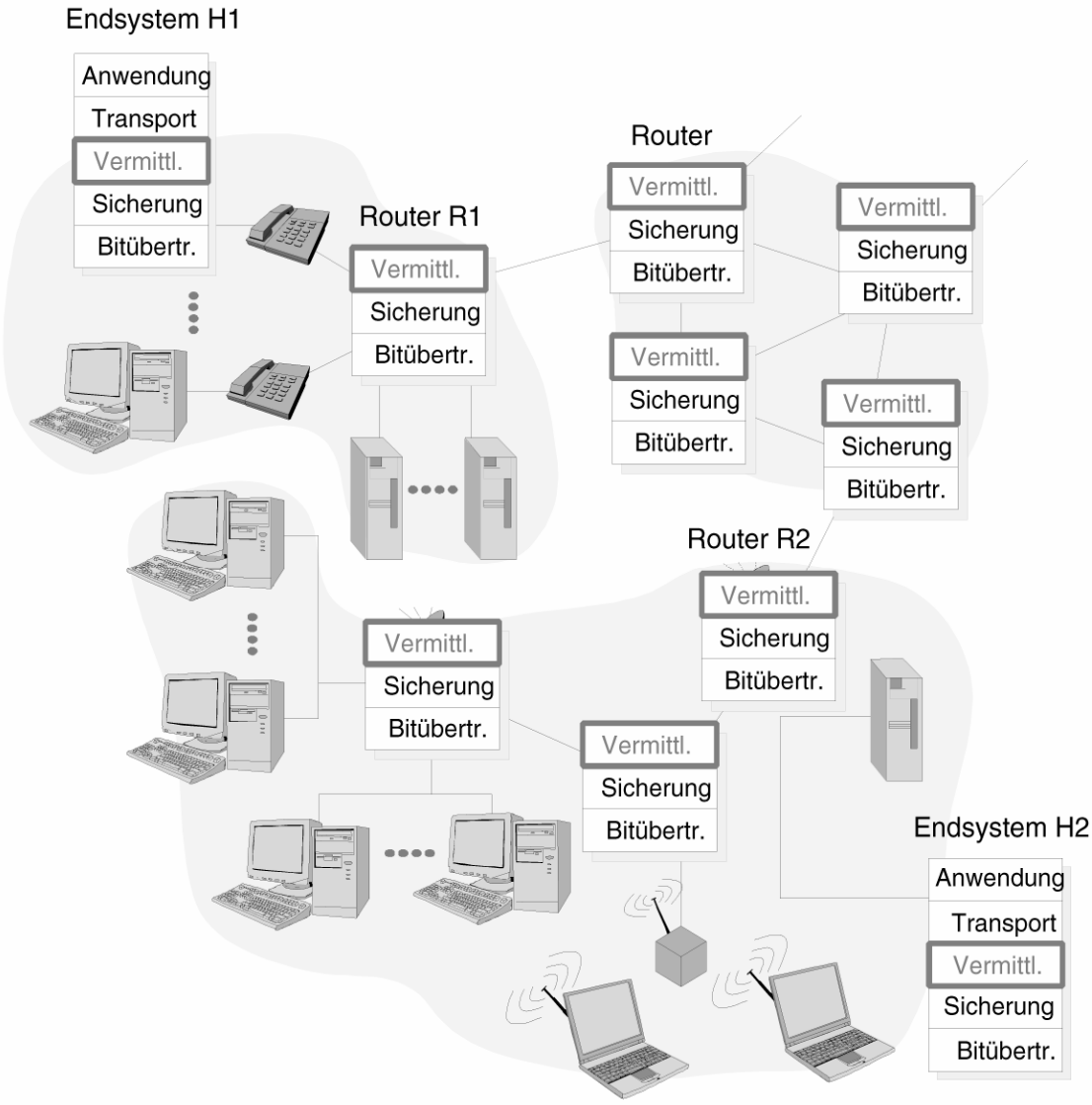
Kap. 3

Netzwerk – Schicht
(Vermittlungsschicht)

Vermittlungsschicht (Netzwerk-Schicht)

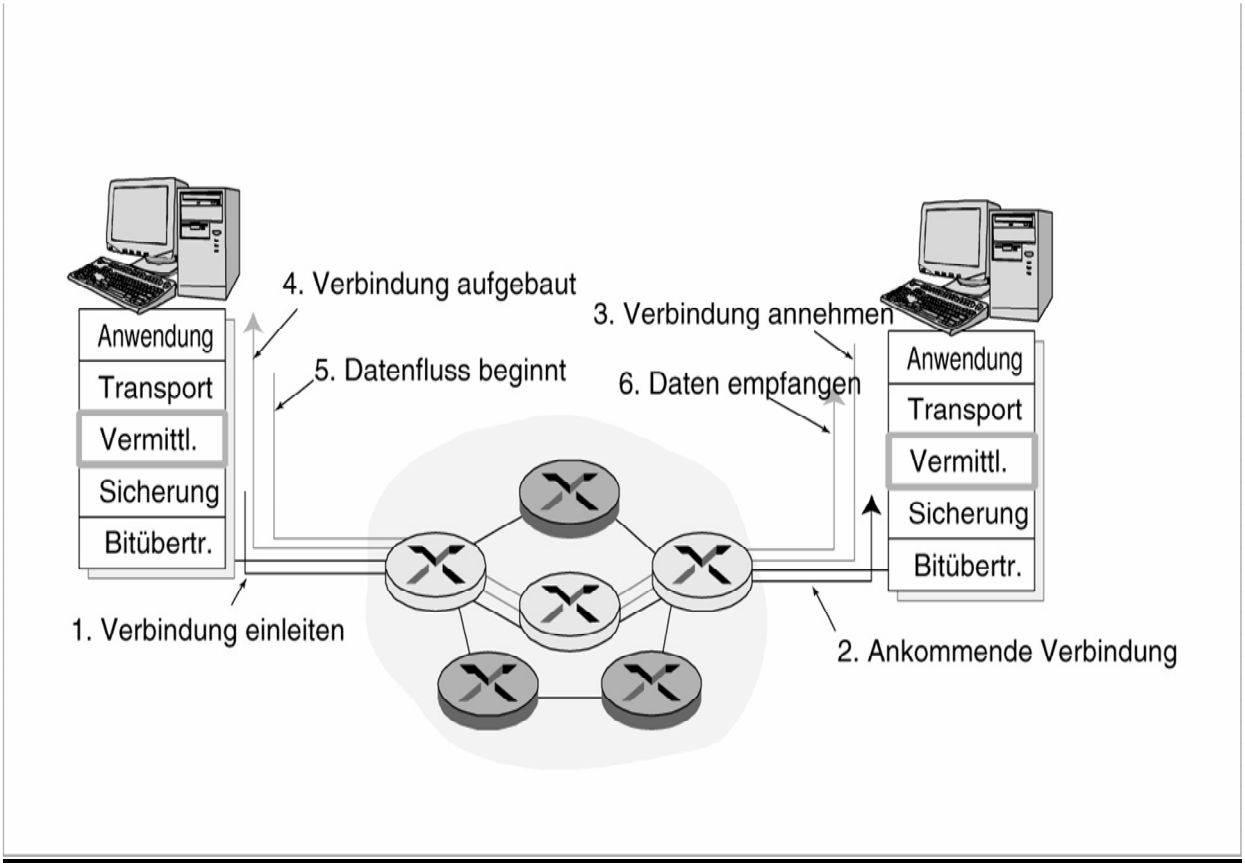


Rolle: - Ermittlung des Pfades zwischen End-Systemen
- Vermittlung von Paketen vom Router zu Router bis zum End-System basierend auf sog. Routing-Prinzipien

Komponenten: involviert sind alle Hosts und Router des Pfades

Routing: besteht aus Routing-Algorithmen und Routing-Protokollen

Netzwerkdienst-Modell (1)

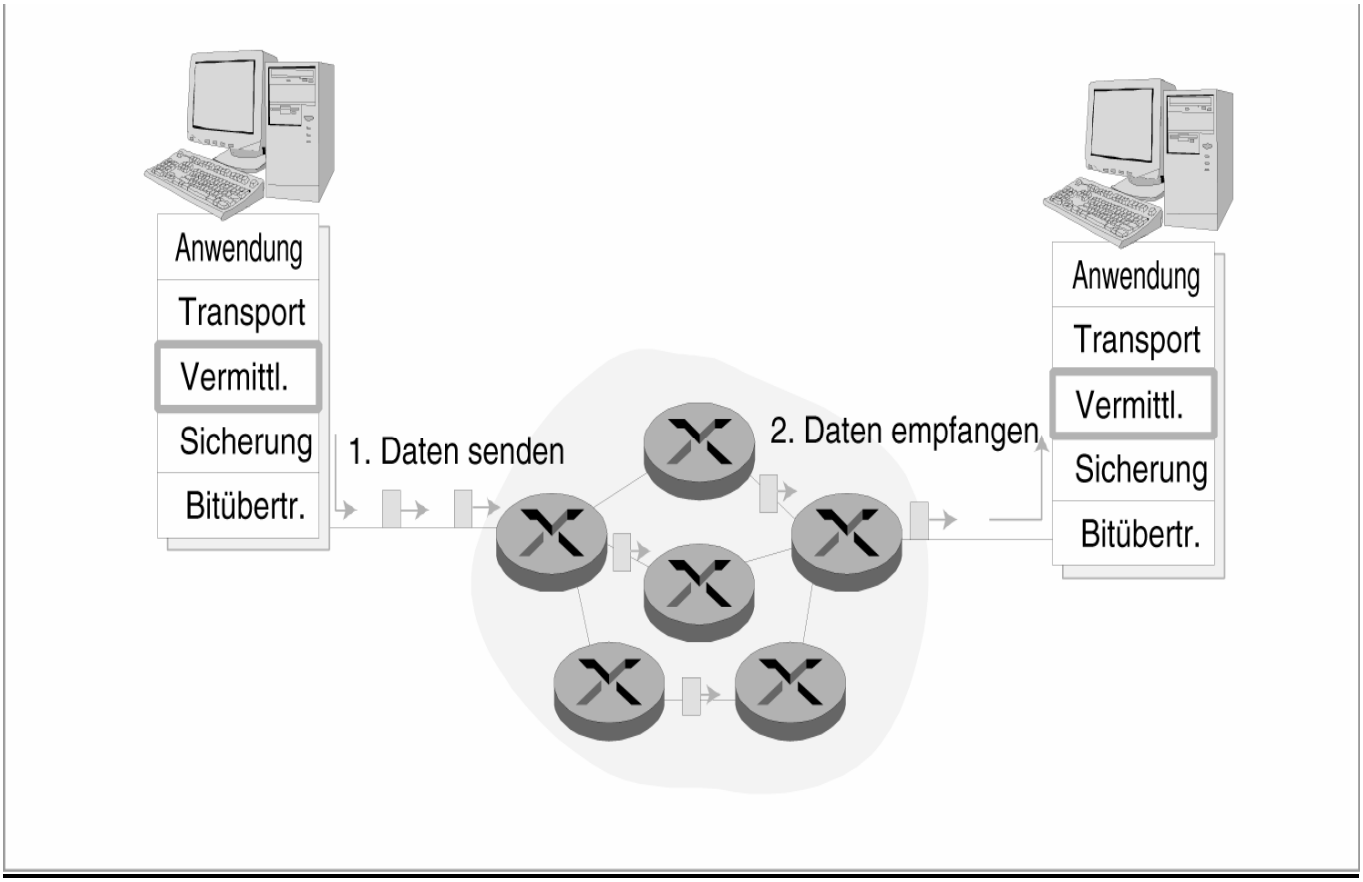


Rolle: definiert die Merkmale des End-To-End-Transports von Daten zwischen Endsystemen

Varianten: 1) virtuelle Kanäle (***Virtual Circuits***, VCs)
2) ***Datagramm***

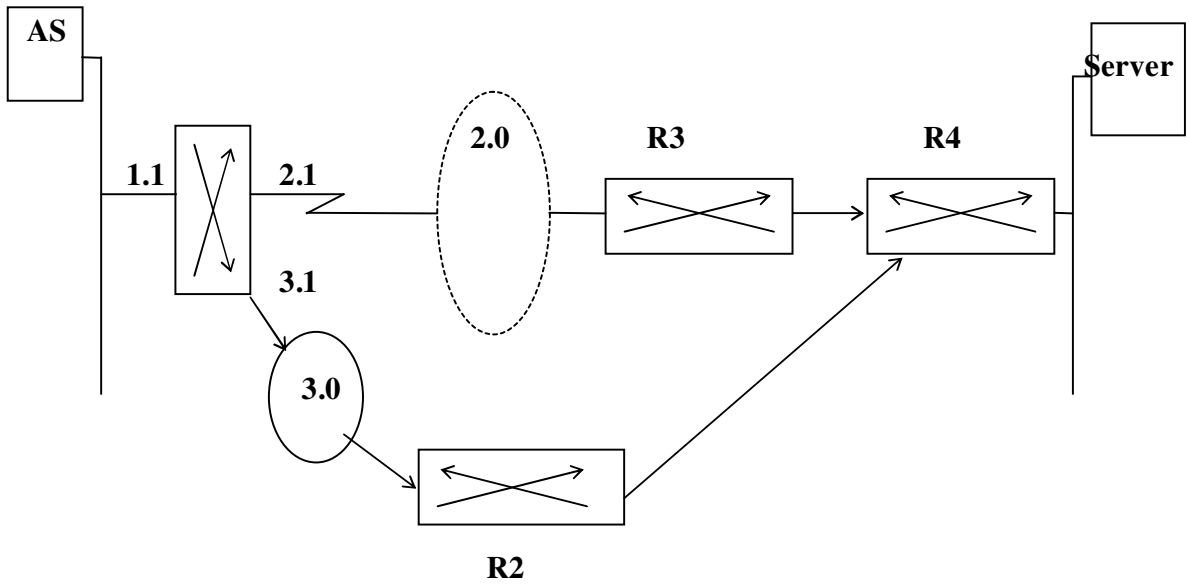
1) VC-Phasen: 1) VC-Setup: VC wird eingerichtet
Es wird der Pfad zwischen Sender und Empfänger bestimmt. Dies erfolgt per Signalisierungs-Protokolle (X.25, Frame Relay)
2) Datentransfer (DÜ)
3) VC-Abbau: nach dem die DÜ beendet ist

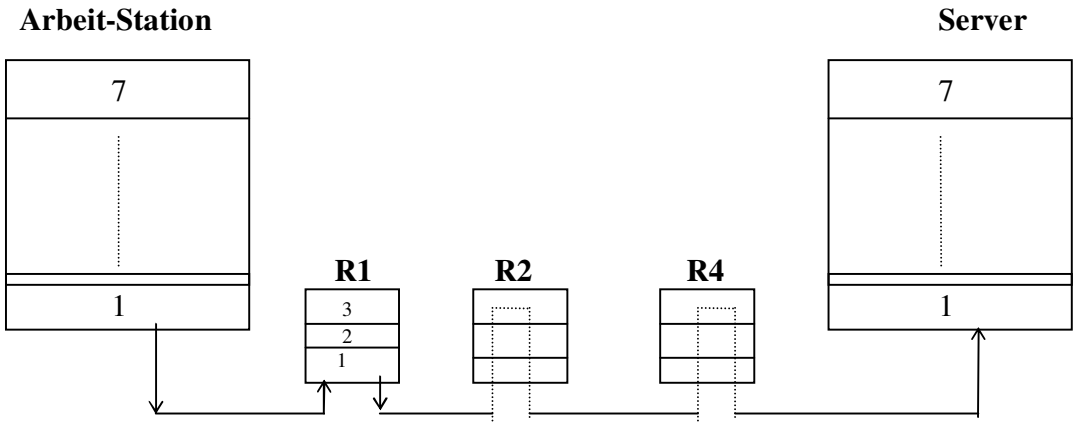
Netzwerkdienst-Modell (2)



2) Datagramm: Das Paket wird jedesmal mit der Adresse des Zielsystems versehen und dann das Paket in das Netzwerk eingespeist.
Das Paket wandert von Router zu Router bis zum Ziel-System. Die Übertragung erfolgt nach dem „***Best- Effort*** „ Prinzip.

Arbeitsprinzip des Netzwerk-Layers





Routing Mechanismus : Eigenschaften/Varianten

Definition:

Weiterleiten eines Pakets, d.h.:

- Feststellung eines Wegs basierend auf Netzw.-Adr.
- Auswahl eines entspr. Interface (Port) wegen Paket-weiterleiten (Paket- Switching)

Routed Protokol:

Ein Prot. daß ausreichend Informationen innerhalb des Headers beinhaltet um die Daten via versch. Netzbereich zwischen End- End Stationen transportieren zu können: Bsp. IP, IPX

Routing Protokolle:

Verwendet nur zwischen den Router wegen Austausch von Kontrol -Informationen wie z.B Routing Tabellen:
Bsp. RIP, IGRP, OSPF:

RIP= Routing Inform. Protokoll
IGRP = Interior Gateway Routing Protokoll
OSPF = Open Shortest Path First

„Routes"-Arten:

- *Static Route:* Die Routing-Information ist manuell von Administrator angegeben. Diese Information wird nicht an andere Router mitgeteilt.

- *Dynamic Route*: Die Routing-Information, die am Anfang eingetragen ist, wird dynamisch immer aktualisiert. Diese Update erfolgt jedesmal wenn eine Topology-Veränderung stattgefunden hat. Die Router tauschen Informtionen unter sich aus, um die jeweiligen sog. „Routing-Tabellen" zu aktualisieren. D. h. die Router müssen:
  - eine Routing-Tabelle administrieren
  - regelmäßige Informationen mit anderen Routern mittels sog. Routing-Protokollen austauschen.

- *Default-Route*: Die Route, die genommen werden muß, falls kein Antrag in der Tabelle für ein besonderes Netzwerk vorhanden ist.

Routing-Algorithmus: Der optimale Weg zwischen zwei Endstationen wird mittels sog. Routing-Alg. berechnet.

Berücksichtigte Faktoren:
Leitungskapazität, Verzögerung, Sicherheit, Anzahl Hops, Belastung, etc.

Basierend auf alle diese Faktoren wird eine Zahl generiert: sog. „Metric-Wert“ (MW).
Metric-Wert wird zu jedem „path“ zugeordnet: je kleiner den MW desto der „path“-optimaler.

Varianten:

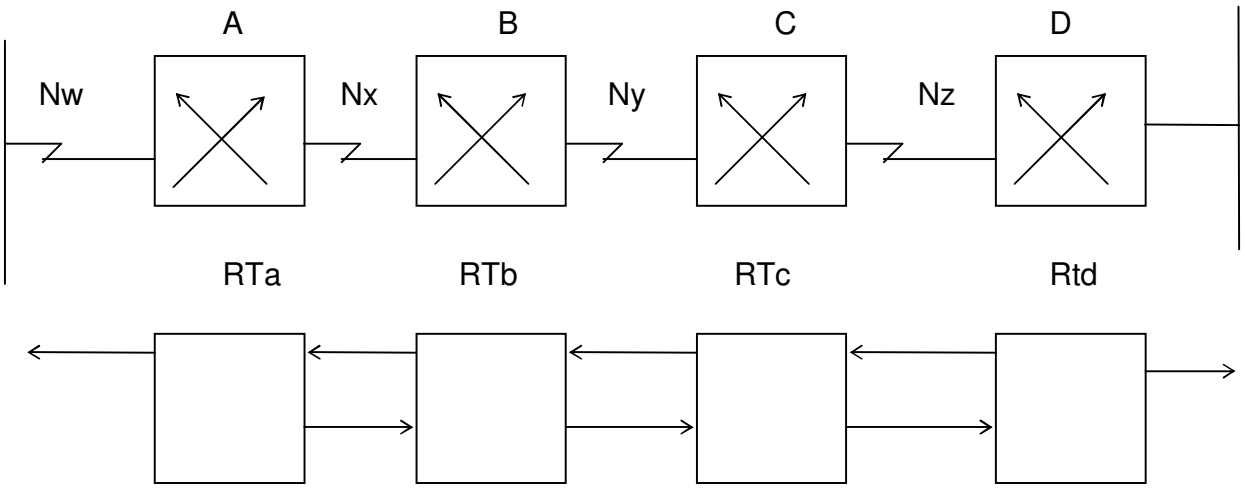
1) Distance Vector
2) Link-State
3) Hybrid Routing

Convergence-Konzept: - Alle Router des globalen Netzwerks müssen konsistenete Information (gleiche Inform.) über das globalen Netz haben

-Im Falle einer Veränderung der Netzwerk-Topology, die Router benötigen einen best. Zeitinterval um wieder konsistente Information zu erhalten:
d.h.:*“reconvergence“-Zeit*

Distance Vector Konzept

(Bellman-Ford-Algorithmus)



Prinzip: Nachbar-Router tauschen die R-Tabellen regelmäßig aus.
Jeder Router addiert eine entsprechende Distance-Vektor-Nummer (Nr. der „Hops“) und überträgt dann die Tabelle zum unmittelbar nächsten Nachbar.

Nachteil: Distance Vektor Alg. erlaubt einem Router nicht, die Kenntnisse über das ganze Netzwerk zu erhalten.

Beispiel:

RTa

Nw	←	**0**
Nx	→	**0**
Ny	→	**1**
Nz	→	**2**

RTb

Nx	←	**0**
Ny	→	**0**
Nw	←	**1**
Nz	→	**1**

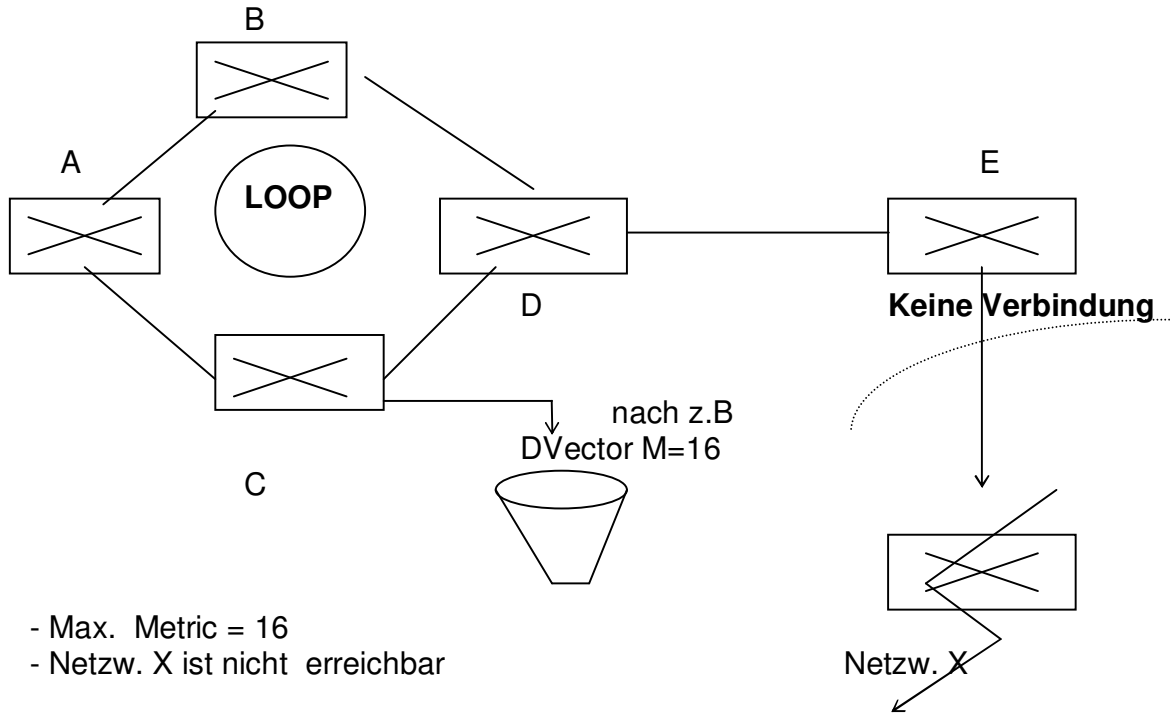
RTc

Ny	←	**0**
Nz	→	**0**
Nw	←	**2**
Nx	←	**1**

Probleme mit Distance-Vektor-Konzept

1) Routing Loops:

Falls nach einer Topology-Veränderung eine konsistente „Convergence“ nicht rechtzeitig erreicht werden kann, entstehen sog. Loops;
d. h. : Pakete zirkulieren unendlich zwischen den Routern des globalen Netzwerkes.



- Max. Metric = 16
- Netzw. X ist nicht erreichbar

2) „Counting to Infinity“

Die Router, die in dem Loop involviert sind, informieren sich irrtümlicherweise gegenseitig. Das Paket erhöht seine sog. hop-zähler jedesmal wenn es einen Router passiert hat; d.h. „counting to infinity“.

Lösung:

a) **Max. Distance Vector Metric**:

Festlegung eines festen max. Wertes für die Metric.
Ergebnis:
Das Paket wird verworfen; das Empfangsnetz wird als unreachable betrachtet.

b) **Split Horizon**:

Falls eine Route via einer bestimmten Schnittstelle des Routers erfahren worden ist, dann ist es nicht erlaubt, Informationen dieser besonderen Route via derselben Schnittstelle in das globale Netz weiterzuleiten.

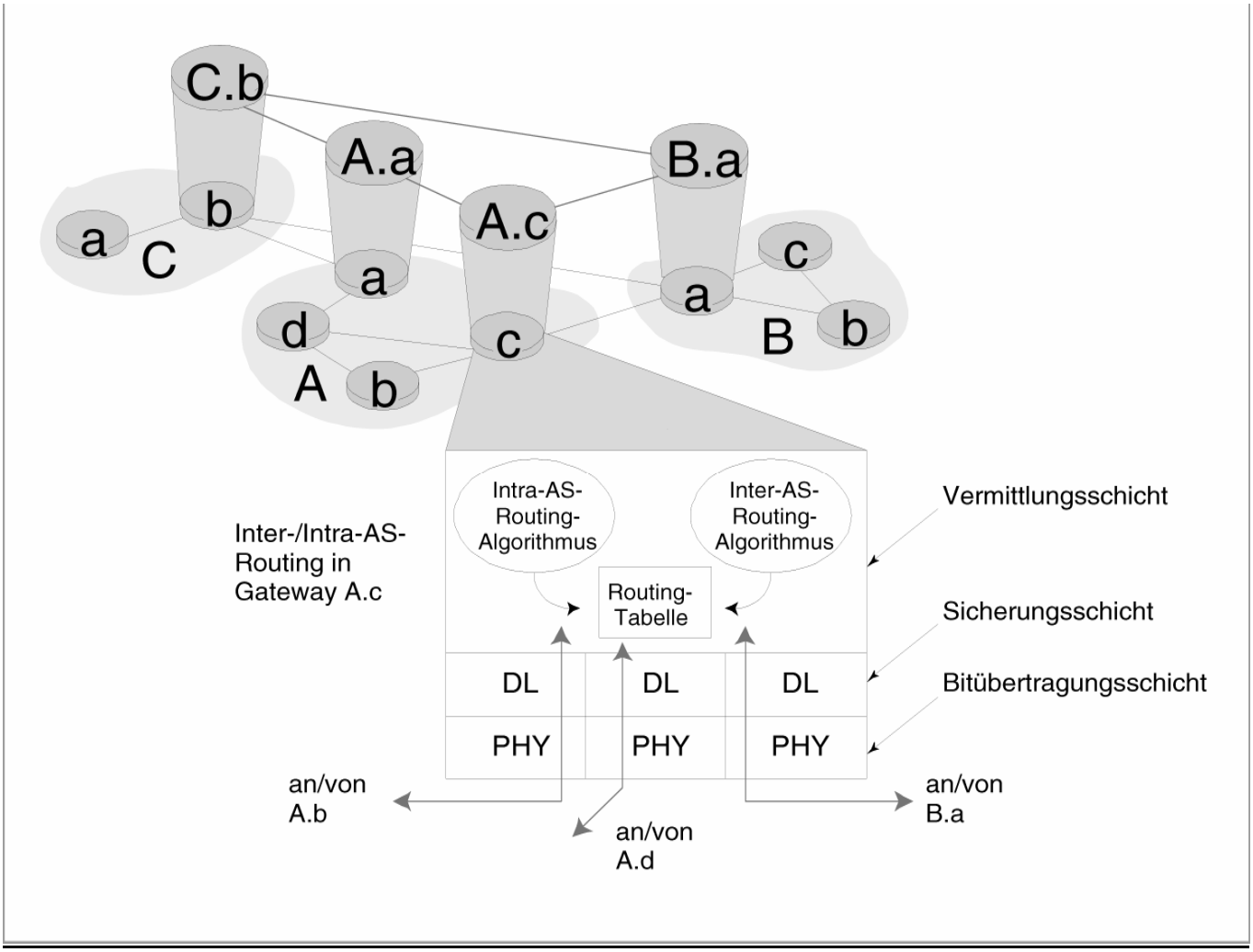
c) **Route Poisoning**:

Die Information über das nicht mehr erreichbare Netzwerk wird von den unmittelbaren Router für eine gewisse Zeit lokal behalten; sie wird nicht weitergeleitet.

d) **Hold down Timers**:

Router ignorieren für eine kurze Zeit alle Topology-Veränderungen, die von Nachbarn mitgeteilt worden sind.

Hierarchisches Routing (1) : Intra-AS- und Inter-AS- Routing

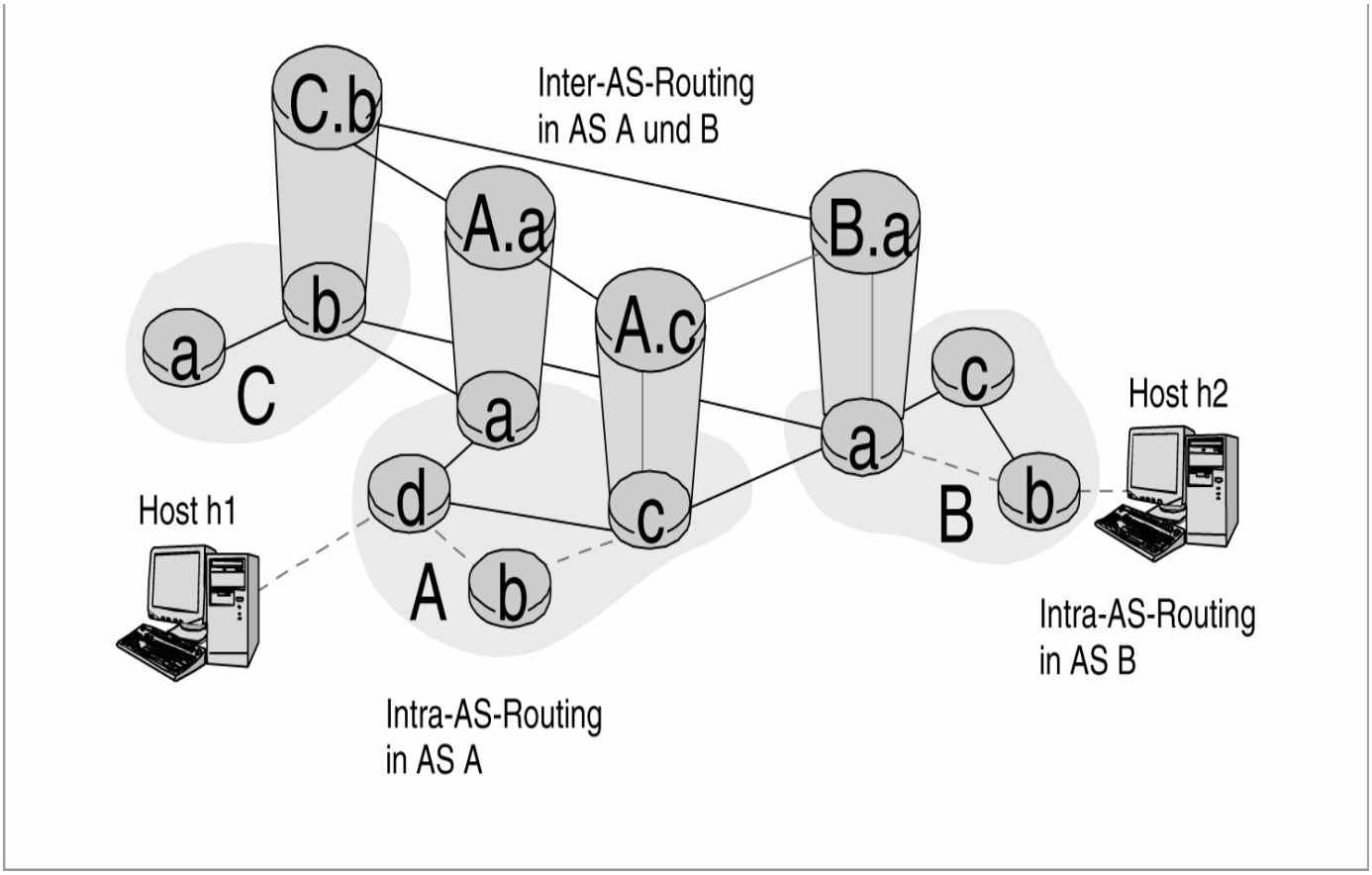


- **Implementierungsprobleme:**

- ***Skalierung***: Bei großer Anzahl von Routern steigt der Overhead für: Berechnung, Speicherung und Übermittlung der Informationen in den RTabellen

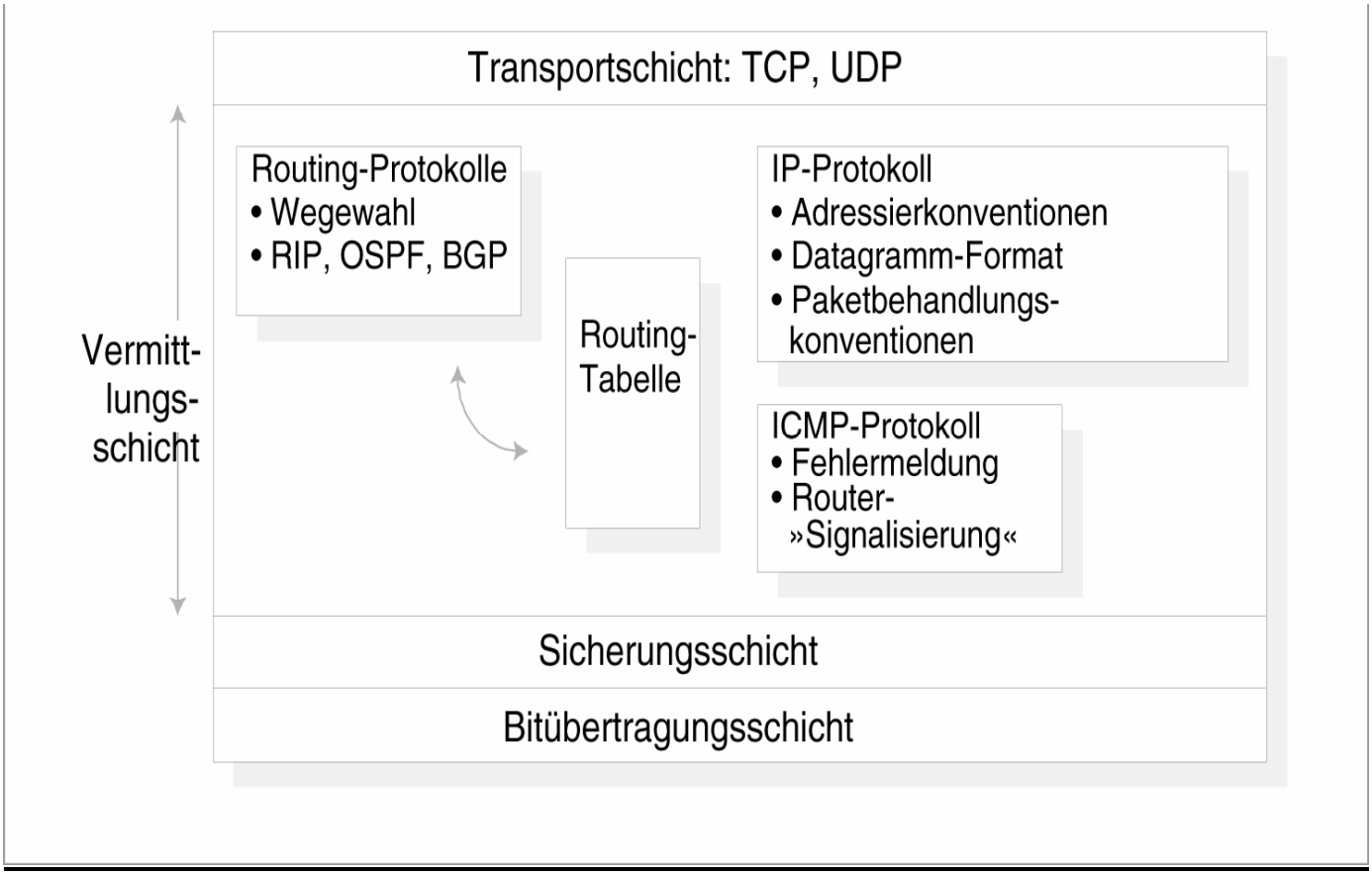
- ***Administrative Autonomie***: Man kann nur eine begrenzte Anzahl von NW-Komp. managen

Hierarchisches Routing (2) Intra-AS- und Inter-AS-Pfade



- **Lösung**: Gruppierung von Routern in Regionen sog. ***Autonome Systeme (AS)***
- **Routing Protokolle**: - Intra-AS-Routing-Prot.: verwendet innerhalb AS
  - Inter-AS-Routing-Prot. verwendet zwischen ASs
- **Gateway-Router:** Router, die verschiedene AS verbinden

Vermittlungsschicht-Aufgaben



Aufgaben:

1. IP-Protokoll
   - Adressierung
   - Paketsegmentierung
   - Paketweiterleitung

2. ICMP-Protokoll
   - Management der Verbindungen
   - Router Signalisierung

3. Routing Protokolle wegen Übertr. der Routing Inform
   - RIP (Distanz Vektor), BGP, OSPF

4. Verwaltung der Routing Tabelle

Routing im Internet

- Routing Protokolle → ***Ermittlung des Pfades*** zwischen Quelle und Ziel
- Autonome System (AS) → Vernetzung von mehreren Netzwerken
- Internet-Konfiguration → Vernetzung von mehreren autonomen Systemen (AS)
- Routing innerhalb von AS → erfolgt per ***Intra-AS-Routing Protokolle***
- Routing zw. mehrerer AS → erfolgt per sog***. Inter-AS-Routing Protokolle***
- ***Intra-AS-Routing:***

  - Rolle: Routing Tabellen innerhalb eines AS zu konfigurieren und zu pflegen

  - Bezeichnung: Interior Gateway Protokolle

  - Wichtige Typen: RIP-Routing information Protokoll
    OSPF – Open Shortest Path First
    EIGRP-Enhanced Interior Gateway RP von CISCO

Routing-Informations-Protokoll (1)

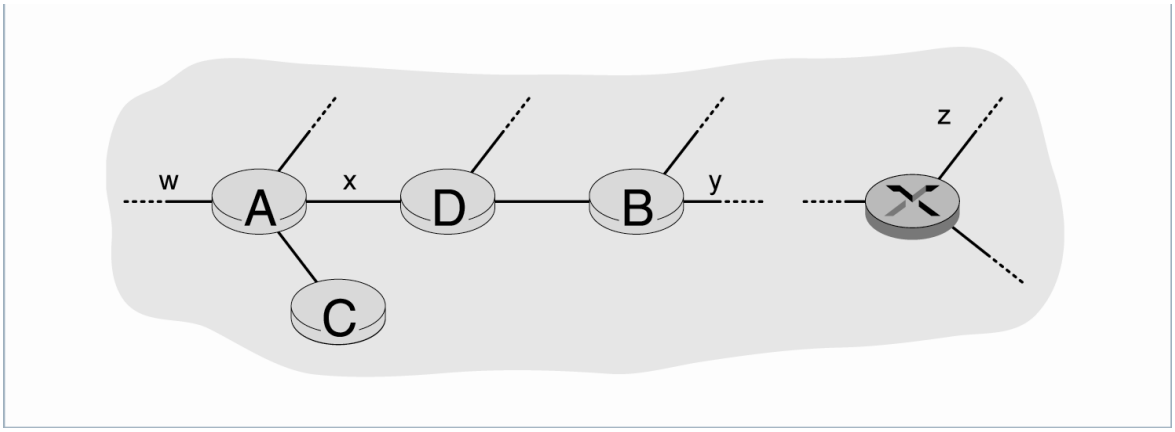
- Typen: - RIP Vers. 1 (RFC 1058)
  - RIP Vers. 2 (RFC 1723)

- RIP basiert auf ***Distanz-Vektor-Algorithmus***

- Annahmen: - Kosten einer Verbindungsleitung = 1
  - Max. Kosten eines Pfades = 15
    d.h. RIP wird für AS verwendet, die weniger als 15 Hops umfassen.

- **Operation:**
  - RIP unterstützt den Austausch der Routing Tabbelle (RT)-Einträge zwischen benachbarten Routern.
  - Der Austausch findet alle 30 sek. statt
  - RIP-Meldungen → bezeichnet als RIP-Advertisement

Beispiel:



Annahme:

- Router A,B,C,D sind wie im Bild mit den Netzen: X,Y,W,Z verbunden

- Router enthalten Routing-Tabellen bestehend aus nur folgenden Informationen (in Wirklichkeit sind es mehr Informationen)
  Zielnetz, nächster Router, Anzahl der Hops zum Ziel

Routing-Informations-Protokoll (2)

Zielnetzwerk	Nächster Router	Anzahl Hops zum Ziel
w	A	2
y	B	2
z	B	7
x	—	1
...	...	...

Operation des Routers D

- Falls eine Meldung an das NW-Ziel "W" gesendet werden muss,
  dann - muss die Meldung an Router A gesendet werden
  - die Meldung wird über 2 Hops bis zum Ziel-NW übertragen.
    Dies ist der kürzeste Weg.

- Die Tabelle enthält ähnliche Informationen für alle Netze, die der Router A kennt.

Annahme:

- Router A sendet an Router D eine RIP-Meldung, die die RT von Router A enthält.

- Innerhalb dieser Meldung → ***Netz „Z" kann via Router A über 4 Hops erreicht werden.***

Routing-Informations-Protokoll (3)

Zielnetzwerk	Nächster Router	Anzahl Hops zum Ziel
w	A	2
y	B	2
z	A	5
...	...	...

Ergebnis:

- Router D ändert seinen Eintrag bezügl. Erreichbarkeit von Netzwerk „Z“
- Jetzt ist „Z“ via A erreichbar, da dieser Weg kürzer als der alte Weg ist.

RIP-Eigenschaften

- Falls ein Router länger als 180 sec. von seinem Nachbar keine RIP-Meldung erhält,
  dann wird diese Verbindung als ***gestört*** betrachtet.
- Der Router ändert dann entsprechend die eigene Routing Tabelle und sendet sie an alle anderen erreichbaren Nachbarn.
- Router können per RIP-Afrage die Kosten von Nachbarn zu einem bestimmten Ziel anfordern.
- RIP-Meldungen: siehe Wireshark Listing (Anhang)

Routing-Informations-Protokoll (4)

- ***RIP Vers 2*** → - ergänzt RIP V1
  - enthält auch die Subnetmask für jedes Subnet innerhalb der RIP-Meldung
  - erlaubt Authentifizierung
  - Routing Domain Field und NextHop erlaubt die Verwendung von „Multiple AS“
  - Route Tag wird verwendet, um „External Routes“ zu identifizieren. Es ist in Verbindung mit EGP und BGP-Protokollen zu verwenden.
- ***RIP V2 Meldung***: siehe Wireshark Listing (Anhang)

RIP1

```
Frame 2 (106 bytes on wire, 106 bytes captured)
Ethernet II, Src: Cisco_76:54:72 (00:00:0c:76:54:72), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 194.95.109.145 (194.95.109.145), Dst:
255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
Routing Information Protocol
    Command: Response (2)
    Version: RIPv1 (1)
    IP Address: 192.168.10.0, Metric: 1
        Address Family: IP (2)
        IP Address: 192.168.10.0 (192.168.10.0)
        Metric: 1
    IP Address: 192.168.30.0, Metric: 1
        Address Family: IP (2)
        IP Address: 192.168.30.0 (192.168.30.0)
        Metric: 1
    IP Address: 192.168.20.0, Metric: 1
        Address Family: IP (2)
        IP Address: 192.168.20.0 (192.168.20.0)
        Metric: 1


Frame 3 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Cisco_83:49:20 (00:11:92:83:49:20), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 194.95.109.130 (194.95.109.130), Dst:
255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
Routing Information Protocol
    Command: Response (2)
    Version: RIPv1 (1)
    IP Address: 194.95.109.58, Metric: 1
        Address Family: IP (2)
        IP Address: 194.95.109.58 (194.95.109.58)
        Metric: 1
```

RIP2

```
Frame 4 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: Cisco_83:49:20 (00:11:92:83:49:20), Dst: 01:00:5e:00:00:09
(01:00:5e:00:00:09)
Internet Protocol, Src: 194.95.109.130 (194.95.109.130), Dst: 224.0.0.9
(224.0.0.9)
User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
    Routing Domain: 0
    IP Address: 194.95.109.48, Metric: 1
        Address Family: IP (2)
        Route Tag: 0
        IP Address: 194.95.109.48 (194.95.109.48)
        Netmask: 255.255.255.240 (255.255.255.240)
        Next Hop: 0.0.0.0 (0.0.0.0)
        Metric: 1
    IP Address: 194.95.109.58, Metric: 1
        Address Family: IP (2)
        Route Tag: 0
        IP Address: 194.95.109.58 (194.95.109.58)
        Netmask: 255.255.255.255 (255.255.255.255)
        Next Hop: 0.0.0.0 (0.0.0.0)
        Metric: 1
    IP Address: 194.95.109.64, Metric: 1
        Address Family: IP (2)
        Route Tag: 0
        IP Address: 194.95.109.64 (194.95.109.64)
        Netmask: 255.255.255.240 (255.255.255.240)
        Next Hop: 0.0.0.0 (0.0.0.0)
        Metric: 1
    IP Address: 194.95.109.80, Metric: 1
        Address Family: IP (2)
        Route Tag: 0
        IP Address: 194.95.109.80 (194.95.109.80)
        Netmask: 255.255.255.240 (255.255.255.240)
        Next Hop: 0.0.0.0 (0.0.0.0)
        Metric: 1
    IP Address: 194.95.109.96, Metric: 1
        Address Family: IP (2)
        Route Tag: 0
        IP Address: 194.95.109.96 (194.95.109.96)
        Netmask: 255.255.255.240 (255.255.255.240)
        Next Hop: 0.0.0.0 (0.0.0.0)
        Metric: 1
```

Routing-Tabellen (1): Beispiel

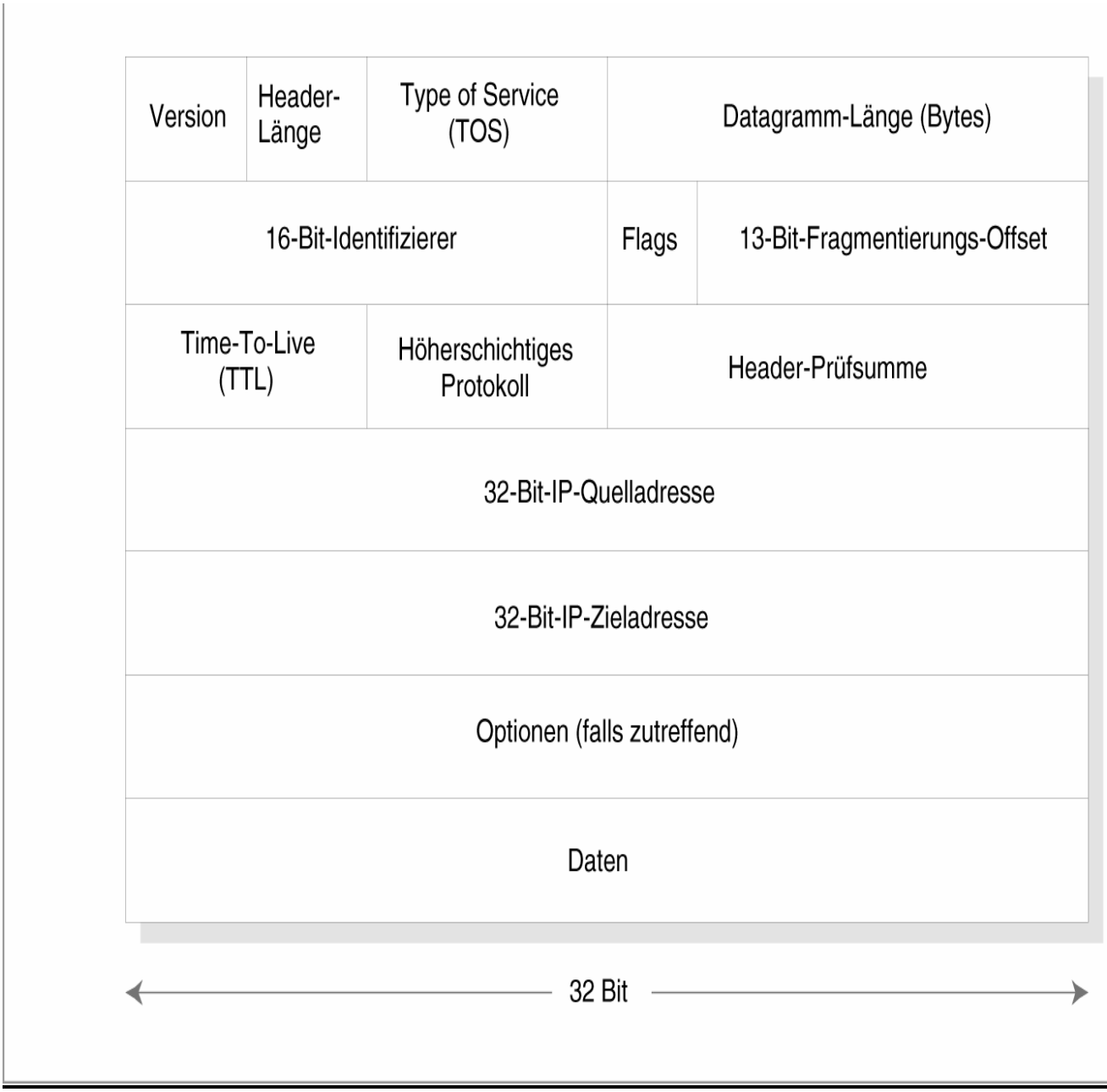
```
rfhci8003#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 194.95.109.129 to network 0.0.0.0

R    192.168.30.0/24 [120/1] via 194.95.109.145, 00:00:12, FastEthernet0/0
     194.95.109.0/24 is variably subnetted, 6 subnets, 3 masks
C       194.95.109.128/26 is directly connected, FastEthernet0/0
C       194.95.109.96/28 is directly connected, FastEthernet0/1
S       194.95.109.80/28 [1/0] via 194.95.109.61
S       194.95.109.64/28 [1/0] via 194.95.109.62
C       194.95.109.48/28 is directly connected, FastEthernet0/1
S       194.95.109.58/32 [1/0] via 194.95.109.57
R    192.168.10.0/24 [120/1] via 194.95.109.145, 00:00:12, FastEthernet0/0
S    192.168.40.0/24 [1/0] via 194.95.109.145
                     [1/0] via 194.95.109.180
R    192.168.20.0/24 [120/1] via 194.95.109.145, 00:00:12, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 194.95.109.129
```

- Routing Tabellen sind unterschiedlich dargestellt, abhängig vom BS oder NW-Komponenten
- Workstations, wie UNIX, LINUX, WINDOWS unterstützen und verwalten auch RTabellen.
- Eine RT einer Work Station lässt sich per Befehl

  „netstatt - Adresse des Hosts“

  erfahren und darstellen.
- In Wirklichkeit enthält eine RT mehr Informationen als in der Darstellung gezeigt wird.

IPV4 Nachrichten Format



Felder:

Version: IPV4 oder IPV6. Dient zur Interpretierung der restlichen Felder

Header-Länge: notwendig, um festzutellen, wo die eigentlichen Nutzdaten anfangen. Header-Länge ohne Optionen = 20 Bytes

TOS (Type Of Service): - Unterscheiden zwischen verschiedenen Datagrammen (z. B. Echtzeit-Datagrammen)
- Neuerdings werden TOS-Bits als Definition unterschiedl. Dienststufen: Differentiated Services

Datagramm-Länge: Gesamtlänge des IPDatagramms gemessen in Bytes

ID, Flags, Offset: Dienen zur IP-Fragmentierung und –Reassemblierungs-Prozedur

TTL (Time To Live): Sicherstellen, dass die Datagramme nicht ewig im Netz kreisen. Wenn TTL = 0, dann wird die Meldung weggeworfen und eine ICMP-Meldung an Sender geschickt.

Protokoll: Bezeichnet den Protokoll-Typ, der innerhalb des Datagramms eingepackt ist, z. B. ***TCP → 6; UDP → 17, ICMP → 1, EGP → 8***

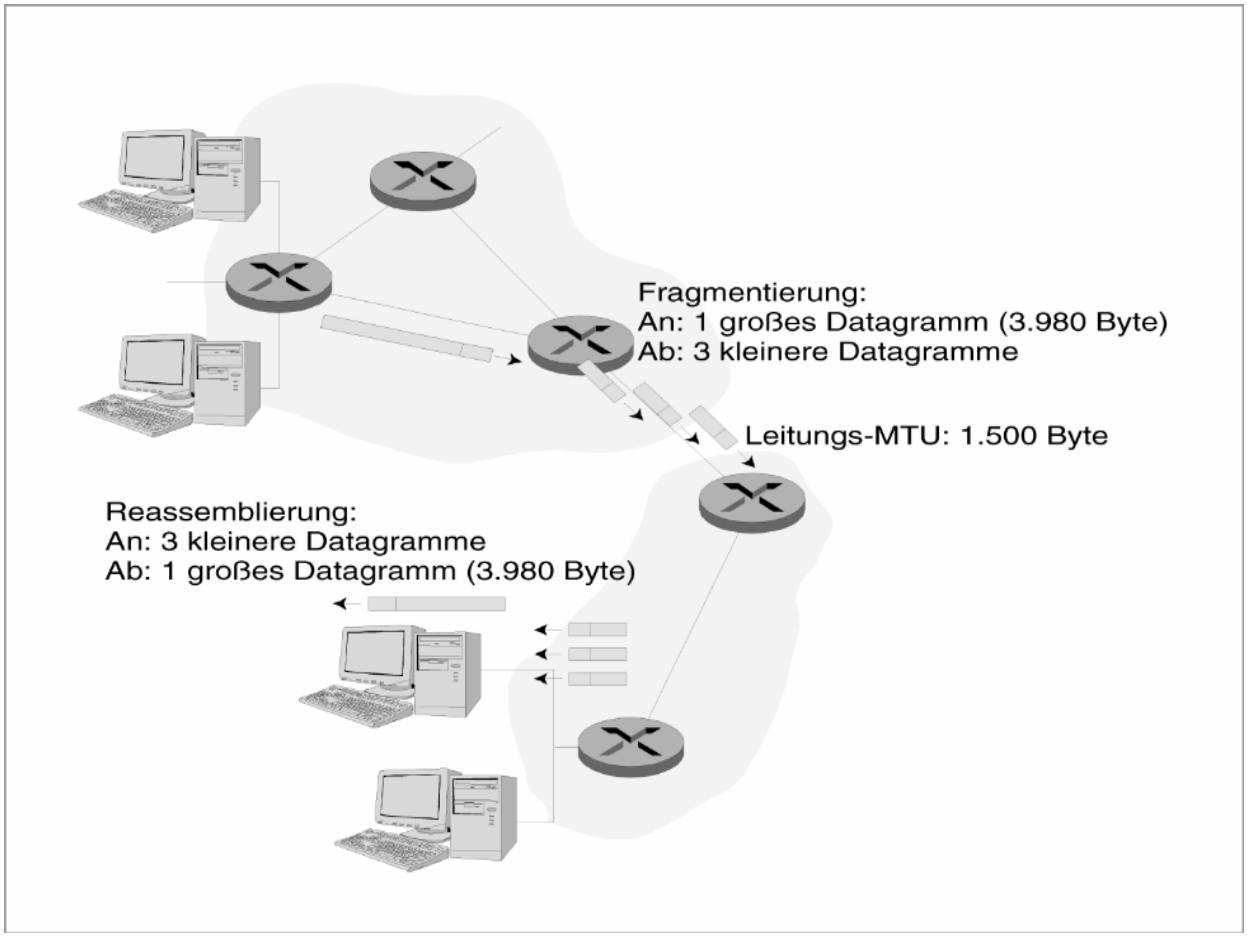
Header-Prüfsumme: Feststellung von Bitfehlern bei der Übertragung. Es wird als 1er Kompl. aller Felder berechnet. Alle Router berechnen erneut diese Prüfsumme, da der Router Felder verändert, bevor er die empfangene Mld. weiterleitet

IP-Adr-Quelle/Ziel: 32 Bit Adr. der Quelle bzw. des Ziels

Optionen: erlaubt die Erweiterung eines IP-Headers. Selten verwendet!

Nutzdaten: In der Regel werden Daten von übergeord. TCP- oder UDP-Protokollen eingepackt. Da aber IP ein routbares Protokoll ist, kann er auch andere Protokolle einpacken und weiter durch das Internet transportieren.

IP-Fragmentierung und – Reassemblierung

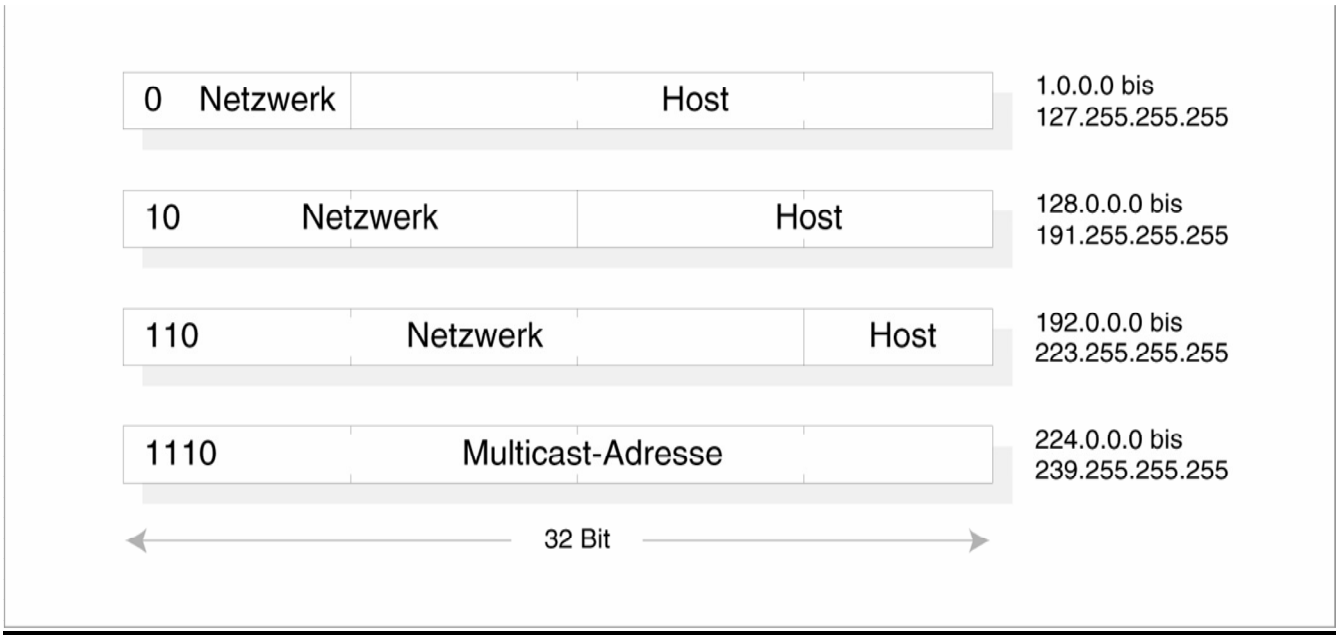


- Fragmentierung & Reassemblierung → Last für Router
  Deswegen soll Fragmentierung → Reduziert auf ein Minimum

- TCP- und UDP-Segmente → sind klein gehalten, um Fragmentierung zu vermeiden.

- Die Mehrheit der WANs unterstützt max. 576 Bytes/Paket
  Folge → Die Mehrheit der Implementierungen hat ***TCP-Segment = 512 - 536 Bytes***, so dass die max. Länge von 576 Bytes (einschl. Header) nicht überschritten wird.

IP-Adressen-Bereich



1. ***Klassen-Adressen (Classful Addressing)***
   A → 7 Bit = Netzwerk; 24 Bit = Host
   B → 14 Bit = Netzwerk; 16 Bit = Host – Ausverkauft
   C → 22 Bit = Netzwerk; 8 Bit = Host
   D → Multicast-Adressen

2. ***Zuweisung von Adressen***:
   _- Manuelle Konfigurierung im Host
   - Dynamische Konfigurierung: Per DHCP-Protokoll
   - Der DHCP ***(Dynamic Host Configuration Protocol***) Server erhält Anfragen von Clients
   - Der Server erteilt dynamisch die IP-Adressen, die vorher für die entsprechenden Hosts innerhalb einer Datei abgelegt waren
   - Die Adress-Bereiche einer Organisation wird in der Regel von ISP zugewiesen.
     Im Falle von deutschen Universitäten werden sie von DFN zugeteilt.

Subnetting. Konfigurations- Beispiel (siehe Anhang)

IP-Adress => 11110011..... 1110001111010

NET-ID	SUBNET-ID	HOST-ID

SUB-Maske

1111111.....11111111111111	11111111...1111	000000000

d.h.: 255.255 .255. 0

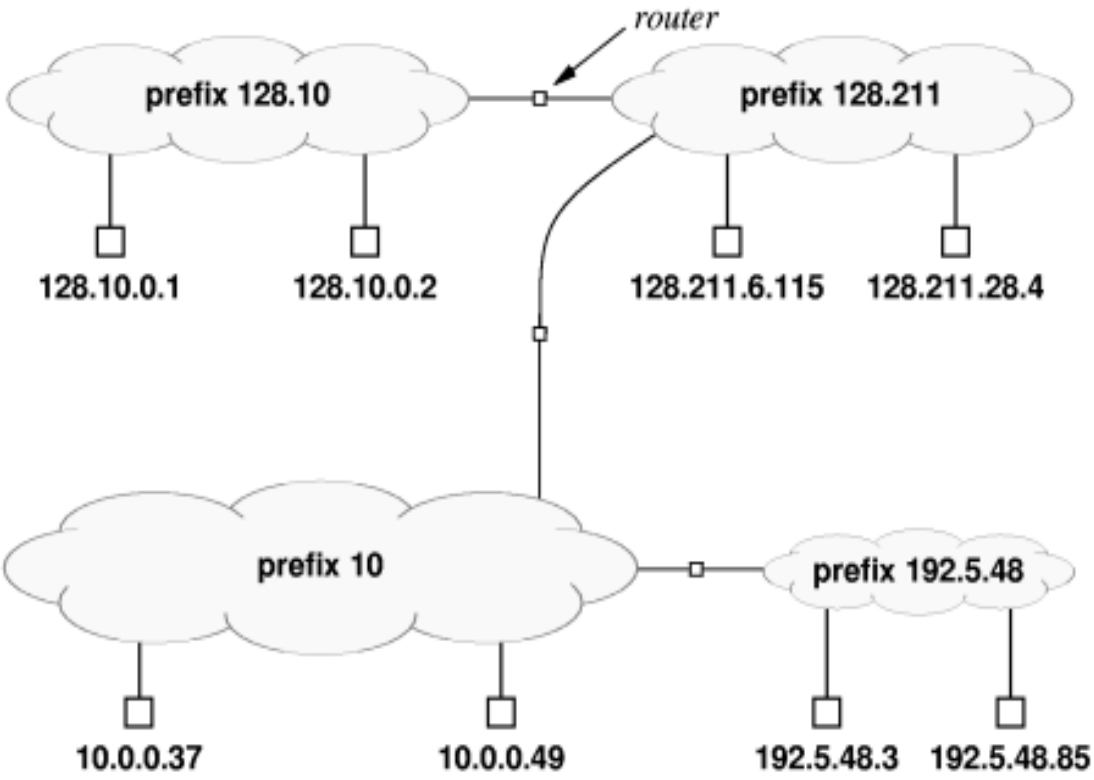
Subnet-ID: es wird festgelegt mittles variablen # Bits von „Host-ID"- Feld

Subnet-Mask: es wird verwendet um die Subnet-Id zu kodieren

Beispiel :

IP- Addesse der Workstation:	**158.**	**152.**	**30.**	**248**
Subnetzmaske:	**255.**	**255.**	**255.**	**0**
d.h. Station befindet sich im Subnetz:	***158.***	***152.***	***30.***	***0***

IP- Klassen Adressierung: Beispiel



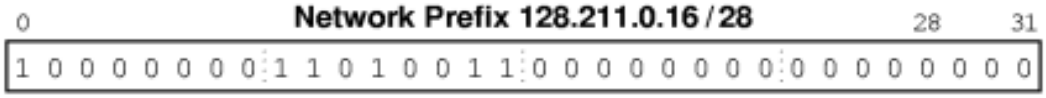
Beispiel: Die Grösse der Wolken wird von der Adress-Klasse bestimmt

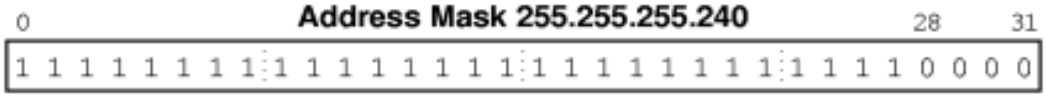
Classless Interdomain Routing (***CIDR***) (RFC 1519)

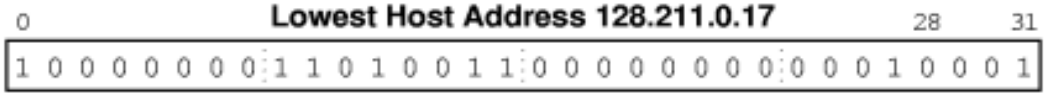
CIDR Notation spezifiziert die Grösse der Maske in Verbindung mit einer Addresse
Netzwerkteil einer IP-Adresse kann beliebig lang sein
Notation: ***a.b.c.d/x***; x => Anzahl führende Bits, die Netzwerkteil darstellen

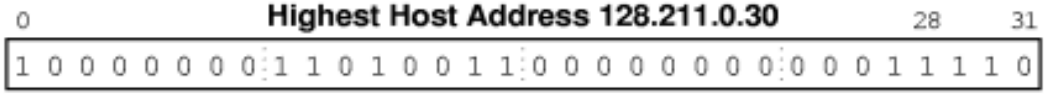
CIDR gegenüber Klassen Notation :

- Klassen-Notation besteht aus 16 Bit Präfix (Netz-Adresse) und 16 Bit Sufix (Host-Adresse) Bp: 128.10.0.0
- CIDR Notation : Host-Sufix kann an einer beleibigen Grenze beginnen
  Vorteil: Die Netzwerk-Präfix sind von null nummeriert und können an beleibige Grenzen gesetzt warden. (siehe Beispiel unten)









Die Bits 0- 27 => Netzwerk Adresse
Die Bits 28 – 31 => Host-Adressen
d.h " 128.211.0.16/28" spezifiziert (16 - 2) Hosts innerhalb des Netzes mit der Adresse : 128.211.0.16

Internet Control Message Protokoll (ICMP) (RFC792)

ICMP-Meldungs-Typen

ICMP-Nachrichtentyp	Code	Beschreibung
0	0	Echo reply (on Ping)
3	0	Destination network unreachable
3	1	Destination host unreachable
3	2	Destination protocol unreachable
3	3	Destination port unreachable
3	6	Destination network unknown
3	7	Destination host unknown
4	0	Source quench (Überlastkontrolle)
8	0	Echo request
9	0	Router advertisement
10	0	R outer discovery
11	0	T TL expired
12	0	I P header bad

ICMP → verwendet zwecks ***Austausch von Control Information*** zwischen Netzwerk-Komponenten

ICMP → - wird als Teil der Netzwerkschicht betrachtet
- Es läuft jedoch via IP-Protokoll, ähnlich wie TCP oder UDP-Meldungen

ICMP-Format – Felder:
- Typ,
- Code,
- IP-Adr. des Datagramms, das die ICMP-Meld. verursacht hat