

Datenkommunikation

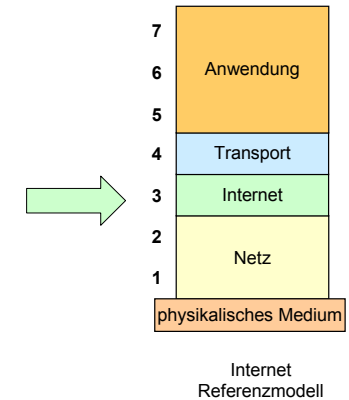
Teil 3.2: Internetschicht

O.Univ.Prof.Dr. Harmen R. van As

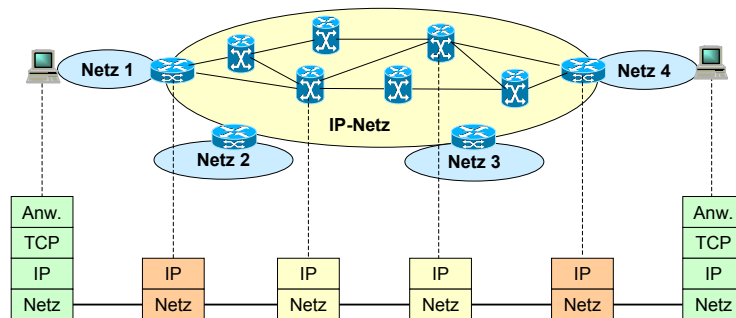
Übersicht

3.2a Internet-Referenzmodell: Internetschicht

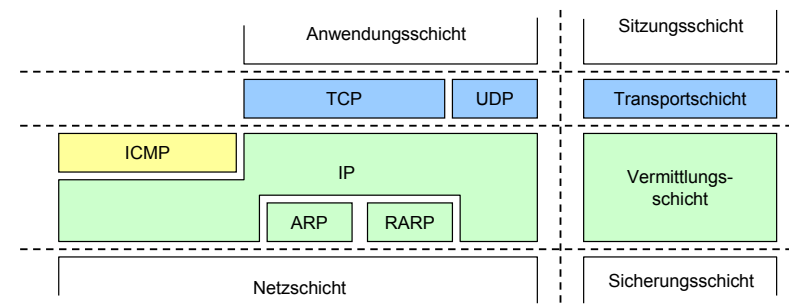
- Netzstruktur, Routeraufbau
- IP (Internet Protocol)
- IPv4/v6 Formate
- Eigenschaften der Protokolle
- Fragmentierung
- ICMP (Internet Control Message Protocol)



IP-Vernetzung

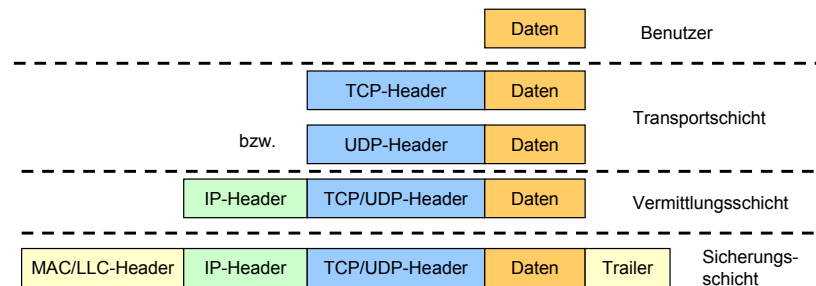


Die TCP/IP-Protokollfamilie

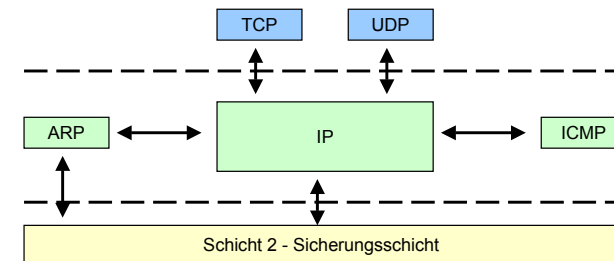


- Die Bezeichnung TCP/IP wird häufig als Synonym für die gesamte Protokollfamilie verwendet
- Obwohl ICMP den IP-Dienst nutzt, wird es dennoch der Vermittlungsschicht zugeordnet

PDU Verschachtelung



Zusammenspiel der Protokollinstanzen



Senden

- TCP- bzw. UDP-Instanz übergibt Daten mit IP-Adresse des Empfängers zur Übertragung an IP-Instanz
- IP-Instanz beauftragt ARP-Instanz mit Ermittlung der entsprechenden Schicht-2-Adresse
- IP-Instanz übergibt PDUs mit ermittelter Schicht-2-Adresse an Instanz der Sicherungsschicht

Empfangen

- IP-Instanz reicht empfangene Daten an TCP- bzw. UDP-Instanzen weiter

Kontrolle

- Probleme während der Übermittlung können den Partnerinstanzen über ICMP mitgeteilt werden (wobei ICMP zur Übertragung der Meldungen IP benutzt)

TCP/IP-Protokollfamilie: Eigenschaften

TCP (Transmission Control Protocol)

- Stellt verbindungsorientierten, zuverlässigen und bytestromorientierten Transportdienst bereit

UDP (User Datagram Protocol)

- Stellt verbindungslosen, unzuverlässigen und nachrichtenorientierten Transportdienst bereit

IP (Internet Protocol)

- Sorgt für Wegewahl und unzuverlässige Übertragung einzelner Dateneinheiten

ICMP (Internet Control Message Protocol)

- Unterstützt Austausch von Kontrollinformationen innerhalb der Vermittlungsschicht

ARP (Address Resolution Protocol)

- Zuordnung von IP-Adressen zu den entsprechenden Adressen der Sicherungsschicht

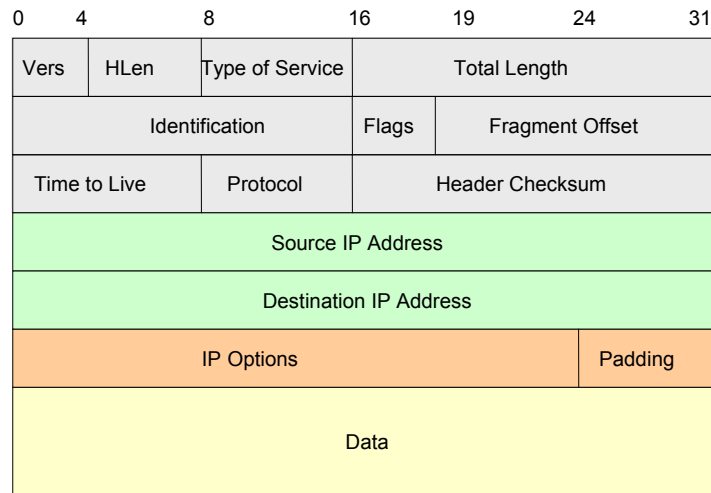
RARP (Reverse Address Resolution Protocol)

- Stellt die Umkehrfunktion von ARP zur Verfügung

IP Features

- Connectionless service
- Addressing
- Data forwarding
- Fragmentation and reassembly
- Supports variable size datagrams
- **Best-effort delivery:** Delay, out-of-order, corruption, and loss possible. Higher layers should handle these
- Provides only "Send" and "Delivery" services
- Error and control messages generated by Internet Control Message Protocol (ICMP)
- RFC 791

IPv4 Datagram Format

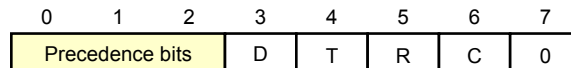


IP Datagram Header (1)

- **Version (4 bit)**
- **Internet Header Length (HLEN) (4 bit):** units of 32-bit words. Min header is 5 words or 20 byte
- **Type of Service (8 bit):** performance requirements (delay bit, throughput bit, reliability bit), priority (precedence bit)
- **Total length (16 bit):** header + data in bytes
Total length must be less than 65 535 Byte. (due to the checksum field)
- **Identification (ID) (16 bit):** Helps uniquely identify the datagram between any source, destination address, fragmentation (no sequence number)

Type of Service (TOS)

Alt:

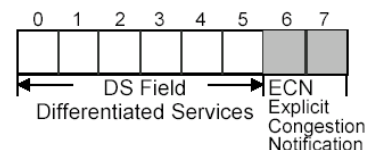


Precedence bits:

000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash override
101	Critic / ECP
110	Internetwork control
111	Network control

Delay bit: 0 ... normal, 1 ... low
 Throughput bit: 0 ... normal, 1 ... high
 Reliability bit: 0 ... normal, 1 ... high
 Cost bit: 0 ... normal, 1 ... low

Neu:



IP Datagram Header (2)

- **Flags (3 bit):**

0	D	M
	F	F

 - DF (do not fragment) flag
0 Fragmentation is allowed by the router
1 Fragmentation is forbidden
 - MF (more fragments) flag
0 last fragment or single fragment
1 more fragments will follow
- **Fragment offset (13 bit):** units of 8 byte (from beginning of datagrams)
- **Time to live (TTL) (8 bit):** Specified in router hops
- **Protocol (8 bit):** Next level protocol to receive the data
 - 1 Internet Control Message Protocol (ICMP)
 - 6 Transmission Control Protocol (TCP)
 - 17 User Datagram Protocol (UDP)

IP Protocols Numbers

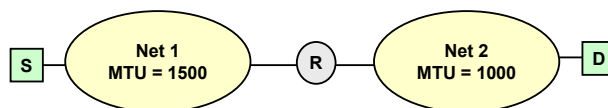
0		Reserved
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Management Protocol
3	GGP	Gateway-to-Gateway Protocol
4	IP	IP encapsulation
5	TCP	Transmission Control Protocol
8	EGP	Exterior Gateway Protocol
9	IGP	Interior Gateway Protocol
17	UDP	User Datagram Protocol
41	IPv6	IP version 6
50	ESP	Encap Security Payload for IPv6
51	AH	Authentication Header for IPv6
89	OSPF	Open Shortest Path

IP Datagram Header (3)

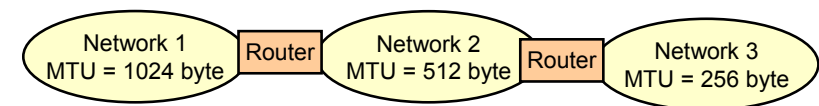
- **Header checksum (16 bit):** 1's complement sum of all 16-bit words in the header. Error in header detected by different checksum using 1's complement arithmetic.
- **Source Address (32 bit):** original source. Does not change along the path.
- **Destination Address (32 bit):** final destination. Does not change along the path.
- **Options (variable):** Security, source route, record route, stream id (used for voice) for reserved resources, timestamp recording
- **Padding (variable):** header length multiple of 4
- **Data (variable):** Data + header (< 65 535 Byte)

Maximum Transmission Unit (MTU)

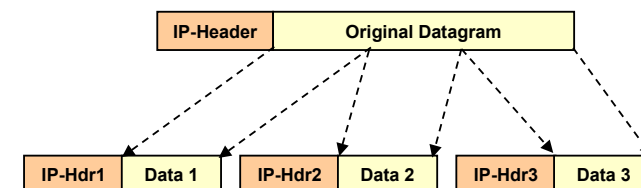
- Each subnet has a maximum frame size
 - Ethernet: 1518 Byte
 - FDDI: 4500 Byte
 - Token Ring: 2 to 4 KByte
- Transmission Unit = IP datagram (data + header)
- Each subnet: maximum IP datagram length ⌊ MTU



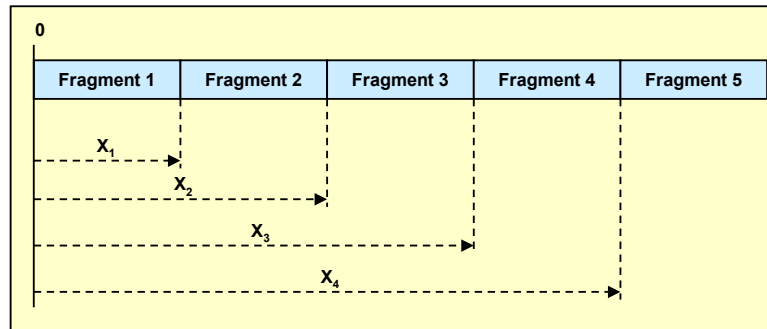
Fragmentation



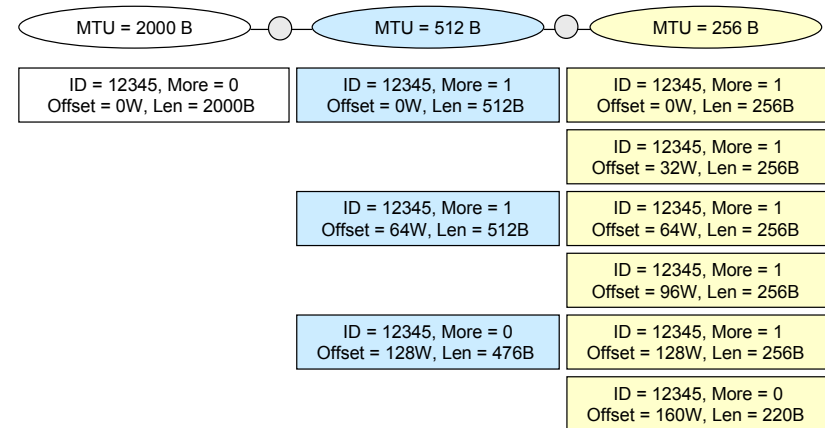
- Datagrams larger than MTU (Maximum Transmission Unit): fragmented
- Original header copied to each fragment and then modified (fragment flag, fragment offset, length)
- Some option fields are copied



IP Fragment Offset

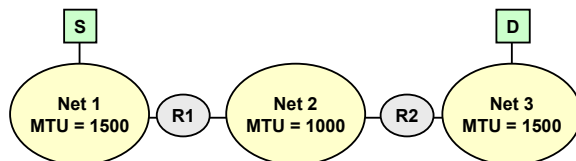


Fragmentation



Reassembly

- Reassemble only at final destination
- Partial datagrams discarded after timeout
- Fragments further fragmented along the path.
Subfragments similar format to fragments.
not possible to tell how many times fragmented
- Minimum MTU along a path = Path MTU



IP Options

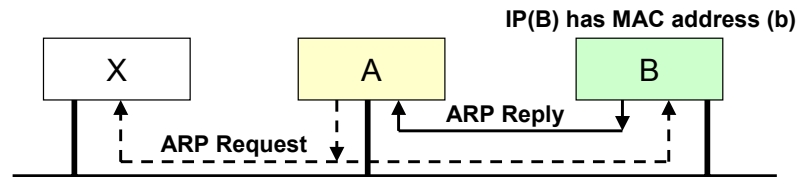
- Record route (List of IP addresses of passed routers)
- Loose source routing
- Strict source routing
- Security
- Timestamp
- Flag Copy:
 - 0 = Copy option only into the first fragment
 - 1 = Copy into all fragments
- Class:
 - 0 = User or control
 - 1 = Reserved
 - 2 = Diagnostics
 - 3 = reserved

Type	Length	Value
1B	1B	nB

Flag Copy	Class	Number
1b	2b	5b

ARP: Address Resolution Protocol

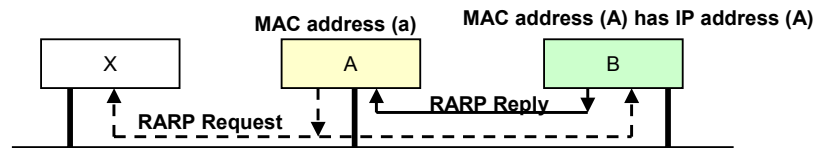
Who knows MAC address of IP (B)?



ARP Request/Reply

Hardware		Protocol
HLEN	PLEN	Operation
Source MAC address (bytes 0-3)		
Source MAC address (bytes 4-5)		Source IP address (bytes 0-1)
Source IP address (bytes 2-3)		Destination MAC address (bytes 0-1)
Destination MAC address (octets 2-5)		
Destination IP address (octets 0-3)		

Reverse Address Resolution Protocol (RARP)



Problem: How can the IP address be resolved? (Initialization)

Solution: manual entry of IP address

IP from configuration file (not possible at diskless station)

IP address global fixed at interface card

Protocol: A sends broadcast information with physical address (a)
RARP server B takes the physical address, maps it to
the IP address of A and sends the IP address (A) back to A

IPv6 Header

IPv6

Version	Priority	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

128 bit

128 bit

IPv4

Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time to Live		Protocol	Header Checksum	
Source Address				32 bit
Destination Address				32 bit
Options			Padding	

Extension Header

Base Header

Base Header Next = TCP	TCP Segment
---------------------------	----------------

Base Header and One Extension Header

Base Header Next = Route	Route Header Next = TCP	TCP Segment
-----------------------------	----------------------------	----------------

Base Header and Two Extension Headers

Base Header Next = Route	Route Header Next = Auth	Auth Header Next = TCP	TCP Segment
-----------------------------	-----------------------------	---------------------------	----------------

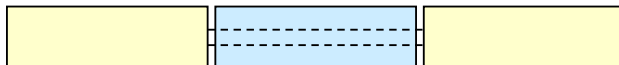
Routing Header

Next Header	Routing Type	Num. Address	Next Address
Reserved	Strict/Loose Bit Mask		
Address 1			
Address 2			
...			
Address n			

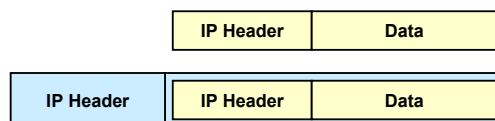
- Strict \Rightarrow Discard if Address [Next-Address] \neq neighbor
- Type = 0 \Rightarrow Current source routing
- Type > 0 \Rightarrow Policy based routing (later)
- New Functionality: Provider selection, Host mobility, Auto-readdressing (route to new address)

Tunneling

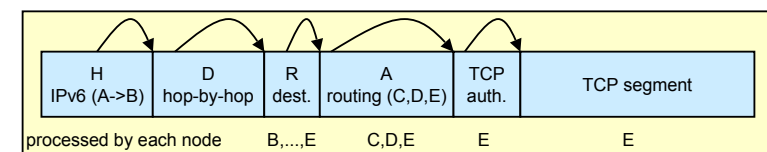
- Tunneling is used to cross islands with different protocols = Encapsulation



- IPv6 routers can encapsulate the original datagram in another IPv6, fragment it, and send it to the final destination.



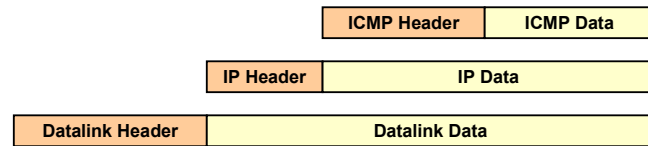
IPv6 Packet Structure



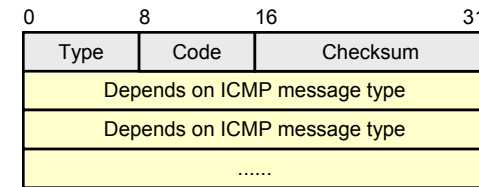
- next header can be IPv4 "tunneling"
- header extension: hop-by-hop options (HHO), routing, fragment, destination options (DO)
- DO, HHO: type-length-value TLV options
- HHO:
 - looked at by each node, immediately after header
 - jumbo payload option (32 bit)
- routing header:
 - fixed header may not contain final address if routing header!
 - mixed loose/strict source route (bitmask)
 - swap destination address and next address from routing header
- fragment header: like IPv4 (32 bit identification, offset, more fragments flag)
- explicit MTU message rather than try-until-fit

Internet Control Message Protocol (ICMP)

- RFC 792
- Used by IP to send error and control messages
- ICMP uses IP to send its messages
- ICMP does not report errors on ICMP messages
- ICMP message are not required on datagram checksum errors
- ICMP reports error only on the first fragment



ICMP Message Format



Type field: type of the ICMP message

Code field: corresponding error specification

Type Field Numbers

0	Echo reply	15	Information request
1	Unassigned	16	Information reply
2	Unassigned	17	Address mask request
3	Destination unreachable	18	Address mask reply
4	Source quench	19	Reserved for security
5	Redirect	20 - 29	Reserved for robustness experiment
6	Alternate host address	30	Traceroute
7	Unassigned	31	Datagram conversion error
8	Echo request	32	Mobile host redirect
9	Router advertisement	33	IPv6 (Where are you)
10	Router selection	34	IPv6 (I am here)
11	Time exceeded	35	Mobile registration request
12	Parameter problem	36	Mobile registration reply
13	Time stamp request	37 - 255	Reserved
14	Time stamp reply		

Application of ICMP Messages

- Echo reply (0) and echo request (8):
test (ping) the accessibility of an IP node (host, router)
- Destination unreachable (3), time exceeded (11) and parameter problem (12):
notification of errors related to
 - accessibility
 - time-to-live
 - reassembly of fragments
 - errors in the IP header
- Source quench (4): **flow control**
- Redirect (5): **path optimization**
- Time stamp request (13), time stamp reply (14), information request (15), information reply (16), address mask request (17) and address mask reply (18):
diagnostics and maintenance

ICMP Messages (1)

- Echo request and reply messages (used for ping)
- Time stamp request and reply messages
- Time exceeded message
- Address mask request and reply messages to discover the subnet mask currently used in a network
- Information request and reply message (e.g. used for discovery of the network ID of an IP address)
- Redirect message
- Router advertisement message
- Source Quench: Slow down
- Time Exceeded: Time to live field in one of your packets became 0 or reassembly timer expired at the destination
- Fragmentation Required: Datagram longer than MTU and "No Fragment bit" was set
- Address Mask Request/Reply: What is the subnet mask on this net?

ICMP Messages (2)

- **Redirect:** Please send to router X instead of me.
 - 0 = Redirect datagrams for the network
 - 1 = Redirect datagrams for the host
 - 2 = Redirect datagrams for the type of service and net
 - 3 = Redirect datagrams for the type of service and host
- Time Stamp Request/Reply:

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence number	
Originate Timestamp			
Receive Timestamp			
Transmit Timestamp			

ICMP Messages (3)

081631

Destination Unreachable Message	Type	Code	Checksum
	Unused		
	Internet Header + 64 bit of original data datagram		

Echo or Echo Reply Message ("Ping")	Type	Code	Checksum
	Identifier		Sequence number
	Data		

Redirect Message	Type	Code	Checksum
	Gateway Internet address		
	Internet Header + 64 bit of original data datagram		

Destination Unreachable

Code	Meaning
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation need and do not fragment bit set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Communication with destination network administratively prohibited
10	Communication with destination host administratively prohibited
11	Network unreachable for type of service
12	Host unreachable for type of service