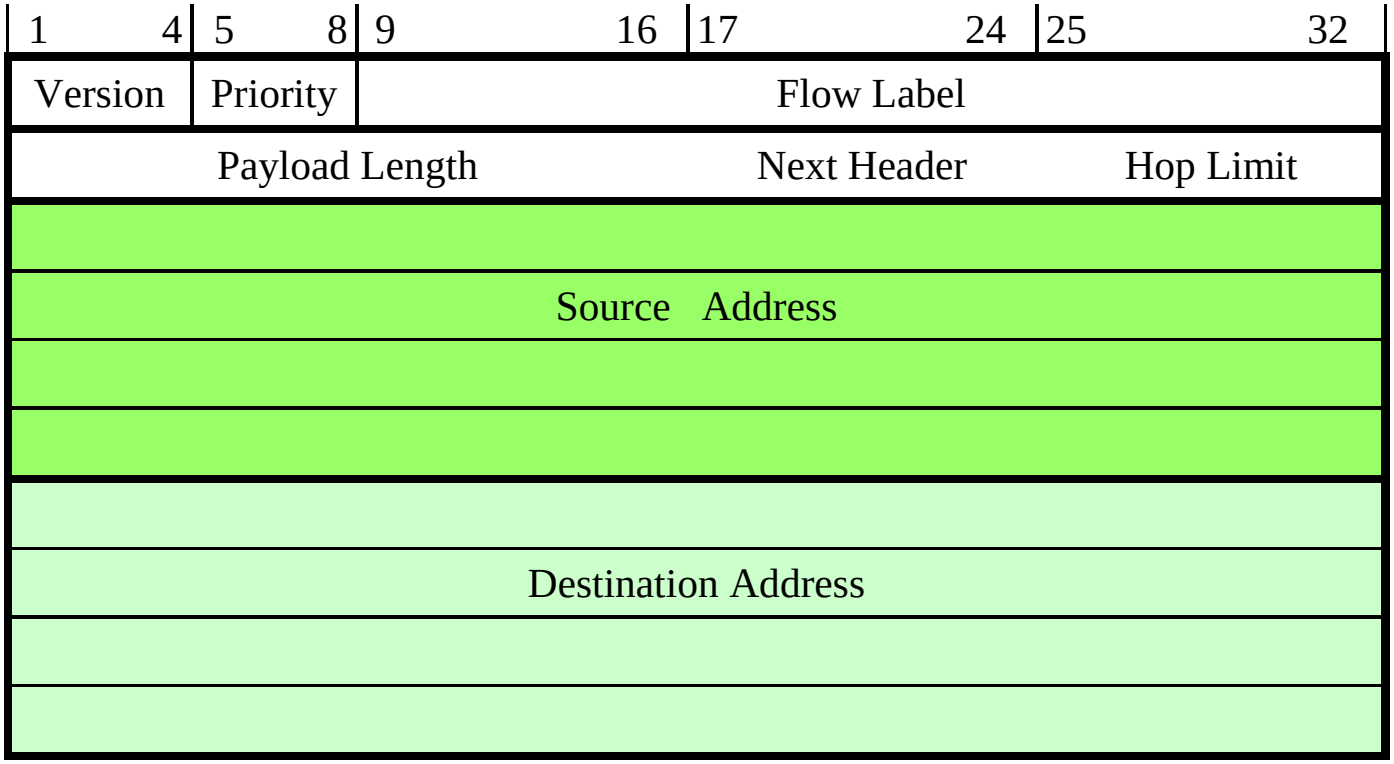
e.g. :204.36.0.0 / 16 (/16 subnet mask) ➔ xyz : all class C networks 204.36.x.x belong to ISP xyz

The ISP could elect to subdivide the /16 CIDR block
into two /17 CIDR blocks, each with 128 contiguous networks, or
into four /18 CIDR blocks, each with 64 contiguous networks

- CIDR avoids very large routing tables (containing every network in the world)

IPv6 Adressen

IPv4: $4{,}3\ 10^9$ Adressen ➔ Ipv6: $3{,}4\ 10^{38}$ Adressen



Schreibweise der Adressen:

4-stellige Hex-Zahlen getrennt durch **:**
108A:EF:0:0:0:0:1A5:67

Führende Nullen weglassen

Adreßteile, die nur aus Nullen bestehen, durch :: abkürzen,
z.B. 0:0:0:0:0:F5:1C:A812
= F5:1C:A812
oder
108A:EF:0:0:0:0:1A5:67
= 108A:EF**::**1A5:67

IP v4 Adressen in IPv6:
z.B.
0:0:0:0:0:0:**141.75.16.248**
oder ::**141.75.16.248**

Priority : 0 niedrigste, 15 höchste Priorität; **0-7** kann bei Überlast in Routern warten, **8-15** nicht (Echtzeit).

Flow Label : Flow = Folge von Datenpaketen, z.B. bei Videoübertragung. Jedes Paket eines solchen Stromes bekommt den gleichen Flow Label. Router speichern Flow-Label in einem Cache; Pakete werden dann schneller weitergrleitet.

Payload Length : Länge der Nutzdaten in Bytes

Hop Limit : Maximale Anzahl von Knoten

Next Header : zeigt Art des Extension-Header an:
keine Erweiterung; Source-Routing; Segmentierung; Authentifizierung; Verschlüsselung; ...

IPv6 Adressen

Unicast address	010 3 Bit	Registry 5 Bit	Provider n Bits	Subscriber 56-n Bits	intranet 64 Bit

Adresse für einzelne Station. Registry-Id. = Institution (NIC) die Adresse vergeben hat; Interface = Rechner z.B. MAC-Adresse (48-Bit)

Multicast address	1111 1111 8 Bit	Flags 4 Bit	SCOP 4 Bits	Group ID 112 Bits

Gruppe von Benutzern z.B. Videokonferenz. Broadcast wird mittels Multicast-Protokoll durchgeführt

Link local address	1111 1110 10 10 Bit	0 0... 0 n-Bits	subnet m Bits	interface 118-n-m Bits

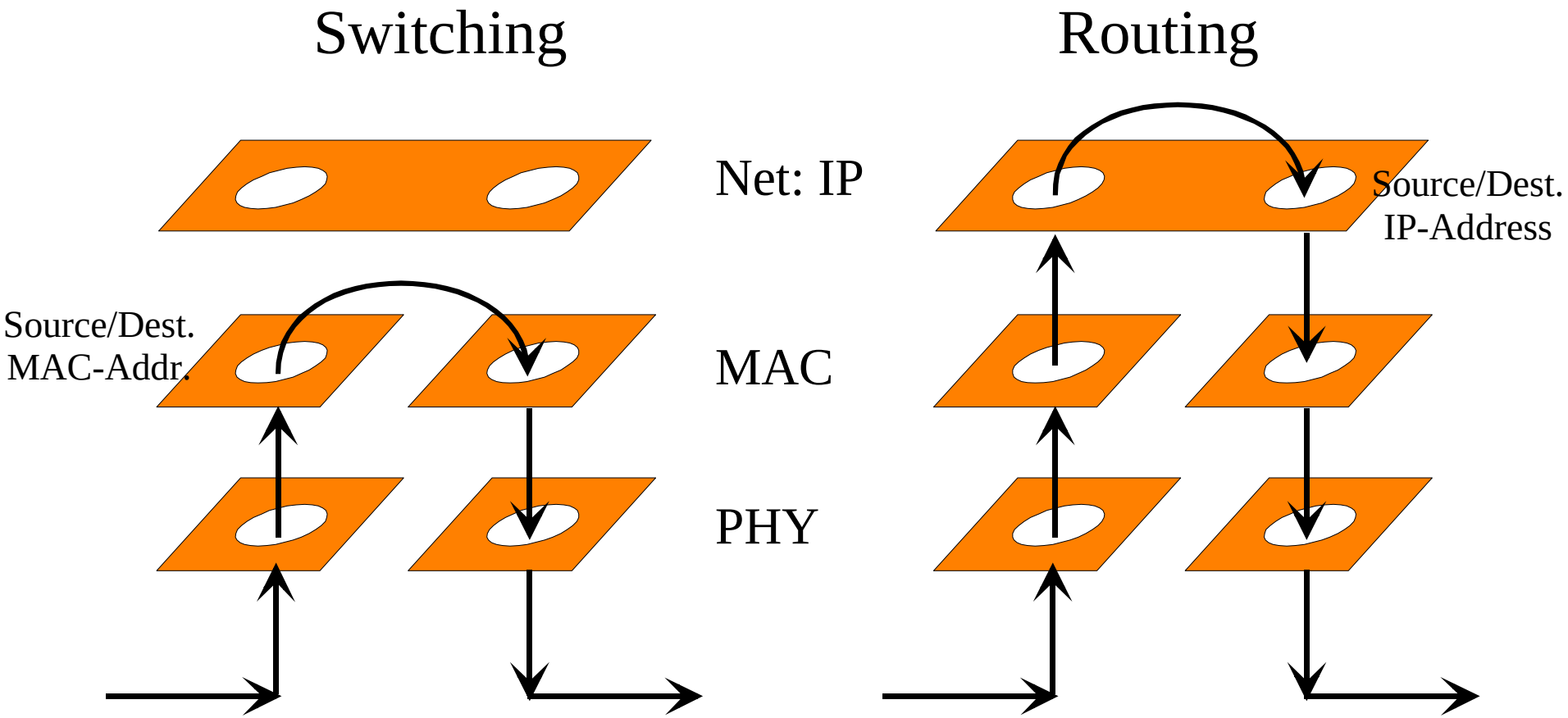
hat nur auf einer Verbindung (link) Bedeutung, nicht ans Internet angeschlossen oder Test

Site local address	1111 1110 11 10 Bit	0 0... 0 n-Bits	subnet m Bits	interface 118-n-m Bits

hat nur innerhalb einer Firma Bedeutung, nicht ans Internet angeschlossen oder Test

IPv4 address compatitbility	0 0... 0 80 Bit	0..0 or 1..1 16 Bits	IPv4 address 32 Bits

Routing - Switching

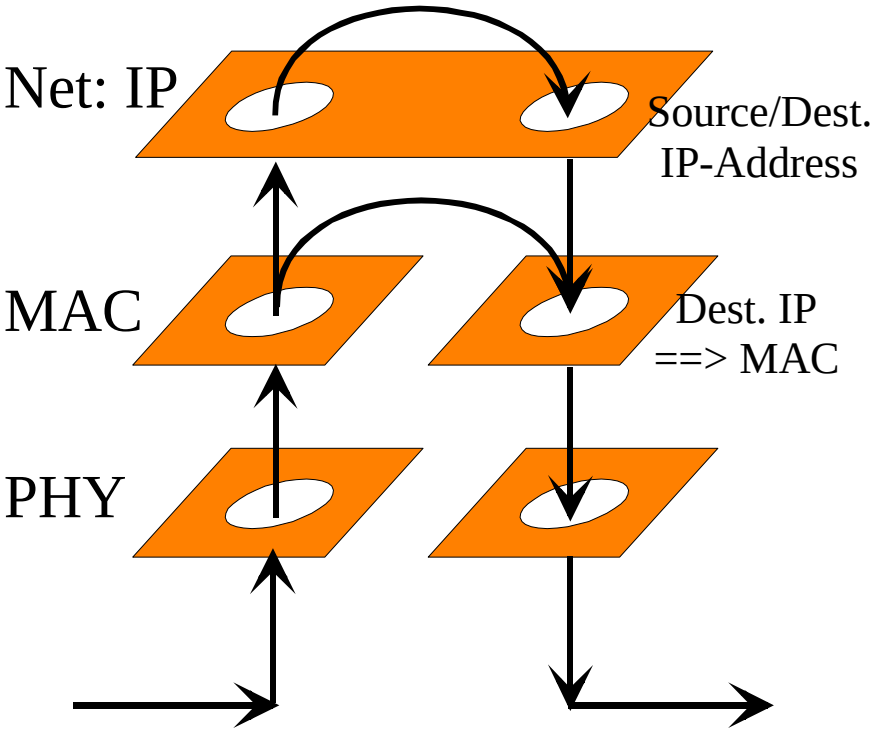


Layer 3 Switching:

1. normal IP-Routing (L3) in the first step
2. the Destination-MAC-Address and output port is stored with the IP-Address
3. for all subsequent frames: search the IP lookup table and route to the Destination-MAC-Address

Routing - Switching

L3 - Switching



Determine Output Port (route) from:

Switch:	dest. MAC-Address dest. MAC ≠ Router itself
Router:	dest. IP- Address
L3-Switch:	dest. MAC = Router itself dest. IP- Address

L3-Switching hat heute große Bedeutung im LAN und besonders zusammen mit VLANs.

VLAN: IP-Adressen, die bisher topographisch durch den Router-Port repräsentiert wurden, können fortan innerhalb des lokalen Netzwerks flächendeckend zum Einsatz kommen.

Layer 4 - Switching

Quality of Service

Der Router liest die Portnummer im TCP- oder UDP-Header.

Bestimmte Applikationen (Port-Nummern) bekommen eine bevorzugte Behandlung im Routing-Switch.

Sie ausgefilterten Applikationsströme werden definierten Ebene-3-VLANs zugewiesen, um die Kommunikation im Ethernet-LAN insgesamt transparent zu halten.

Damit Layer-4-Switching zum Zuge kommen kann, müssen die eingesetzten Routing-Einheiten den IP-Stack in voller Breite unterstützen.

Alternative: Type-of-Service-Feld (TOS-Feld) im IP-Header:
Heute unterstützen nur wenige (Netzwerk-)Betriebssysteme und Anwendungen das TOS-Feld für die Anforderung spezieller Dienstgüten. Windows NT soll ab Version 5.0 soll NT das TOS-Feld besetzen können.

Probleme beim Ebene-4-Switching heute:

- Prioritäten können derzeit nur statisch vergeben werden.
- Die Vergabe benutzerspezifischer Prioritäten für einzelne Applikationen ist heute über Ebene-4-Switching noch nicht möglich - es sei denn, die Vergabe wird mittels dynamischer IP-Adressen über einen sogenannten Policy-Server realisiert.

Sonstige IP-Protokolle : ICMP (Internet Control Message Protocol)

ICMP setzt auf IP auf und transportiert Fehler- und Diagnoseinformationen

0 7	8 15	16 23	24 31
IP-Address			
ICMP-Typ	ICMP-Code	ICMP Checksum	
abhängig vom ICMP-Typ			

Rahmenformat von ICMP Meldungen

	ICMP-Typ	
Fehler-meldungen	3	Destination Unreachable (nächste Verbindung unterbrochen, don't fragment,..)
	4	Source Quench (Warteschlange läuft über, Sender reduziert Datenrate)
	5	Redirect (Wegumleitung, falscher Router wurde angesprochen)
	11	Time Exceeded (ein Teilpaket für *reassembly* ist noch nicht angkommen)
	12	Parameterproblem
Informations-meldungen	8 / 0	Echo request / reply (PING-Befehl)
	9	Router Advertisement (Router kündigt sich periodisch an, broadcast)
	10	Router Solicitation (ein Host sucht einen Router)
	13 / 14	Timestamp request / reply (Sende und Empfangszeit dieser Meldungen)
	15 / 16	Information request/ reply (Host kann z.B. seine Netzadresse erfragen)
	17 / 18	Address Format request/ reply (Länge der Subnetzadresse, Netzwerkmaske)

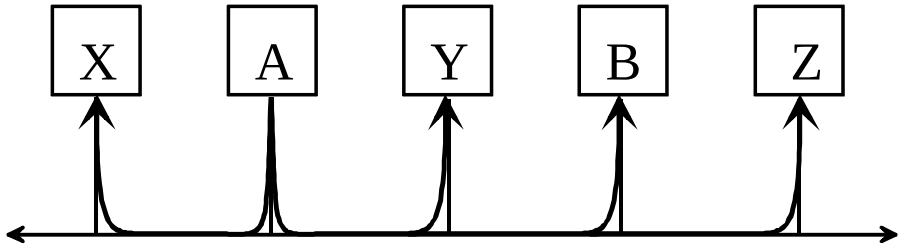
ICMP : ARP (Address Resolution Protocol)

IP-Adresse wird auf die zugehörige Ethernetadresse abgebildet

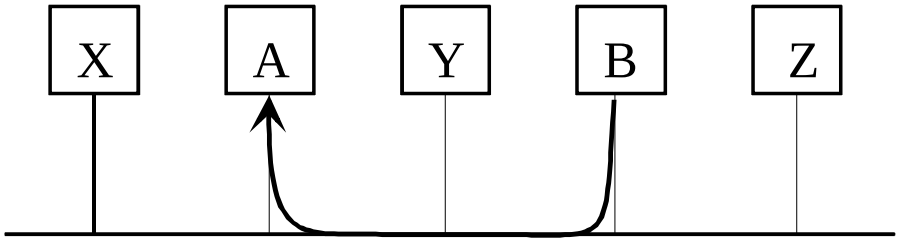
Address Resolution through Direct Mapping ➔ IPX (netware)

Address Resolution through Dynamic Binding ➔ IP

ARP-Request = Broadcast mit IP-Adresse von B



ARP-Reply mit Ethernet-Adresse von B



0 – 7	8 – 15	16 – 23	24 – 31
Hardware		Protocol	
HW Length	SW Length	Option Code	
Source MAC address			
Source MAC Address		Source IP Address	
Source IP Address		Destination MAC Address	
Destination MAC Address			
Destination IP Address			

Ethernet Type Field: 0806 ARP

Hardware: Übertragungsmedium,
Datenrate,
Datenstruktur

dadurch ist ARP flexibel für alle Netze

HW Length: Länge MAC Adresse

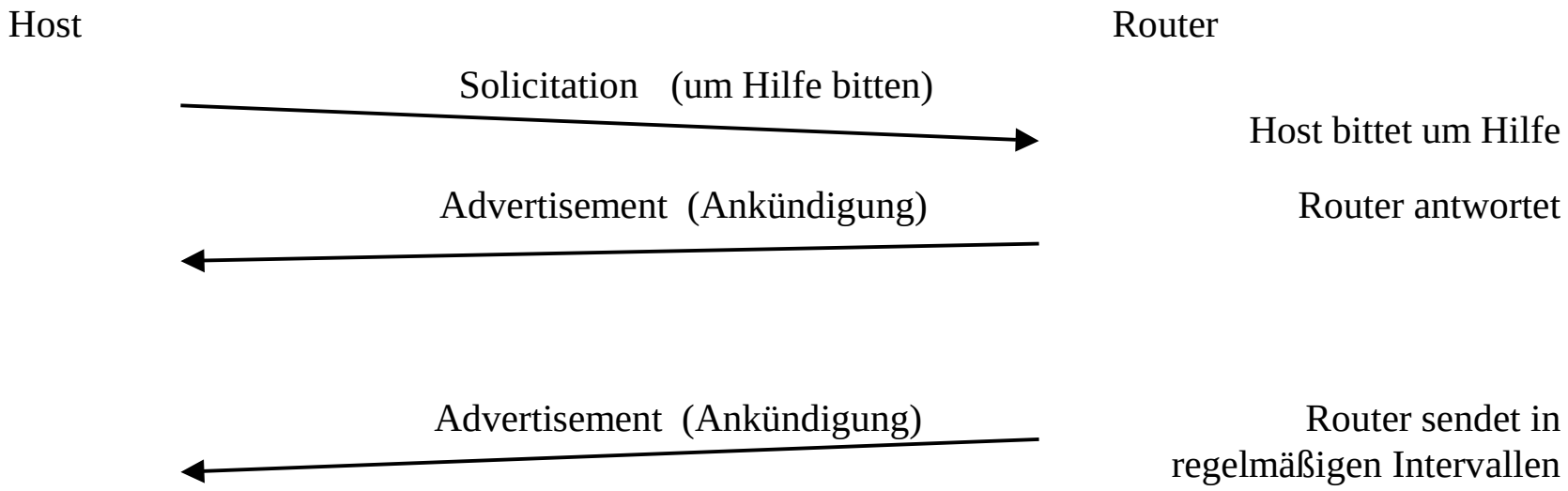
SW Length: Länge SW-Adresse = IP

Option Code: 1 = ARP Request
2 = ARP Reply

ICMP : der Host (PC) sucht sein Gateway (Router)

1. Manuelle Eingabe bei der Konfiguration des Netzwerkprotokolls (Gateway = Router-Adresse)

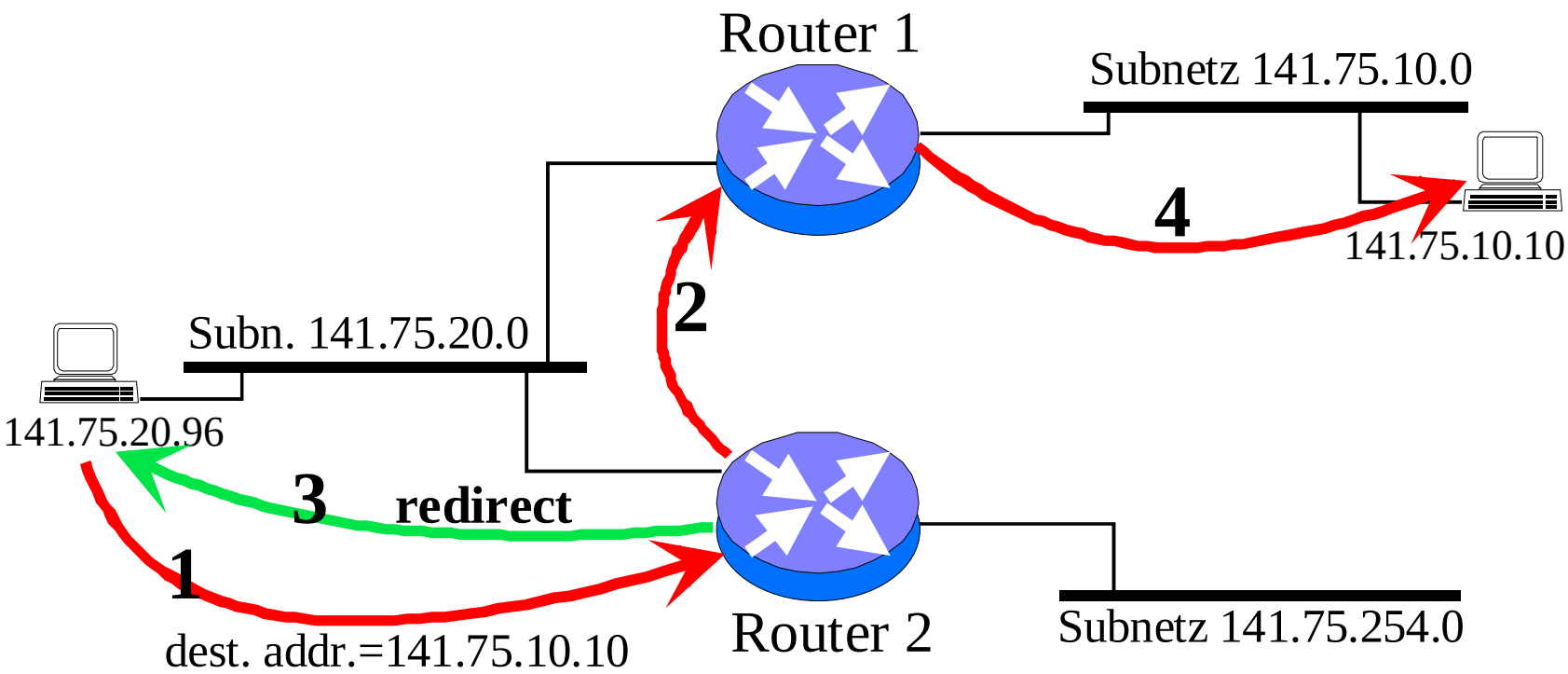
2. Host schickt beim Booten eine (ICMP-) Nachricht ins Netzwerk.



Mit dem Kommando **netstat -rn** lassen sich alle auf dem lokalen Host konfigurierten Routen angezeigt (Netzwerk- und Gateway-Adressen sowie der Subnet-Maske).

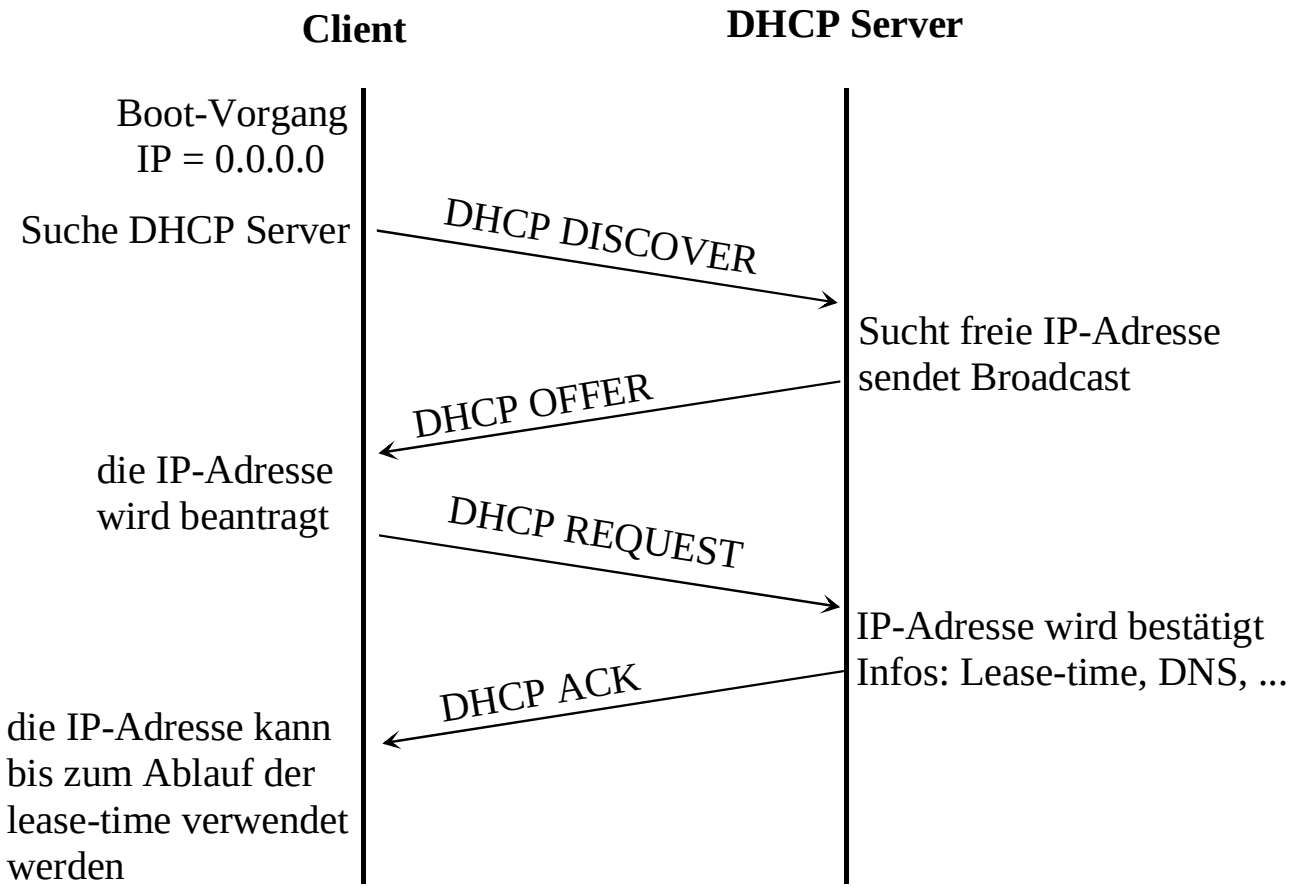
Mit **traceroute** (UNIX) oder **tracert** (NT) läßt sich der Weg verfolgen, den die Daten zum Zielhost nehmen. Allerdings macht das entsprechende Kommando tracert von Windows NT Probleme, wenn sich der Ausgangshost hinter einem Firewall befindet.

ICMP : Redirect



DHCP Dynamic Host Configuration Protocol

automatische Vergabe von IP-Adressen

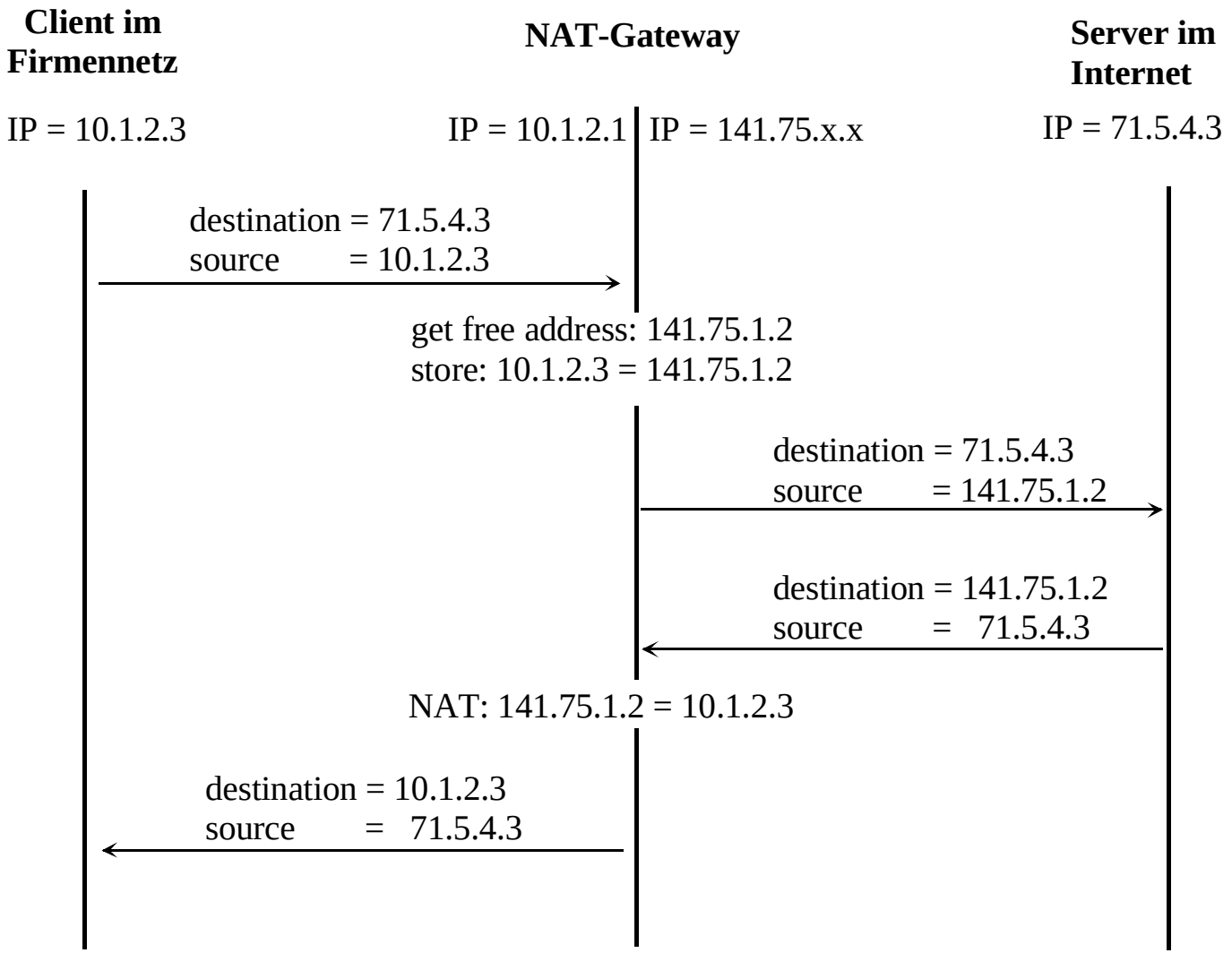


Vorteil:

- wenig Arbeit beim der Konfiguration
- Client (PC, Notebook) kann im Netz bewegt werden
- Es werden weniger IP-Adressen benötigt als PCs vorhanden sind

Der DNS muß das **DDNS-Protokoll** (Dynamic Domain Name System) unterstützen, damit im DNS immer die aktuelle, über DHCP vergebene IP-Adresse verfügbar ist.

Network Address Translation NAT



IP-Adressen für private (interne) Zwecke

1 Klasse A Netz: **10.x.x.x**, (16 Mio. Host-Adressen von 10.0.0.1 bis 10.255.255.254)

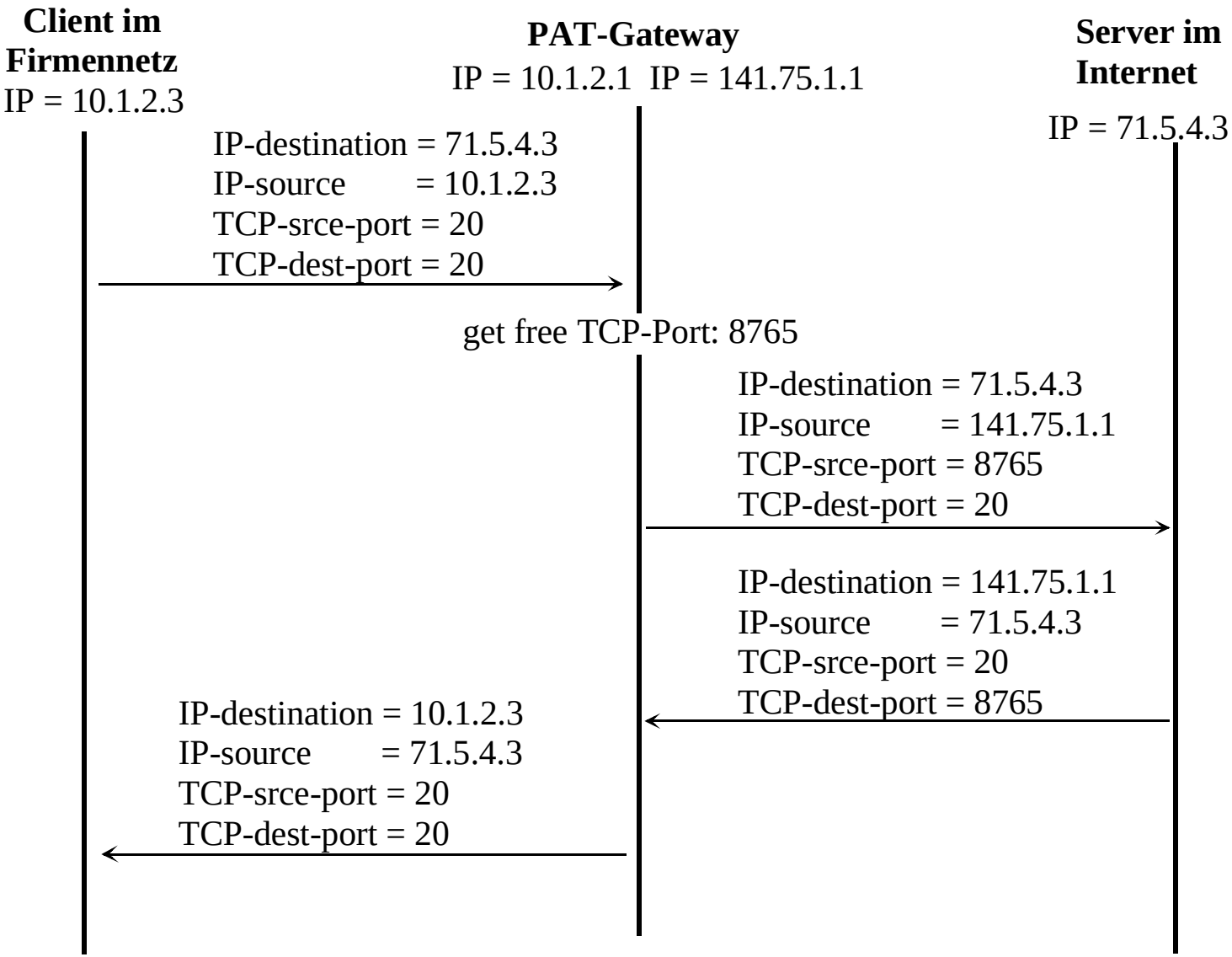
16 Klasse B Netze:
172.16.0.0. bis 172.31.0.0

256 Klasse C Netze:
192.168.0.0 bis 192.168.255.0

Adressumsetzung = IP-Masquerading

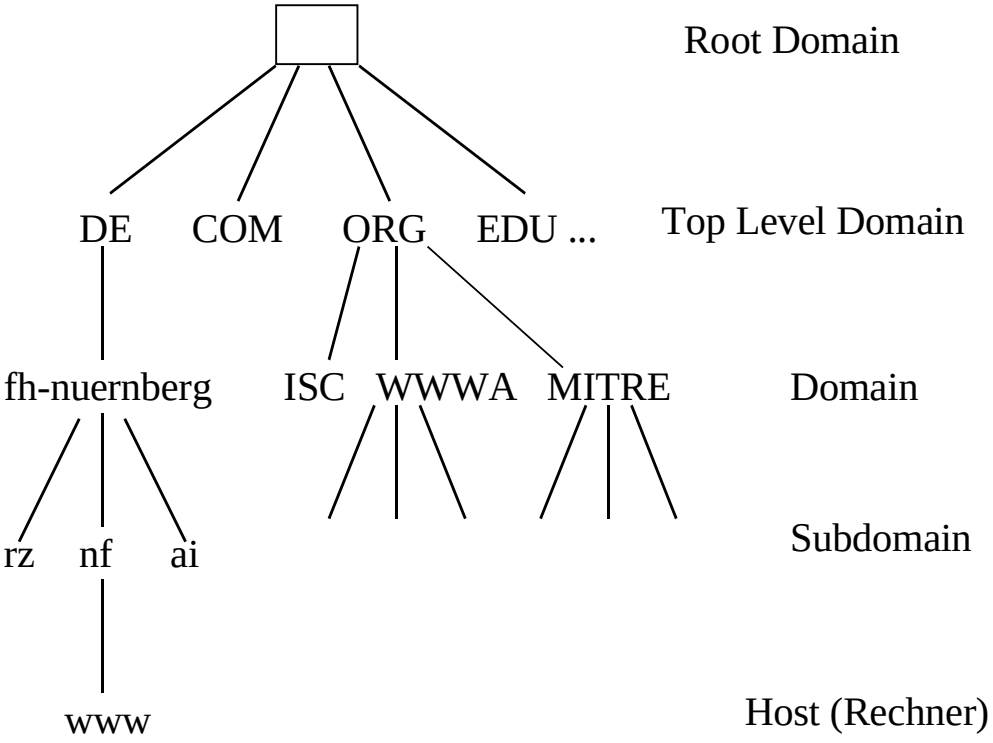
Port and Address Translation PAT

Viele Rechner ←→ eine IP-Adrwesse im Internet



Domain Name Service DNS

ICAN Internet Corporation for Assigned Names and Numbers vergibt Top Level Domains



Top-Level-Domains:

DE, UK, US,.. (Länder)
COM (kommerzielle Nutzung), .
GOV (US-Regierung),
EDU (Bildungseinrichtungen)
MIL (US-Militär),
ORG (Non-Profit-Gesellschaften)
NET (Netzwerk-Dienstanbieter)

ab 2001: name (Privatpersonen)
prof (Berufsgruppen)
museum
biz (kommerzielle Anbieter)
aero (Luftfahrt)
info (Informationsanbieter)

1. Ping nf-soft.nf.fh-nuernberg.de ➔ 141.75.16.225
2. Ping 141.75.16.225 -a ➔ nf-soft.nf.fh-nuernberg.de

Host-Namen ⇔ IP-Adressen

Kleine Netze: durch die Textdatei *hosts*.

Große Netze: DNS - hierarchisch verteilter Dienst auf Basis einer Datenbank

DNS ist Client/Server-Dienst:

1. Client (*Resolver*) schickt Anfrage an Server (Adresse in der TCP/IP-Konfiguration
2. Server antwortet mit IP-Adresse oder übergibt die Anfrage an den übergeordneten Server

nf-soft.nf.fh-nuernberg.de = Fully Qualified Domain Name FQDN.

Mobilität im Internet

Host-Migration

Arbeitsplatz und neuer Aufenthaltsort haben Zugang zum selben Subnetz
↓
trivial

alle anderen Fälle
↓
Zuweisung einer neuen IP-Adresse ist notwendig
(entweder von Hand oder automatisch)

Problem: Computer hat neue Identität, alle Netzwerkanwendungen müssen neu gestartet werden

➔ keine Mobilität sonder höchstens Portabilität

Mobile Host Protocols (**MHP**) **:**

- ermöglichen Mobilität eines Hosts
- der mobile Nutzer erhält dieselbe Qualität der Netzwerkdienste wie ein stationärer

Zwei Forderungen an Transparenz:

1. operational transparency: Nutzer braucht keine speziellen Aktionen bei Host-Migration durchzuführen
2. performance transparency: nach Migration sollen die Anwendungen wie gewohnt weiterlaufen

Mobile Packet Data : Vorteile

- echte Mobilität - nicht an eine Leitung gebunden
- immer online, immer verbunden
  - *instant IP dial tone*
  - keine Abrechnung der *Air-time*
  - Gebühren nach Datenvolumen und Qualität des Dienstes,
    d.h. man bezahlt das, was man wirklich genutzt hat
- Verbindungen zum Firmennetz (*Intranet*) und zum Internet
- kostengünstiges *roaming* mit *full connectivity*
- beibehalten der eigenen Identität

Mobile IP erlaubt

- Interoperability: transparenter Datenverkehr zwischen allen Hosts
- Identity: der Mobile Host ist immer unter der gleichen Adresse erreichbar
- Roaming: nur der Home Agent HA muß den Aufenthaltsort des Mobile Host wissen
- Routing: alle Router außer dem Home Agent machen normales Routing

Mobile IP: normal Scenario

The Mobile Host keeps its original home IP-address

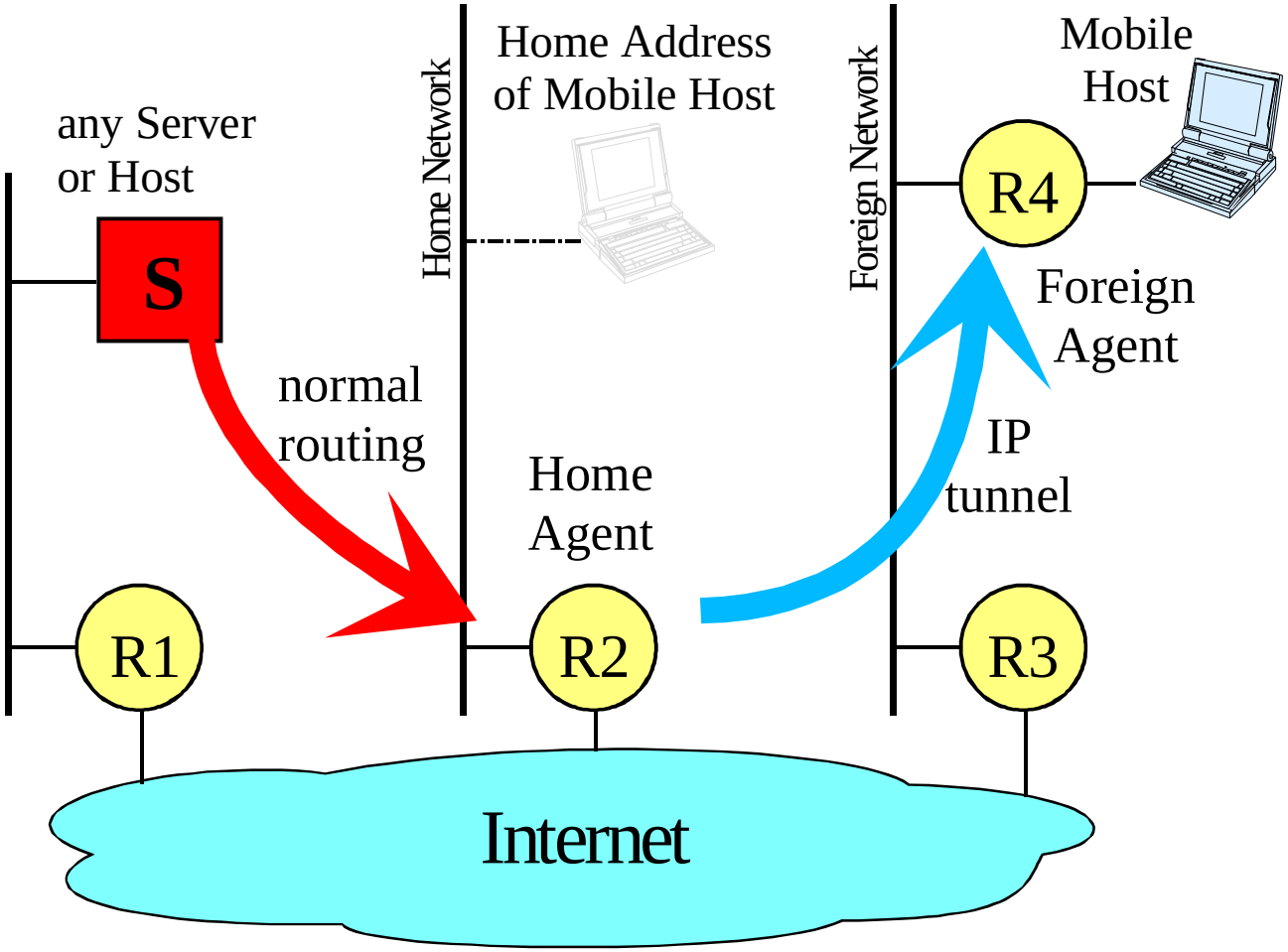
The Foreign Agent allocates a care-of-address for the Mobile Host

A tunnel is set up between the Home Agent and the Foreign Agent

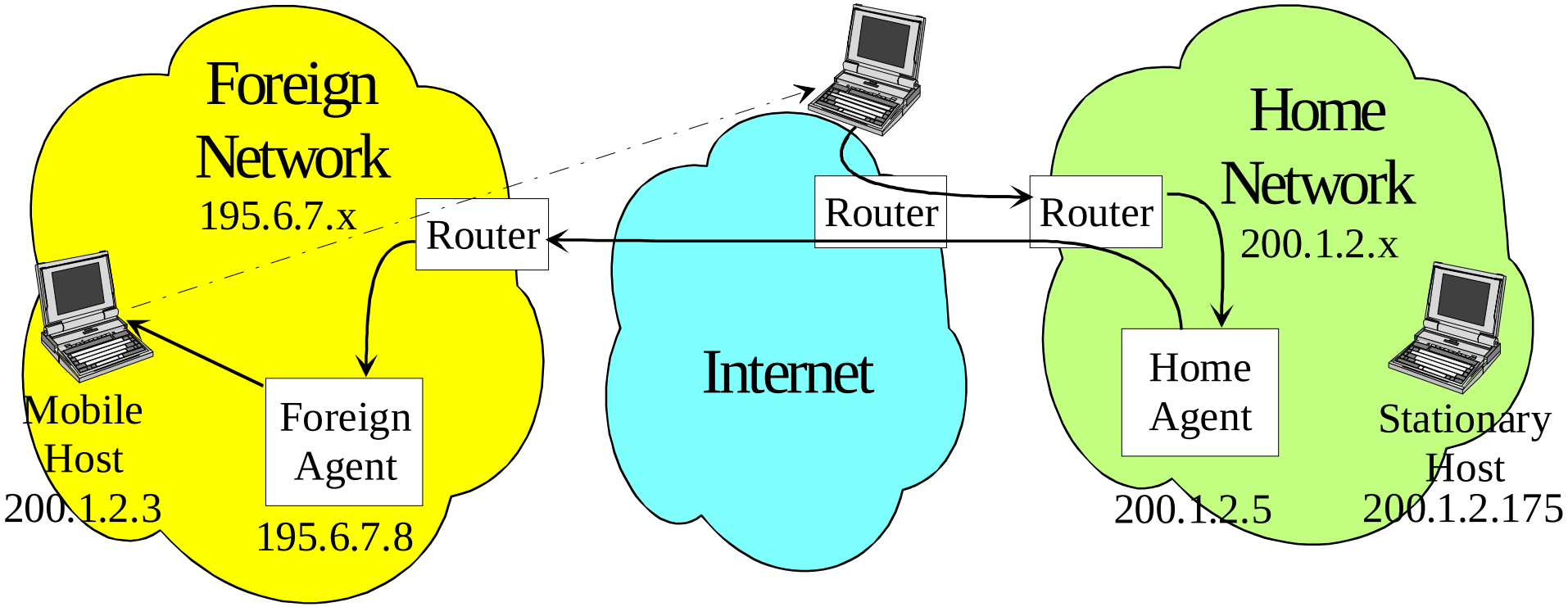
R1, R2, R3, R4 : Router

R2 : Home Agent

R4 : Foreign Agent



Mobile IP: Example for the normal Scenario



Mobile IP: Mobile Host requests Service

Mobile Host contacts Foreign Agent FA

[Solicitation] →

← Advertisement

Foreign Agent discovery protocol: extension of the ICMP router discovery protocol

Mobile Host registers at FA

Registration request →

FA allocates the **care-of address** for the mobile host

e.g 195.6.7.8 is **care-of** for 200.1.2.3

HA registers 195.6.7.8 as care-of address for Mobile Host 200.1.2.3

Registration Request →

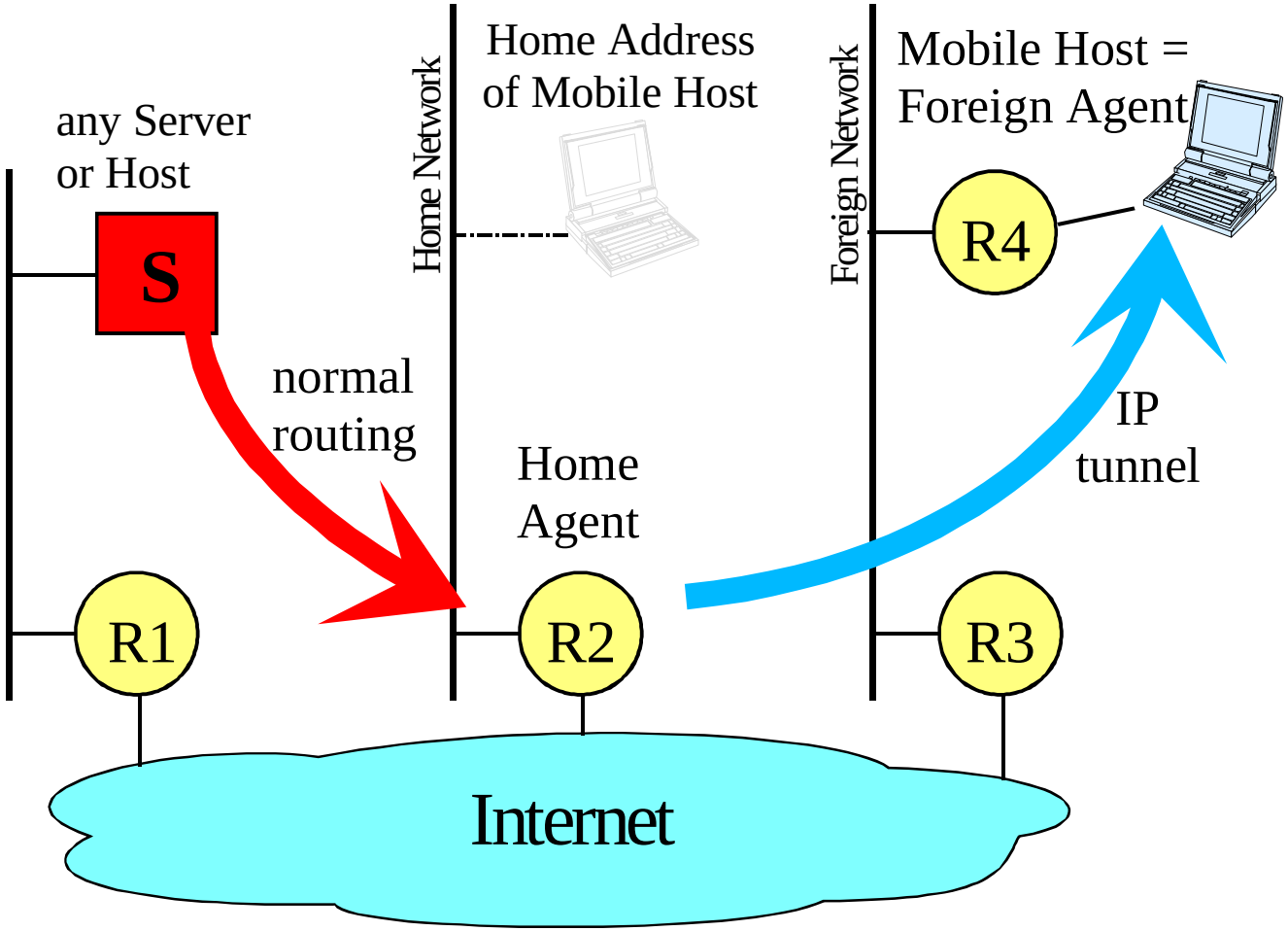
← Registration reply

(lifetime)

← Registration reply

Mobile IP: the Mobile Host acts as Foreign Agent

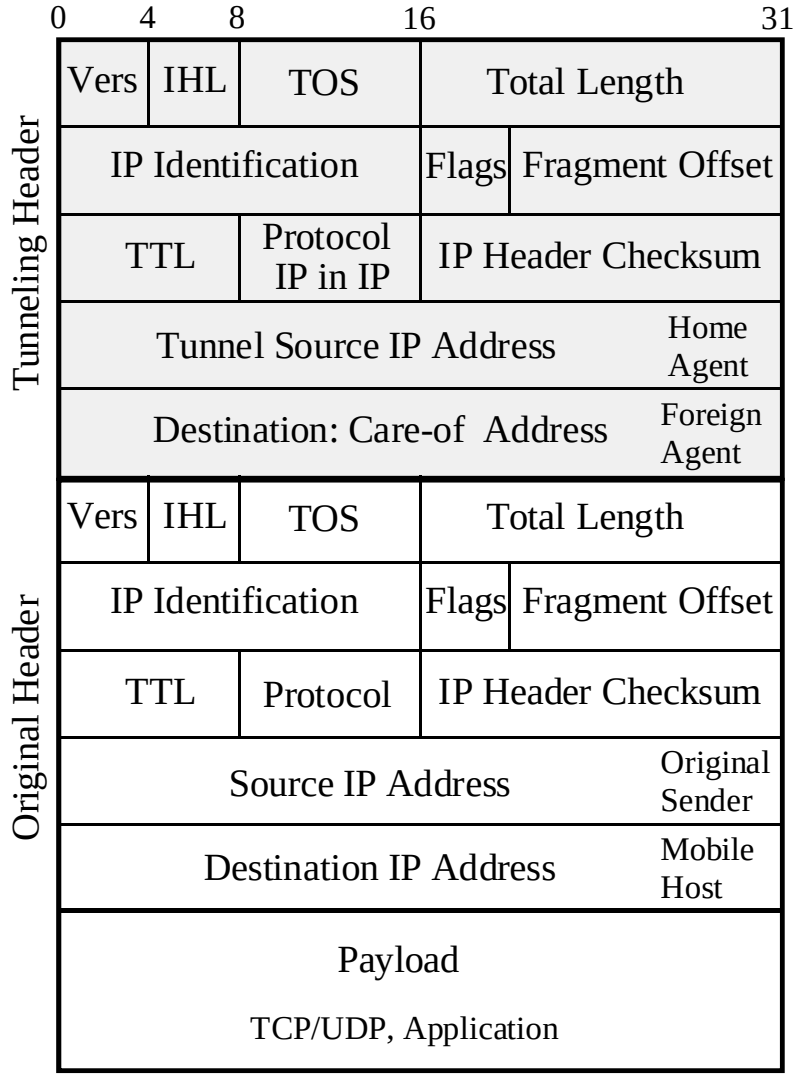
The Mobile Host keeps its original home IP-address and additionally
gets an IP-address in the foreign subnet (DHCP) which serves as care-of-address



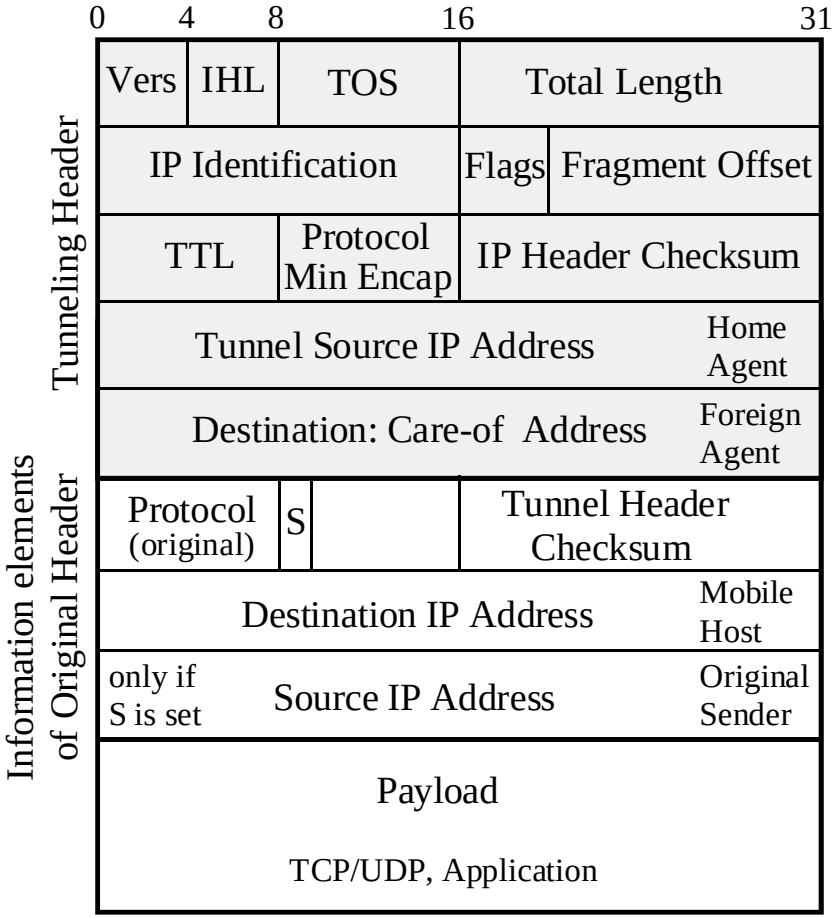
A tunnel is set up between
the Home Agent and
the Mobile Host

Mobile IP: Tunnelling Protocol

IP in IP encapsulation



Minimal encapsulation



IHL: Internet Header Length
TTL: Time To Live

TOS: Type Of Service
S: bit is set when original source address is present

Identification: fragmentation/reassembly