INTERNETWORKING

Problemstellung:

Wie können mehrere Netzwerke integriert werden?

Lernziel:

- Die Teilnehmer sollen das Design des IP-Protokolls als integrierende Komponente des Internets erklären können.

Inhalt:

- Was ist ein Internetwork?
- Internet Protocol (IP): Grundlagen
- IP: Adressierung und Forwarding
- Hilfsprotokolle für IP
  - Address Resolution: ARP / ATMARP
  - Host Configuration: DHCP
  - Error Reporting: ICMP
- Virtuelle Private Netzwerke / IP Tunneling

Was ist ein Internetwork?

Bei der Vorstellung der LAN-Technologien wurde gezeigt, wie mit Hilfe von Bridges bzw. Switches mehrere LAN-Stränge zu einem sogenannten "extended LAN" (eLAN) verbunden werden können. Bei einem eLAN handelt es sich im Allgemeinen nach wie vor um *ein einziges LAN*, bei dem lediglich zur Überwindung von physikalischen Limits (z.B. Leitungslänge) über Bridges und/oder Switches mehrere Segmente zusammengefügt wurden. (Ein anderes wichtiges Argument für Switches ist natürlich die Verbesserung der Leitungskapazität durch Verkleinerung bzw. Wegfall der Kollisionsdomänen.)

Ein LAN bzw. eLAN wird auch als *physikalisches Netz* bezeichnet. Unter einem Internetwork versteht man die Verbindung mehrere physikalischer Netze zu einem *logischen Netzwerk*. Die einzelnen physikalischen (Teil-)Netze werden dabei über sog. Router miteinander verbunden. Router sind Netzwerkknoten, die Packete aus einem Teilnetz in ein anderes weiterleiten. Die Information, welches Teilnetz auf welchem Weg (welcher Route) zu erreichen ist, ist in den Routern tabellarisch gespeichert.

Die Grenze zwischen den verschiedenen Arten von Netzwerkknoten ist allerdings unscharf. Dies ist dadurch bedingt daß Hersteller beim Entwurf ihrer Produkte wenig Wert legen auf klare Klassifizierung wie z.B. die Einordnung in das OSI-Modell. (warum auch?) Generell kann man sagen, daß Switches Packete auf der Protokollebene der Sicherungsschicht (der LAN-Ebene) weiterleiten. Router arbeiten mit Protokollen der Netzwerkschicht (was genau der Definition der Netzwerkschicht entspricht, mehrere Teilnetze miteinander zu verbinden.)

Das heute wichtigste Netzwerk-Protokoll ist IP ("Internet Protocol") aus der TCP/IP Protokoll-Familie. Gängige Router arbeiten deshalb mit IP-Packeten, allerdings gibt es auch Produkte, die sich IP-Switches nennen. Dabei muß man im Einzelfall genau hinsehen, was das jeweilige Gerät leistet...

Schließlich sollte noch unterschieden werden zwischen einem Internetwork und "dem Internet". Letzteres hat seinen Namen genau daher bekommen, die auf der Erde vorhandenen Netzwerke miteinander zu verbinden. Das Internet ist deshalb das allgegenwärtige Anschauungsbeispiel für Internetworks.

Abb. INW–1 zeigt ein typisches Beispiel für ein Internetwork. Hier sind Hosts an insgesamt vier physikalischen Netzwerken angeschlossen. Die einzelnen Netze sind von verschiedener Art (Ethernet, FDDI und eine Punkt-zu-Punkt Verbindung). Die Verbindungen zwischen den Netzen erfolgt über Router.

Beim Entwurf eines Internetwork-Protokolls gibt es zwei wesentliche Kriterien zu beachten:

- Heterogenität
  Es sollen Netzwerke unterschiedlicher Art miteinander verbunden werden (und auch solche, die erst in Zukunft entwickelt werden). Ein Internetwork-Protokoll kann somit nur auf den "kleinsten gemeinsamen Nenner" möglicher Netzwerk-Architekturen zurückgreifen.
- Skalierbarkeit

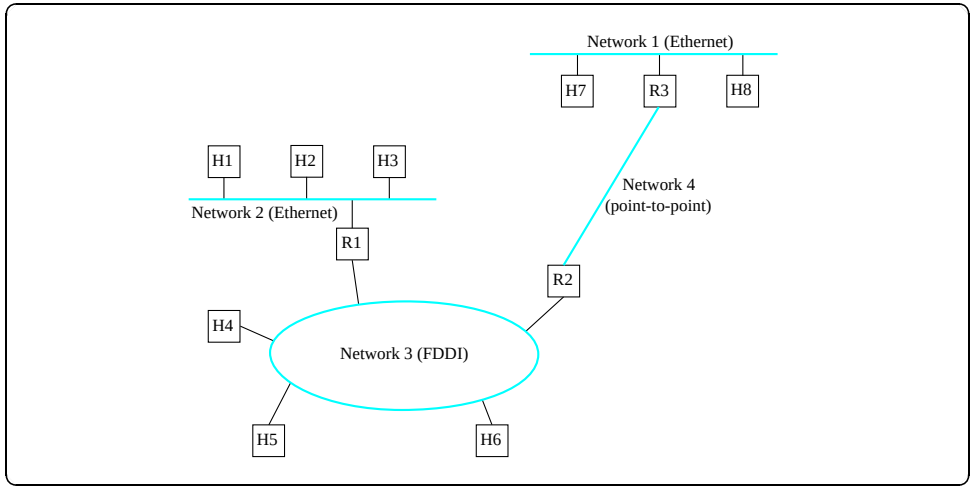

Abb. INW–1 Beispiel für ein Internetwork
Hn = Host, Rn = Router

Die Integration vieler Netzwerke und Rechner muß möglich sein (siehe Internet). Problemlösungen (Algorithmen, Adressierung, etc.) müssen darauf vorbereitet sein.

Internet Protocol (IP)

Dieses Kapitel handelt im Wesentlichen von IP, dem Internetwork Protocol des Internet. Abb. INW–2 veranschaulicht, wie IP zur Integration heterogener Netzwerke eingesetzt werden kann. (Vergleiche dies mit der Diskussion von Protokollstacks im Kapitel "Protokollarchitekturen".)

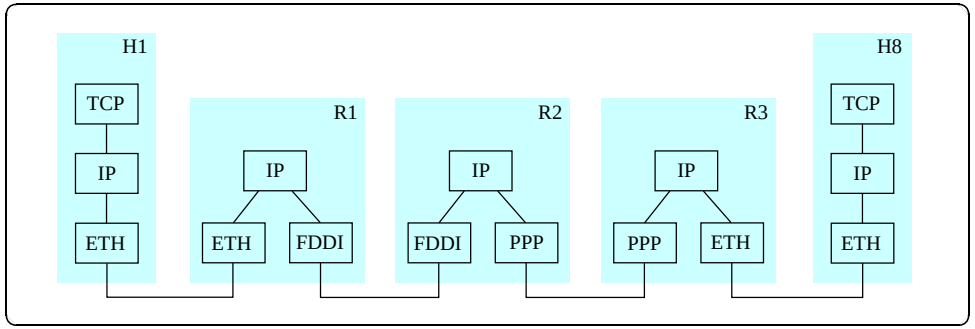

Abb. INW–2 Protokoll-Layer im Beispiel-Internetwork aus Abb. INW–1
(ETH sei das Ethernet-Protokoll)

IP Service Modell

Das Service-Modell eines Protokolls beschreibt, welche Dienste vom Protokoll angeboten werden. IP berücksichtigt dabei die Anforderungen von Heterogenität und Skalierbarkeit.

- IP bietet als Dienst die "best effort" Datagramm-Zustellung an.
- Dabei bedeutet "best effort", daß keinerlei Garantien über die Zustellung eines Datagramms gegeben werden. Datagramme können somit
  - verloren gehen
  - in veränderter Reihenfolge zugestellt werden
  - mehrfach zugestellt werden
  - mit zeitlicher Varianz (Jitter) und ohne garantierte Laufzeiten ("mit Verspätung") zugestellt werden
- Jedes denkbare Netzwerk kann dies garantieren.
- Router können somit relativ einfach aufgebaut werden. (keine komplexen Services im Netzwerk-Layer)
- Somit sind auch keine "überflüssigen" Services im Netzwerk-Layer definiert. Protokolle höherer Schichten können komplexere Services definieren und implementieren, je nach den Anforderungen dieser Protokolle.
  - z.B. gesicherte Übertragung

Header-Format

- Einträge im IP-Header:
  - Version (4): momentan 4
  - IHL (4): Anzahl von 32-Bit-Wörtern im Header
  - Type of Service (8): Art des Services (nicht oft verwendet)
  - Totel Length (16): Anzahl der Bytes in diesem Datagramm
  - Identification (16): wird von der Fragmentierung verwendet
  - Flags/Offset (16): wird von der Fragmentierung verwendet
    - ◇ DF = Don't fragment
    - ◇ MF = More fragments
  - Time to Live (TTL) (8): Zähler, wird einmal pro Hop (Router) dekrementiert (evtl. mehrmals bei langen Warteschlangen.)

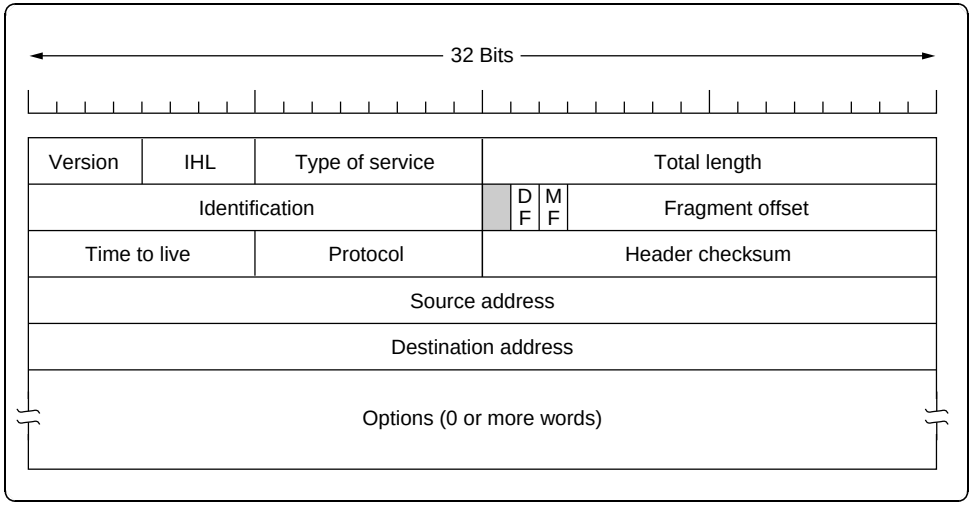

Abb. INW–3 Das IP-Header Format.

Bei TTL = 0 wird das Paket weggeworfen.

- Protokoll (8): Demux-Schlüssel (TCP=6, UDP=17)
- Checksum (16): nur vom Header
- DestAddr & SrcAddr (32)
- Options:
  - ◇ Security
    - ▷ Tanenbaum: "The *Security* option tells how secret the information is. In theory, a military router might use this field to specify not to route through certain countries the military considers to be 'bad guys.' In practice, all routers ignore it, so its practical function is to help spies find the good stuff more easily."
  - ◇ Strict source routing
    - ▷ Gibt den vollständigen Pfad zum Ziel vor.
  - ◇ Loose source routing
    - ▷ Gibt eine Liste von Routern vor, die auf jeden Fall verwendet werden müssen.
  - ◇ Record route
    - ▷ Jeder Router muß seine IP-Adresse anfügen.
  - ◇ Timestamp
    - ▷ Jeder Router muß seine IP-Adresse und einen Timestamp anfügen.

Maximum Transmission Unit (MTU)

Verschiedene Netzwerk-Technologien haben verschiedene MTU's (vgl. Tab. INW–1.) Dies führt dazu daß auch IP-Packete ggf. in Fragmente zerlegt werden müssen.

Netzwerk	MTU (Bytes)
16 Mbits/sec Token-Ring (IBM)	17914
4 Mbits/sec Token-Ring (IEEE 802.5)	4464
FDDI	4352
Ethernet	1500
IEEE 802.3	1492
ATM (LAN Emulation)	1500
ATM (Classical IP)	9180
PPP	1500

Tab. INW–1 MTU-Werte verschiedener Netzwerke

Path-MTU

- Bei zwei über ein einziges Netz verbundenen Rechnern ist die MTU direkt vom verwendeten Netzwerk abhängig.
- Bei zwei über mehrere Netze verbundenen Rechnern ergibt sich die nutzbare MTU aus dem Minimum aller MTU-Werte der verwendeten Netzwerk-Verbindungen.
  - *Path-MTU* bezeichnet diesen Wert.
- Die Path-MTU einer Verbindung kann mit IP und ICMP bestimmt werden.

Fragmentierung und Rekonstruktion

- "Fragmentation and Reassembly"
- IP–Datagramme sollen unabhängig von verwendeter Netzwerk-Technologie sein.
- Wenn Datagramme länger als die verwendete MTU sind, werden sie fragmentiert und beim Empfänger wieder zusammengesetzt.
- Strategie
  - Fragmentierung, wenn notwendig (MTU < Datagramm)
  - Versuche, Fragmentierung am Quellknoten zu vermeiden
  - Weitere Aufsplittung (von Fragmenten) auf dem Weg zum Ziel möglich
  - Fragmente sind selbständige Datagramme
  - Benutze CS-PDU (keine Zellen) für ATM
  - Verzögere die Rekonstruktion bis zum Zielknoten
  - Versuche nicht, verlorene Fragmente wiederzufinden
    - ◇ Somit führt ein verlorenes Fragment dazu, daß das gesamte Packet verloren ist. (alle anderen Fragmente sind wertlos)
    - ◇ Somit sollten Packete maximal mit der Path-MTU gesendet werden.
- Beispiel:
  Annahme: Ethernet-MTU = 1500 Bytes, FDDI-MTU = 4500 Bytes, P2P-MTU = 532 Bytes; Datagramm = 1420 Bytes (20-Byte IP Header plus 1400 Bytes Daten)

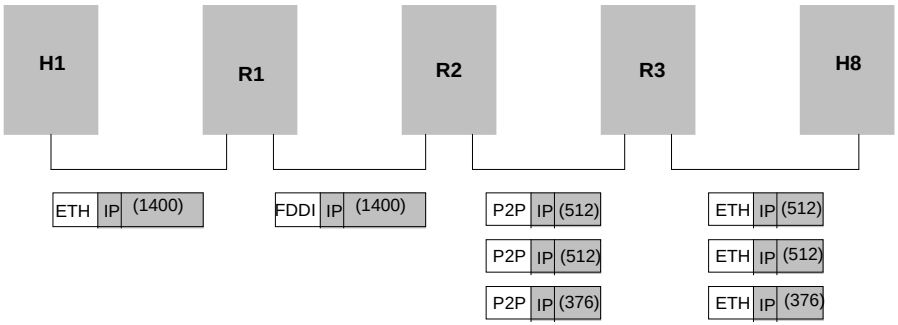

Abb. INW–4 Beispiel für IP-Fragmentierung

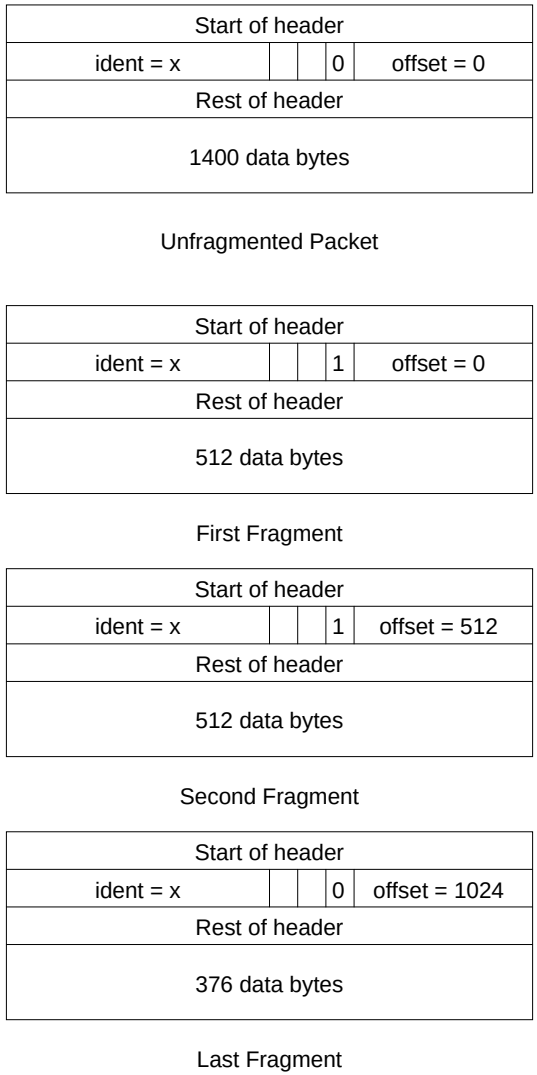

Abb. INW–5 Header-Felder im Beispiel für Fragmentierung

Adressierung

- Eigenschaften
  - global eindeutig, um jeden Knoten im Internet zu erreichen
  - hierarchisch: Netzwerk + Host
- Werden koordiniert vergeben vom *Network Information Center* (NIC)

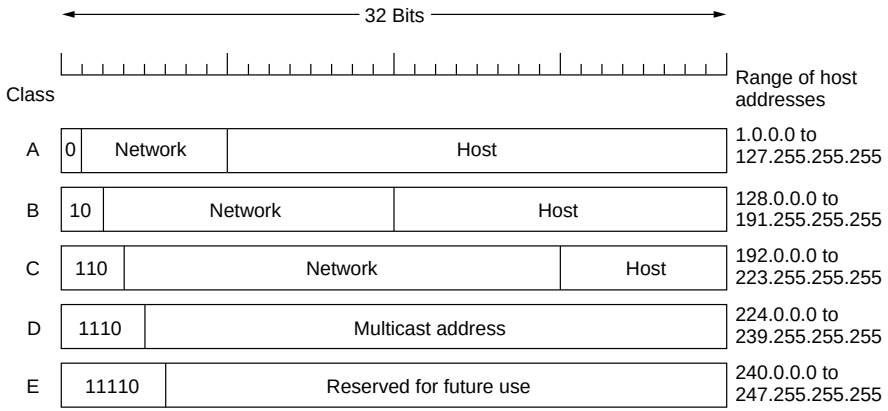

Abb. INW–6 Klassen von IP-Adressen.

- Klasse A:
  - 126 Netze zu je 16 Millionen Hosts
- Klasse B:
  - 16.382 Netze zu je 64K Hosts
- Klasse C:
  - 2 Millionen Netze zu je 254 Hosts
- Klasse D:
  - Multicast-Gruppen; nicht global eindeutig
- Klasse E:
  - Reserviert für zukünftigen Gebrauch

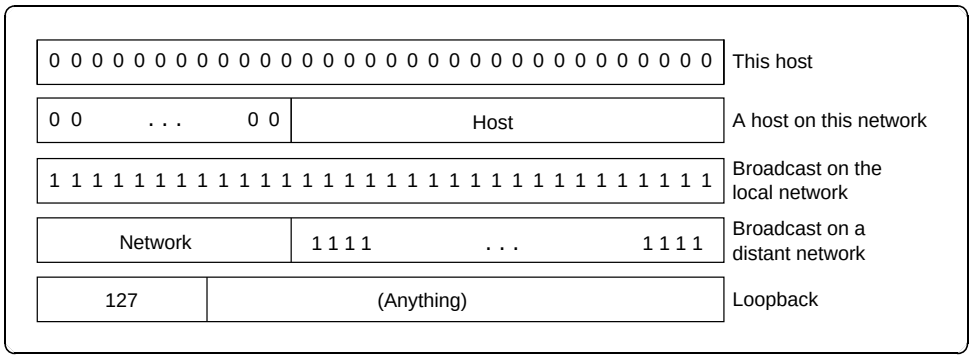

Abb. INW–7 Spezielle IP Adressen.

- Es gibt auch einige Adressen mit spezieller Bedeutung.
  - Broadcast-Adressen
  - Loopback (typischerweise 127.0.0.1), wird zur Kommunikation zwischen Prozessen auf dem gleichen Rechner verwendet.
    - ◇ Z.B. zu Testzwecken
    - ◇ Weil gleichzeitiges Senden und Empfangen normalerweise nicht möglich ist.
    - ◇ Weil Senden auf dem Netzwerk in diesem Fall auch gar nicht notwendig ist.

IP-Forwarding

Forwarding von IP-Packeten geschieht auf der Basis der Netzwerk-Nummern (der Netzwerk-Anteile der Adressen). Jedes IP-Datagramm enthält die IP-Adresse des Empfängers, somit wird jedes Datagramm isoliert zugestellt. Alle Knoten (Rechner und Router) mit gemeinsamer Netzwerk-Adresse bzw. Netzwerk-Nummer kommunizieren direkt über dieses Netzwerk. Die Kommunikation mit anderen Netzwerk-Nummern erfolgt über Router. Router haben im Allgemeinen mehrere Netzwerk-Interfaces; IP-Adressen werden den Interfaces zugeordnet und nicht den Routern. (Somit hat ein Router mehrere IP-Adressen.)

Das IP-Forwarding erfolgt in drei Schritten:

- Der Empfänger hat die gleiche Netz-Adresse:
  - direkt (auf dem gemeinsamen physikalischen Netz) versenden
- Der Empfänger hat eine andere Netz-Adresse und für diese Netz-Adresse existiert ein Eintrag in der Routing-Tabelle:
  - Sende an den “next hop” Router, der in der Tabelle angegeben ist
- Der Empfänger hat eine andere aber unbekannte Netz-Adresse:
  - Sende an den “default router”

Diese drei Routing-Ebenen unterstützen direkt die Skalierbarkeit von IP-Netzwerken: Entweder ein Rechner kann ein Datagramm direkt zustellen, oder der Rechner kennt einen Router, der das Datagramm zustellen kann, oder der Default-Router leitet das Datagramm (an unbekannte oder bzw. weit entfernte Netze) weiter.

Auch die MAC-Adressen der Netzwerk-Adapter sind global eindeutig. Allerdings sind diese nicht für das Routing brauchbar, da es für MAC-Adressen keine sinnvolle räumliche Zuordnung gibt. (Außer man konstruiert Forwarding-Tabellen mit 2^{48} Einträgen, was natürlich nicht realisierbar ist.)

Beispiel für IP Forwarding-Tabellen

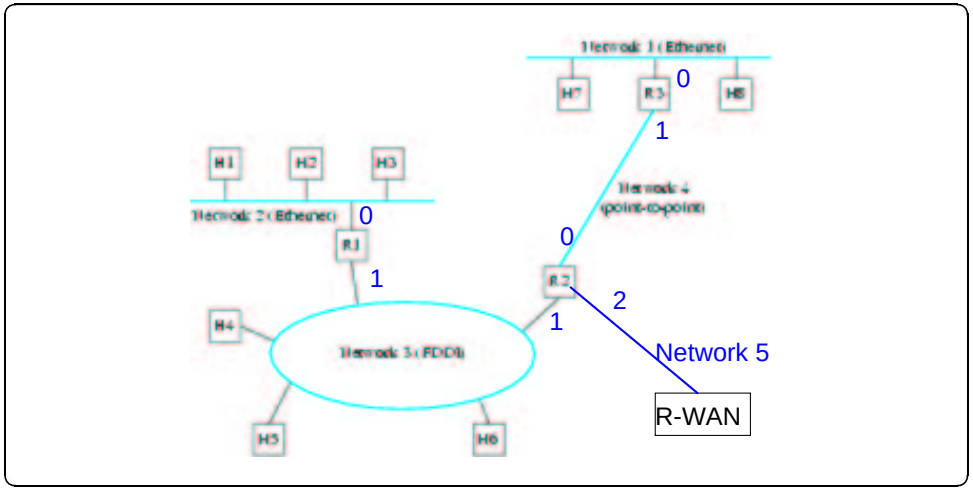

Abb. INW–8 Beispiel für IP Forwarding-Tabellen

Abb. INW–8 erweitert das Internetwork aus Abb. INW–1 um eine Anbindung über ein WAN (z.B. an das Internet). Router R2 hat dann die folgende Forwarding-Tabelle:

Netzwerk Nr.	Empfänger
1	R3
2	R1
3	Interface 1
4	Interface 0
5	Interface 2
default	R-WAN

Übung: Erstellen Sie analog Forwarding-Tabellen für die Router R1 und R3, sowie für die Hosts H1 und H8! (Dabei sei das einzige Netzwerk-Interface eines Hosts das Interface 0.)

Internet Kontroll–Protokolle

Address Resolution Protocol (ARP)

- Ziel: Bilde IP-Adressen auf physikalische Adressen (MAC) ab
  - "Wer hat IP-Adresse A.B.C.D?"
  - Um einen Ziel-Host oder Next-Hop-Router zu finden.
- Techniken
  - kodiere die physikalische Adresse in dem Host-Teil der IP-Adresse
    - ◇ Nicht wirklich realisierbar, da den MAC-Adressen die räumliche Zuordnung fehlt.
  - verwende Tabelle
    - ◇ statische Zuordnung, nur schwer zu verwalten (Änderungen)
- *Adress Resolution Protocol (ARP)*
  - Tabelle, die IP-Adressen auf physikalischen Adressen abbildet
  - Verwende Broadcast, falls IP-Adresse nicht in der Tabelle ist
  - Ziel-Maschine antwortet mit ihrer physikalischen Adresse
  - Tabellen-Einträge werden vernichtet, falls sie nicht verwendet bzw. erneuert werden
- ARP-Paket Format

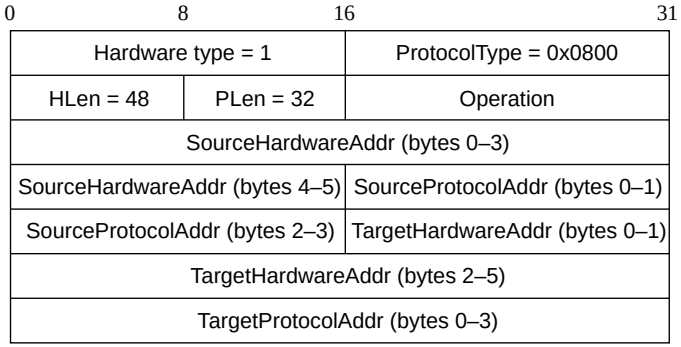

Abb. INW–9 ARP-Paket Format

  - Hardware-Typ: Art des physikalischen Netzwerks (z. B. Ethernet)
  - Protokolltyp: Art des höheren Protokolls (z. B. IP)
  - HLEN & PLEN: Länge der physikalischen und Protokoll-Adressen
  - Operation: Anfrage oder Antwort
  - Quelle/Ziel physikalische/Protokoll-Adressen
- Anmerkungen:
  - Tabelleneinträge werden ca. alle 10-15 Minuten ungültig
  - bringe die Tabelle mit der Quelle auf den neuesten Stand, wenn du das Ziel bist
    - ◇ (wird mit hoher Wahrscheinlichkeit für ein Antwort-Paket benötigt)
  - bringe die Tabelle auf den neuesten Stand, wenn du bereits einen Eintrag hast
  - erneuere keine Tabelleneinträge, falls nicht selbst Zielknoten
- Beispiel:
  - UNIX Utility arp zeigt den aktuellen Inhalt der ARP-Tabelle an.

```
paragon:~ $ arp -a
paragon:~ $ telnet pinkfloyd
Trying 141.99.130.23...
Connected to pinkfloyd.informatik.uni-siegen.de.
...

paragon:~ $ arp -a
pinkfloyd.informatik.uni-siegen.de (141.99.130.23) at 08-00-2b-31-ab-b8
paragon:~ $ ping parabola2
PING parabola2.informatik.uni-siegen.de (141.99.130.201): 56 data bytes
...

paragon:~ $ arp -a
pinkfloyd.informatik.uni-siegen.de (141.99.130.23) at 08-00-2b-31-ab-b8
parabola2.informatik.uni-siegen.de (141.99.130.201) at 08-00-09-64-43-d6
```

Zu Beginn ist die ARP-Tabelle leer. Nach einer telnet-Verbindung zum Host pinkfloyd ist dessen Ethernet-Adresse im ARP-Cache. Nach einem ping zum Drucker parabola2 ist auch dessen Ethernet-Adresse im ARP-Cache.

Classical IP over ATM: ATMARP

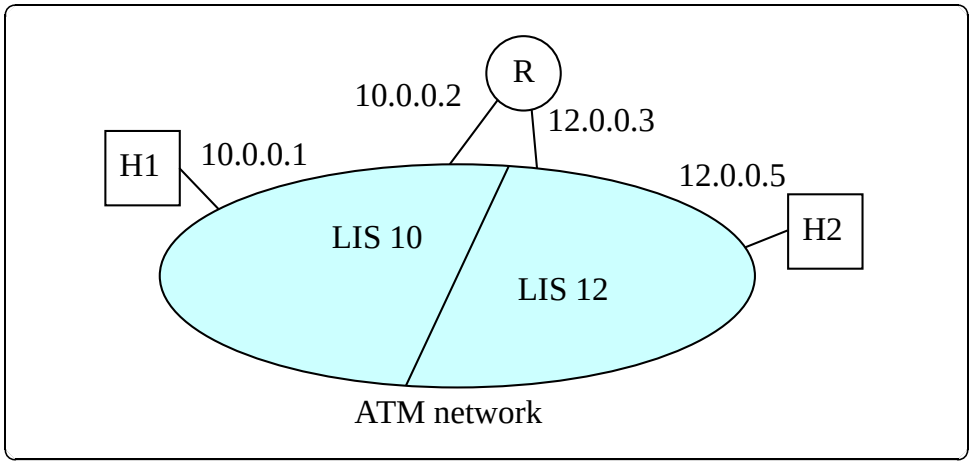

Abb. INW–10 Logische IP-Subnetze (LIS)

Abb. INW–10 zeigt ein Classical IP over ATM Netzwerk, in dem auf einem physikalischen ATM-Netz mehrere logische IP Subnetze (LIS) vorhanden sind.

Da ATM nicht über eine Broadcast-Möglichkeit verfügt, kann auch kein ARP-Protokoll benutzt werden. (vgl. Kapitel über ATM) Die LAN Emulation (LANE) emuliert LAN-Funktionalität über diverse Server, allerdings ist LANE schlecht skalierbar, da hier zu viele Broadcasts verschickt werden müssen um ARP zu simulieren. Bei "Classical IP" wird stattdessen ein dedizierter ATMARP-Server eingesetzt, der zentral eine ARP-Tabelle verwaltet. Pro LIS wird ein ATMARP Server verwendet.

Ein Rechner muß beim Booten einen VC zum ATMARP-Server öffen. (Die ATM-Adresse des ATMARP-Servers muß dem Rechner per Konfiguration bekannt sein.) Dabei registriert sich der Rechner mit seiner ATM-Adresse und seiner IP-Adresse. Die Auflösung unbekannter IP-Adressen funktioniert dann durch direkte Anfrage beim ATMARP-Server (ohne Broadcast).

Der Name "Classical IP" kommt daher, daß alle Rechner im gleichen LIS direkt miteinander kommunizieren können. Somit paßt dieses Schema direkt in die Strategie zum IP-Forwarding.

Dynamic Host Configuration Protocol (DHCP)

Auch die Zuteilung von IP-Adressen an Rechner bedeutet administrativen Aufwand. Beim Transport eines Rechners (oder vieler Rechner) in ein anderes Netzwerk kann dies erheblichen Aufwand bedeuten. Insbesondere mobile Rechner (z.B. Laptops mit drahtlosem Ethernet) benötigen des öfteren andere IP-Adressen.

Das DHCP Protokoll (Dynamic Host Configuration Protocol) ermöglicht die Zuweisung von IP-Adressen ganz ohne Rechner-Konfiguration. (siehe Abb. INW–11)

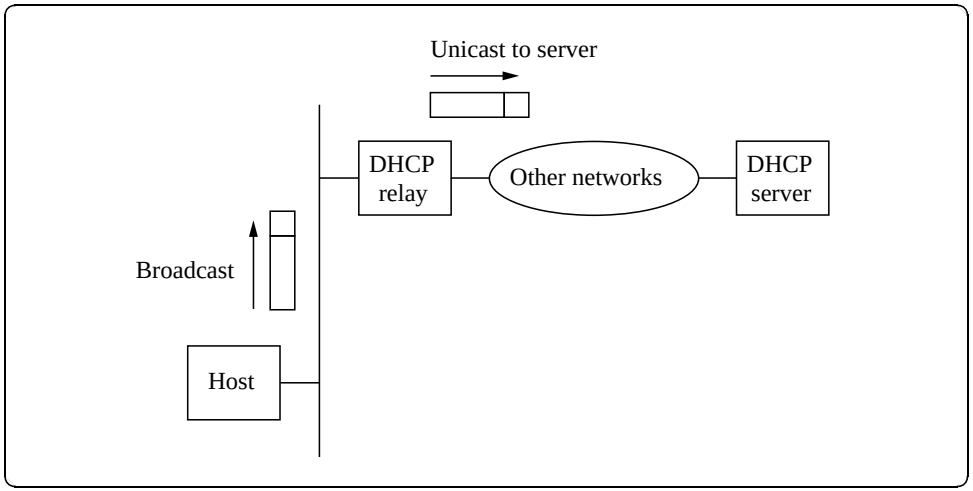

Abb. INW–11 Ein DHCP Relay-Agent empfängt eine Broadcast-DHCPDISCOVER Nachricht von einem Host und sendet ein Unicast-DHCPDISCOVER an den DHCP-Server.

Um eine IP-Adresse zu bekommen, schickt ein Host eine Broadcast-Nachricht (DHCPDISCOVER) über sein Netzwerk-Interface. Ein DHCP-Server antwortet mit einer Unicast-Nachricht. Allerdings werden Broadcast-Nachrichten von Routern nicht weitergeleitet. (Sonst würde jeder Broadcast automatisch im gesamten Internet verbreitet.) Um nicht in jedem physikalischen Netzwerk einen DHCP-Server installieren zu müssen (und ein Kontingent IP-Adressen dafür zu reservieren), können sog. DHCP-Relays eingesetzt werden, die Broadcasts empfangen und per Unicast an den eigentlichen Server weiterleiten.

Die Zuweisung einer IP-Adresse geschieht auf einer "Leasing-Basis", also für eine gewisse Zeitspanne. Nach Ablauf dieser Zeitspanne wird die IP-Adresse automatisch freigegeben, es sei denn, der Host erneuert das Leasing der Adresse nicht beim Server. Somit werden Adressen (z.B. nach Crashs) automatisch freigegeben.

DHCP ist eine Weiterentwicklung von BOOTP, einem Protokoll zum Booten von Rechnern über das Netzwerk. Deshalb enthalten DHCP-Packete ggf. noch weitere Informationen wie Rechnernamen und Dateinamen von Systemsoftware zum Download beim Booten.

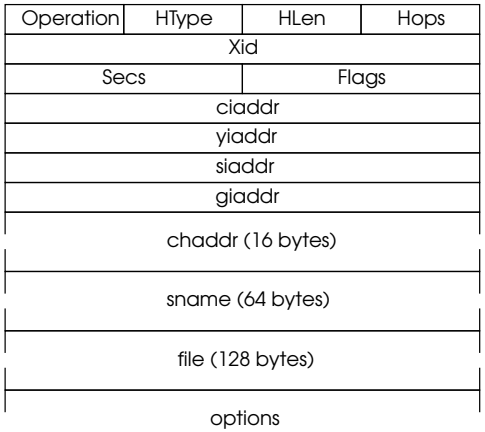

Abb. INW–12 DHCP Packet-Format.

Internet Control Message Protocol (ICMP)

- Über ICMP können Kontroll–Nachrichten (insbesondere Fehlermeldungen) verschickt werden.
- ICMP–Datagramme werden in IP–Paketen verschickt.

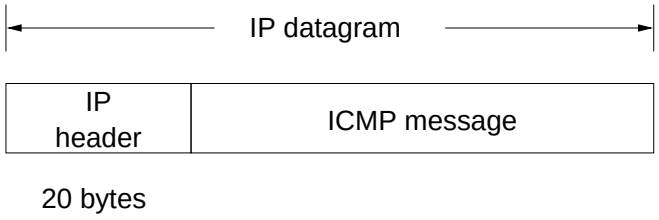

Abb. INW–13 Eine ICMP-Nachricht, verpackt in einem IP-Datagramm.

Message Type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

Tab. INW–2 Die wichtigsten ICMP Nachrichten-Typen.

Packet InterNet Groper (PING)

- UNIX Utility, testet ob andere Hosts erreichbar sind.
- Basiert auf ICMP, Echo Request/Reply
- Vorsicht:
  - Wenn ein Host nicht auf ping reagiert, bedeutet dies heute nicht unbedingt, daß der Host überhaupt nicht erreichbar ist!
  - Ein Firewall-Router auf dem Weg zu diesem Host könnte ggf. ICMP ausfiltern, Applikations–Protokolle jedoch durchlassen.
- ping in einem LAN:

```
paragon:~ $ ping cocker
PING cocker.informatik.uni-siegen.de (141.99.92.4): 56 data bytes
64 bytes from 141.99.92.4: icmp_seq=0 ttl=64 time=13 ms
64 bytes from 141.99.92.4: icmp_seq=1 ttl=64 time=0 ms
64 bytes from 141.99.92.4: icmp_seq=2 ttl=64 time=0 ms
64 bytes from 141.99.92.4: icmp_seq=3 ttl=64 time=0 ms
64 bytes from 141.99.92.4: icmp_seq=4 ttl=64 time=0 ms
64 bytes from 141.99.92.4: icmp_seq=5 ttl=64 time=1 ms

----cocker.informatik.uni-siegen.de PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/2/13 ms
```


- ping in einem WAN:

```
paragon:~ $ ping cclab.konkuk.ac.kr
PING cclab.konkuk.ac.kr (203.252.134.46): 56 data bytes
64 bytes from 203.252.134.46: icmp_seq=0 ttl=242 time=464 ms
64 bytes from 203.252.134.46: icmp_seq=1 ttl=242 time=330 ms
64 bytes from 203.252.134.46: icmp_seq=2 ttl=242 time=338 ms
64 bytes from 203.252.134.46: icmp_seq=3 ttl=242 time=303 ms
64 bytes from 203.252.134.46: icmp_seq=5 ttl=242 time=314 ms
64 bytes from 203.252.134.46: icmp_seq=6 ttl=242 time=323 ms
64 bytes from 203.252.134.46: icmp_seq=7 ttl=242 time=321 ms

----cclab.konkuk.ac.kr PING Statistics----
8 packets transmitted, 7 packets received, 12% packet loss
round-trip (ms)  min/avg/max = 303/342/464 ms
```

- ping mit Record Route Option (IP)
- Vorsicht: IP-Header hat nur Platz für neun RR-Einträge!

```
paragon:~ $ ping -R harley.unix-ag.uni-siegen.de
PING harley.unix-ag.uni-siegen.de (141.99.42.44): 56 data bytes
64 bytes from 141.99.42.44: icmp_seq=0 ttl=62 time=9 ms
RR:     fddi-gw.informatik.uni-siegen.de (141.99.216.254)
        gate.unix-ag.uni-siegen.de (141.99.42.254)
        harley.unix-ag.uni-siegen.de (141.99.42.44)
        harley.unix-ag.uni-siegen.de (141.99.42.44)
        ether-gw.informatik.uni-siegen.de (141.99.216.252)
        atm-gw.informatik.uni-siegen.de (141.99.92.254)
        paragon.informatik.uni-siegen.de (141.99.92.2)
64 bytes from 141.99.42.44: icmp_seq=1 ttl=62 time=6 ms (same route)
64 bytes from 141.99.42.44: icmp_seq=2 ttl=62 time=6 ms (same route)

----harley.unix-ag.uni-siegen.de PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 6/7/9 ms
```

ICMP Redirect Pakete

- Werden von einem Router an den Absender eines IP Datagramms geschickt, wenn dieses an einen anderen Router hätte gehen sollen.

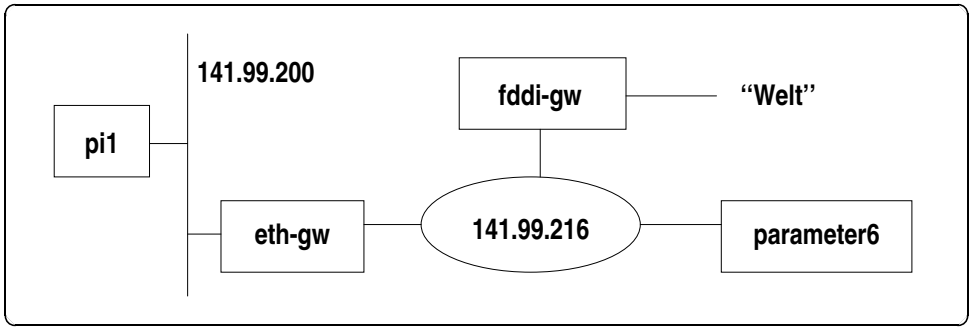

Abb. INW–14 Szenario für das Redirect-Beispiel.

- Beispiel:
  - parameter6 schickt ping-Paket an pi1.
  - Die (Netz-)Adresse von pi1 ist bei parameter6 nicht bekannt.
  - Somit gehen ping-Pakete über den Default-Router (fddi-gw).
  - fddi-gw bekommt das erste Paket und stellt fest, daß es über den Router eth-gw geschickt werden muß.
  - fddi-gw schickt Paket an eth-gw.
  - fddi-gw bemerkt, daß das Paket auf dem gleichen Interface wieder ausgesendet wird, auf dem es angekommen ist.
    - ◇ Demzufolge könnte parameter6 das Paket auch direkt an eth-gw schicken.
  - fddi-gw informiert parameter6 darüber mit einem ICMP Redirect Paket.

- ping -v zeigt ICMP Pakete an:

```
parameter6:~ $ ping -v pi1
PING pi1 (141.99.200.1): 56 data bytes
64 bytes from 141.99.200.1: icmp_seq=0 ttl=254 time=5 ms
36 bytes from fddi-gw.informatik.uni-siegen.de (141.99.216.254):
   Redirect Host(New addr: 0xffffffffcd8638d)
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst Data
 4  5  00 5400 0c93   0 0000  40  01 ce2c 141.99.216.6  141.99.200.1

64 bytes from 141.99.200.1: icmp_seq=1 ttl=254 time=3 ms

----pi1 PING Statistics----
2 packets transmitted, 2 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 3/4/5 ms
```

- Danach ist die Route bei parameter6 direkt eingetragen:

```
parameter6:~ $ netstat -r
Routing tables
Destination      Gateway            Flags     Refs     Use  Interface
Netmasks:
Inet             255.255.255.0

Route Tree for Protocol Family 2:
default          fddi-gw.informatik UG          9    21760  fta0
localhost        localhost          UH          5     5238  lo0
ethernet         parameter6-eth.Inf U           4     1313  ln0
appletalk        met                UG          0        0  ln0
pi1              ether-gw.informati UGHD        0        0  fta0
141.99.216       parameter6.informa U          12     4676  fta0
```

Virtuelle Private Netzwerke (VPN)

Die bisherigen Überlegungen in diesem Kapitel hatten zum Ziel, mehrere Netzwerke miteinander zu verbinden, wobei Rechner in allen Netzwerken miteinander kommunizieren können sollen. Dieses Ziel des Internetworkings ist das am weitesten verbeitete. Allerdings gibt es auch Situationen, in denen die Möglichkeit uneingeschränkter Kommunikation unerwünscht ist. Abb. INW–15 zeigt ein Beispiel dafür. Hier unterhalten die Firmen X und Y jeweils private Netzwerke zwischen ihren Standorten. Aus Geheimhaltungsgründen für interne Daten ist es dabei unerwünscht, daß Rechner der einen Firma mit Rechnern der anderen Firma kommunizieren können.

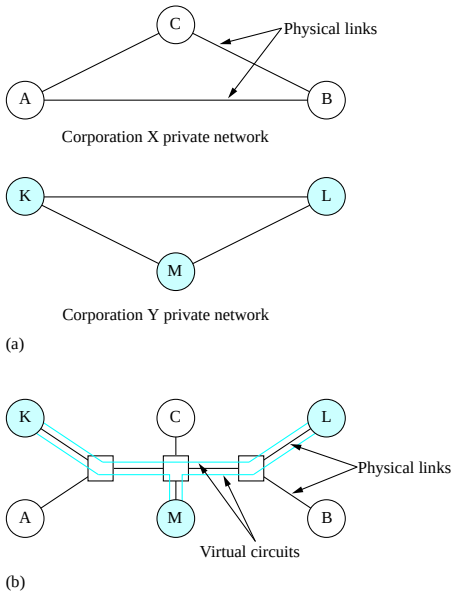

Abb. INW–15 Private Netzwerke
(a) separate private Netzwerke
(b) virtuelle private Netzwerke mit gemeinsamen Switches

Die einfachste Lösung dieses Problems ist es, private Netzwerke aufzubauen (z.B. mit gemieteten Standleitungen). Allerdings ist dies auch die teuerste Lösung. Etwas einfacher wird es, zwar die physikalischen Leitungen mit anderen Firmen gemeinsam zu nutzen, aber auf diesen Leitungen private Virtual Circuits (VCs) zu betreiben. Diese Lösung setzt allerdings voraus, daß das gesamte (wide-area) Netzwerk mit ATM-Hardware aufgebaut ist.

IP-Tunneling

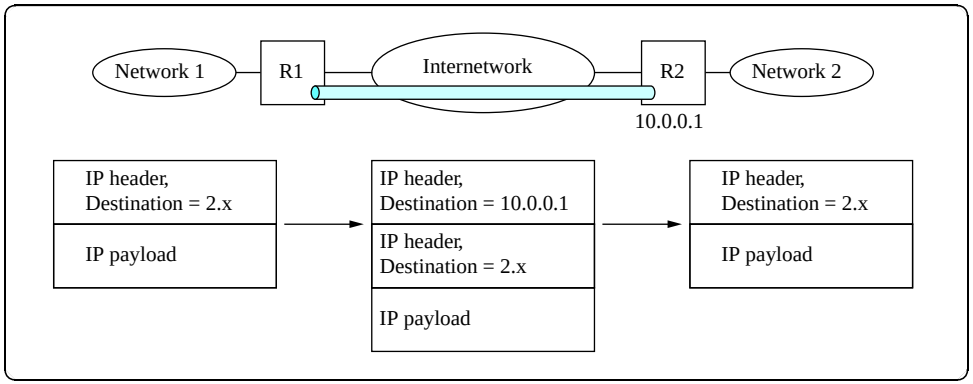

Abb. INW–16 IP Tunneling

Abb. INW–16 zeigt eine Technik zum Aufbau virtueller privater Netzwerke, die ohne private Leitungen und ohne spezielle Hardware-Anforderungen auskommt. Lediglich die Router, die die Teilnetze eines VPN miteinander verbinden, müssen erweiterte Funktionaliät besitzen.

Ein sogenannter *IP-Tunnel* wird zwischen zwei Routern aufgebaut. IP-Packete von Netzwerk 1 für Empfänger in Netzwerk 2 werden in R1 in ein weiteres IP-Packet für R2 eingepackt und als Payload (Benutzer-Daten) in diesem Packet über das Internetwork transferiert. Durch geeignete Konfiguration der Router an den Enden eines Tunnels kann gesteuert werden, ob die Rechner in den Netzwerken 1 und 2 nur miteinander oder auch mit Rechnern in anderen Netzwerken kommunizieren können.

Tunneling kann auch für andere Zwecke inegesetzt werden:

- Durch Verschlüsselung der “getunnelten” Packete kann weitere Sicherheit erreicht werden.
- Über einen Tunnel können auch Packete anderer Protokolle (z.B. Novell’s IPX oder Appletalk) übertragen werden, ohne daß die Router/Switches im Internetwork dafür geeignet sein müssen.