



••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

Netzwerksicherheit

Grundlagen des Internet Protocol

Stephen Wolthusen



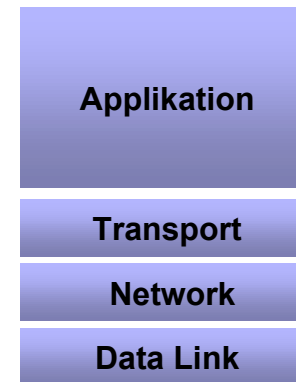


ISO/OSI und TCP/IP: Entsprechungen der Schichten in den Modellen

... department security technology ... department security technology ... department security technology ... department security technology ...



OSI-Referenzmodell



TCP/IP-Protokollstapel





TCP/IP (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Internet Protocol Version 4: 1981 publiziert
- IP (Internet Protocol):
 - Verbindungsloses, Best-Effort-Protokoll
 - Datenströme werden in Pakete variabler Länge unterteilt
 - Routing der Pakete (oder Paket-Fragmente) unabhängig voneinander
 - Grundlage für ICMP, IGMP, TCP, UDP
- ICMP
 - Protokoll zur Informations- und Fehlerübermittlung
 - Basiert direkt auf IP





TCP/IP (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- IGMP (Internet Group Management Protocol)
 - Kontrolliert Zugehörigkeit zu Multicast-Gruppen
- UDP (User Datagram Protocol)
 - Verbindungslos, Best-Effort
- TCP (Transmission Control Protocol)
 - Verbindungsorientiert
 - Stellt gegen Paketverlust-, Prüfsummen-, und Sequenzierungsfehler gesicherten Kanal zur Verfügung
 - Kann als Paar von Byteströmen aufgefaßt werden

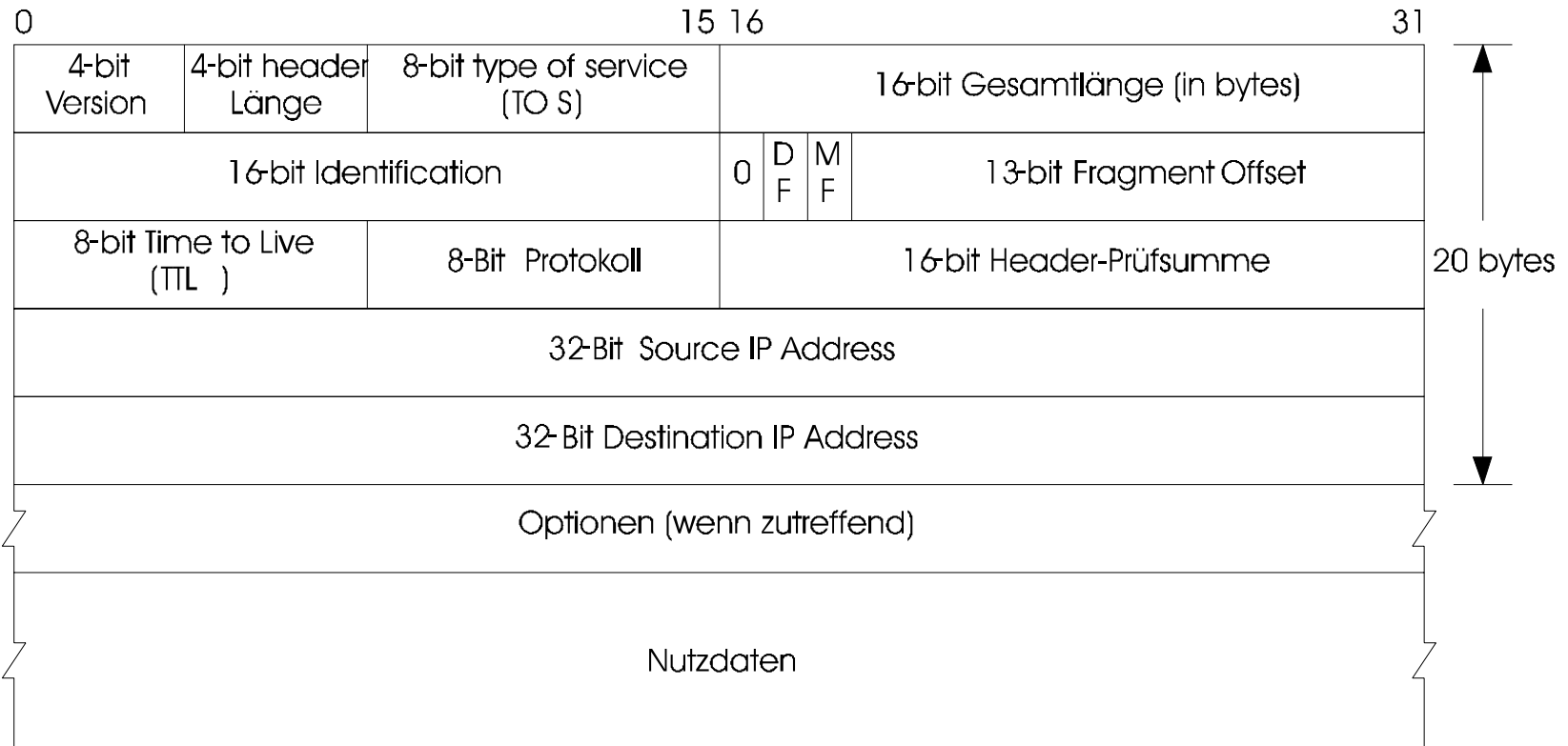




IP-Header (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

IP Header Version 4





IP-Header (2)

... department security technology ... department security technology ... department security technology ... department security technology ...

- Big Endian
 - (Bits 0...31 in dieser Folge, „Network Byte Order“)
- x86, Alpha: Little Endian, umgekehrte Reihenfolge: „NUXI“
- Dichte Packung, Bitfelder
- Vermengung von immer benötigten und selten genutzten Feldern und Optionen - alles muß stets durch den Parser
- Version Number: 4 Bits
 - Derzeit nur 4, 6 im Einsatz
- Header-Länge: 4 Bits
 - Anzahl 32-Bit Worte inklusive Optionen, ohne Optionen: 5





IP-Header (3)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Type of Service: 8 Bits

- 3 Bits Precedence
- 4 Bits TOS
 - ▲ Minimierung von Kosten (Bit 0)
 - ▲ Maximierung der Zuverlässigkeit (Bit 1)
 - ▲ Maximierung des Durchsatzes (Bit 2)
 - ▲ Minimierung der Verzögerung (Bit 3)
- 1 Bit reserviert (muß immer 0 sein)

■ Router und Hosts ignorieren diese Felder meist.





IP-Header (4)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Gesamtlänge: 16 Bits
 - Länge des Datagramms in Bytes
- Identification: 16 Bits
 - Identifiziert jedes Datagramm für Fragmentierung
- Flags: 3 Bits
 - 1 Bit reserviert (stets 0)
 - 1 Bit DF („Don´t Fragment“)
 - 1 Bit MF („More Fragments“)





IP-Header (5)

... department security technology ... department security technology ... department security technology ... department security technology ...

- **Fragment Offset: 13 Bits**
 - Versatz des aktuellen Fragments

- **Time to Live: 8 Bits**
 - Eigentlich: Lebenszeit in Sekunden
 - Wird bei jedem Hop um 1 verringert, bei 0 wird Paket verworfen

- **Protocol: 8 Bits**
 - Verwendetes Protokoll (TCP, UDP, IGMP, ICMP...)

- **Header-Prüfsumme: 16 Bits**
 - 1-Komplement der 1-Komplemente der Header





IP-Header (6)

... department security technology ... department security technology ... department security technology ... department security technology ...

- Source IP Address: 32 Bits
- Destination IP Address: 32 Bits
- Optionen (immer auf 32 Bit ausgerichtet)
 - Sicherheits-Optionen
 - Routen-Katalogisierung
 - Zeitstempel
 - Loose Source Routing
 - Strict Source Routing





IP-Adressen in IPv4

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

32 Bit, geteilt in:

NetID

SubnetID

HostID

Besondere Adressen:

Net ID	Subnet ID	Host ID	Quelle	Ziel
0	0	0	Ja	Nein
0	0	Host ID	Ja	Nein
127	0	*	Ja	Ja
-1	0	-1	Nein	Ja
Net ID	0	-1	Nein	Ja
Net ID	Subnet ID	-1	Nein	Ja
Net ID	-1	-1	Nein	Ja





Fragmentierung (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Übertragungskanäle weisen MTU auf
 - Ethernet: 1492..1522 Bytes
 - minimal 576 Bytes

- Pakete größer 576 Bytes nur nach „Path MTU Discovery“
 - Versand von Paketen mit DF gesetzt mit jeweils erhöhter TTL
 - Wenn „Host Unreachable“, so ist für den Hop die MTU gefunden
 - Konforme Hosts geben in „Host Unreachable“ die eigene MTU an
 - PMTU kann sich mit jedem (!) Paket ändern





Fragmentierung (2)

... department security technology ... department security technology ... department security technology ... department security technology ...

■ Fragmentierte Datagramme

- weisen bis auf letztes Fragment ein MF-Flag auf.
- Enthalten im Fragment Offset den Versatz vom Anfang des Datagramm-Datenfeld
- Werden anhand Identification, Source, Destination, Protocol-Felder zusammengeführt
- MF-Flag ist bei allen Fragmenten gesetzt, Fragment mit gleicher Identification und MF=0 beendet Fragmentierung
- Einige Optionen (z.B. „Record Route“) sind nur im ersten Fragment vorhanden





IP-Optionen (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Sicherheits-Optionen

- RFC 1108, überholt - „Labeling“ von Datagrammen

■ Routenkatalogisierung

- Jeder Router trägt eigene Adresse ein, max. 9 Adressen

■ Zeitstempel

- ms seit Mitternacht UTC, optional mit IP-Adressen

■ Source Routing

- Loose: Router, die passiert werden sollen werden angegeben
- Strict: Nur angegebene Router dürfen passiert werden





IP-Optionen (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Vorgang Source Routing

- Felder werden bei jedem durchlaufenen Router modifiziert
- Als Zieladresse wird erstes Element der Options-Liste eingetragen, neue Source ist eigene Adresse
- Alte Werte werden „nach vorn“ verschoben
- Ursprüngliche Zieladresse wird in frei gewordenem Feld eingetragen, PTR um 4 verschoben
- Vorgang wird wiederholt, bis PTR über das Ende des Optionsfeldes zeigt
- Empfänger hat somit invertierte Route vorliegen





Host Routing

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Entscheidung für Host (!Router)

- Adresse befindet sich auf direkt erreichbarem Interface
 - ▲ Versendet Paket direkt
- Adresse nicht direkt erreichbar
 - ▲ Versand an Default Router (muß direkt erreichbar sein)





Adressierungsarten

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Unicast

- Eindeutige Quell- und Zieladresse

■ Broadcast

- Allgemein, gerichtet an Netze, Subnetze

■ Multicast

- Multicast-Gruppen (Adreßbereich Class D: 224.0.0.0 - 239.255.255.255) mit wahlweiser Zugehörigkeit
- Zugehörigkeit wird über IGMP bestimmt
- Verteilung der Multicasts (Spanning Tree, Flooding) mit eigenen Routing-Algorithmen (PIM, MOSPF...)





ICMP - Internet Control Message Protocol

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Setzt direkt auf IP auf
- Besteht aus
 - IP-Header (20 Bytes)
 - ICMP-Header
 - ▲ Typ (1 Byte)
 - ▲ Code (1 Byte)
 - ▲ Prüfsumme (2 Bytes)
 - ICMP-Nutzlast
 - ▲ Optional, bis zur maximalen Paketgröße (65511 Bytes)





ICMP (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- ICMP-Nachrichten dürfen nie erzeugt werden
 - Als Reaktion auf eine andere ICMP-Nachricht
 - Als Reaktion auf Pakete, deren Zieladressen IP Broadcast oder IP Multicast Adressen sind
 - Als Reaktion auf Paket, das mittels Link Layer Multicast/Broadcast versandt wurde
 - Wenn die Ursache ein Paket war, dessen Ziel kein eindeutiger Host war
 - ▲ NULL-, Loopback-, Broadcast-, Multicast-Adresse





ICMP (3)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Typ 0: Echo-Antwort (immer Code 0)
- Typ 3: Nicht erreichbar
 - 0: Netz nicht erreichbar
 - 1: Host nicht erreichbar
 - 2: Protokoll nicht erreichbar
 - 3: Port nicht erreichbar
 - 4: Fragmentierung notwendig, aber nicht erlaubt
 - 5: Source Route fehlgeschlagen
 - 6: Ziel-Netz unbekannt





ICMP (4)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Typ 3: Nicht erreichbar

- 7: Ziel-Host unbekannt
- 8: Quell-Host isoliert
- 9: Ziel-Netz administrativ nicht erreichbar
- 10: Ziel-Host administrativ nicht erreichbar
- 11: Netz für Diensttyp nicht erreichbar
- 12: Host für Diensttyp nicht erreichbar
- 13: Kommunikation durch Filter administrativ verboten
- 14: Host-Vorrang verletzt
- 15: Vorrang aktiv





ICMP (5)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Typ 4: Source Quench (immer Code 0)
- Typ 5: Redirect
 - 0: Redirect für Netz
 - 1: Redirect für Host
 - 2: Redirect für Diensttyp und Netz
 - 3: Redirect für Diensttyp und Host
- Typ 6: Andere Host-Adresse (immer Code 0)
- Typ 8: Echo-Anforderung (immer Code 0)
- Typ 9: Router-Bekanntgabe (immer Code 0)





ICMP (6)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Typ 10: Router-Anforderung (immer Code 0)
- Typ 11: Zeitüberschreitung
 - 0: TTL=0 bei Durchgang
 - 1: TTL=0 bei Fragment-Zusammensetzung
- Typ 12: Parameter-Fehler
 - 0: IP-Header fehlerhaft
 - 1: Notwendige Option nicht gesetzt
- Typ 13: Zeitstempel-Anforderung (immer Code 0)
- Typ 14: Zeitstempel-Antwort (immer Code 0)





ICMP (7)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Typ 15: Informations-Anforderung (immer Code 0)
- Typ 16: Informations-Antwort (immer Code 0)
- Typ 17: Adreßmasken-Anforderung (immer Code 0)
- Typ 18: Adreßmasken -Antwort (immer Code 0)
- Typ 30: Traceroute (immer Code 0)
- Typ 31: Datagramm-Konvertierungsfehler (immer Code 0)
- Typ 32: Umleitung mobiler Host (immer Code 0)
- Typ 33: IPv6 Where-are-you (immer Code 0)
- Typ 34: IPv6 I-am-here (immer Code 0)





ICMP (8)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Typ 35: Mobile Host Registrierungs-Anfrage
(immer Code 0)
- Typ 36: Mobile Host Registrierungs-Antwort
(immer Code 0)

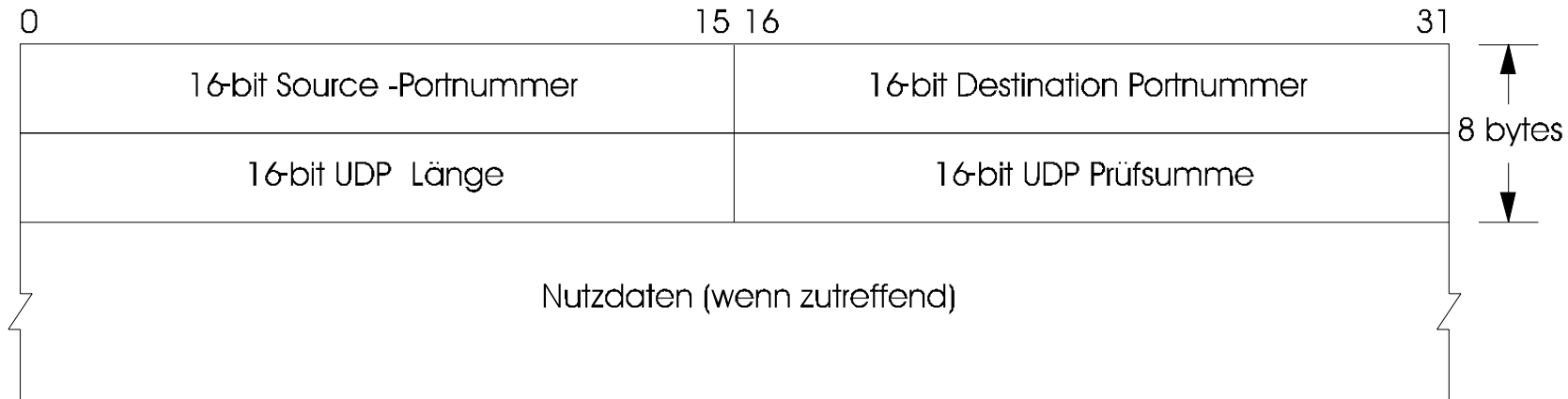




UDP - User Datagram Protocol

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

UDP Header





UDP-Header

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Source / Destination Port Number (jeweils 16 Bit)
 - Multiplexing von Verbindungen
- UDP Länge (16 Bit)
 - Länge von (UDP-Header + Nutzlast), Minimum: 8
- UDP-Prüfsumme (16 Bit)
 - Optional, Algorithmus wie IP-Prüfsumme
 - Prüfsumme über UDP-Header, Nutzdaten, IP-Quell und Zieladresse, Protocol, UDP-Länge
 - Wenn ungerade Anzahl Bytes: Padding mit 0
 - Bei Resultat 0: 0xFFFF (äquivalent zu 0x0, aber 0x0 reserviert)





UDP (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- UDP bietet wie IP nur „best effort“-Übertragung
- UDP-Datagramme werden in voller Größe an IP-Schicht gereicht
 - keine MTU-Anpassung: Fragmentierung
- Keine Bestätigung der Übertragung
 - Erhöhtes Verlustrisiko durch Fragmentierung
- Wird für Broadcast, Multicast benötigt
 - Derartige Mechanismen lassen sich nicht verbindungsorientiert realisieren





UDP (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Einige Protokolle, die UDP verwenden

- DNS
- TFTP
- Sun RPC (NFS, NIS, etc.)
- SNMP
- IKE
- RTP

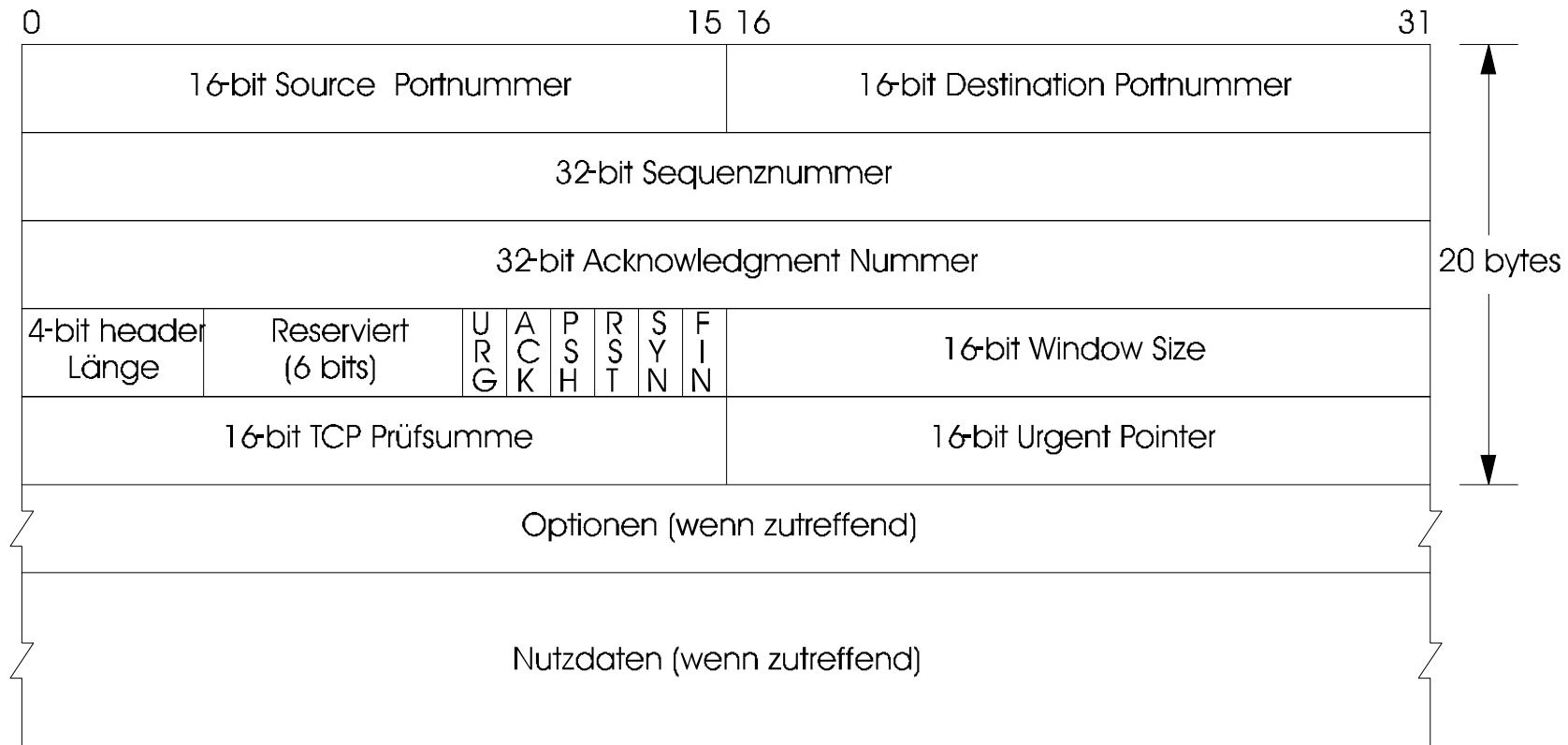




TCP - Transmission Control Protocol

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

TCP Header





TCP-Header (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Source / Destination Port Number (jeweils 16 Bit)
 - Multiplexing von Verbindungen
- Sequenznummer (4 Bytes)
 - Laufende Nummer des ersten Bytes des Segments im Datenstrom des Senders mod 2^{32}
- Acknowledgment Nummer (4 Bytes)
 - Vom Empfänger als nächste Sequenznummer erwartetes Bytes
 - Bestätigt Empfang aller vorheriger Daten
 - nur gültig in Verbindung mit ACK-Flag





TCP-Header (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Header-Länge (4 Bit)
 - Länge des TCP-Headers in 32 Bit- Worten (max. 60 Bytes)
- Reserviertes Feld (6 Bit)
 - muß mit 0-Bits aufgefüllt sein
- URG-Flag (1 Bit)
 - Urgent Pointer ist gültig
- ACK-Flag (1 Bit)
 - Acknowledgment-Sequenznummer ist gültig





TCP-Header (3)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- PSH-Flag (1 Bit)
 - Daten sollen schnellstmöglich an Anwendung übergeben werden
- RST-Flag (1 Bit)
 - Verbindung soll zurückgesetzt werden
- SYN-Flag (1 Bit)
 - Sequenznummern sollen synchronisiert werden (Verbindungsaufbau)
- FIN-Flag (1 Bit)
 - Sender will Verbindung beenden





TCP-Header (4)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Window Size (16 Bits)
 - Maximale Anzahl Bytes, die Sender ab Acknowledgment empfangen will
- TCP-Prüfsumme (16 Bits)
 - Prüfsumme über erweiterten Header - obligatorisch
- Urgent Pointer (16 Bits)
 - Offset, gerechnet von aktueller Sequenznummer, an der die dringenden Daten bei gesetztem URG stehen





TCP-Header (5)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Optionen

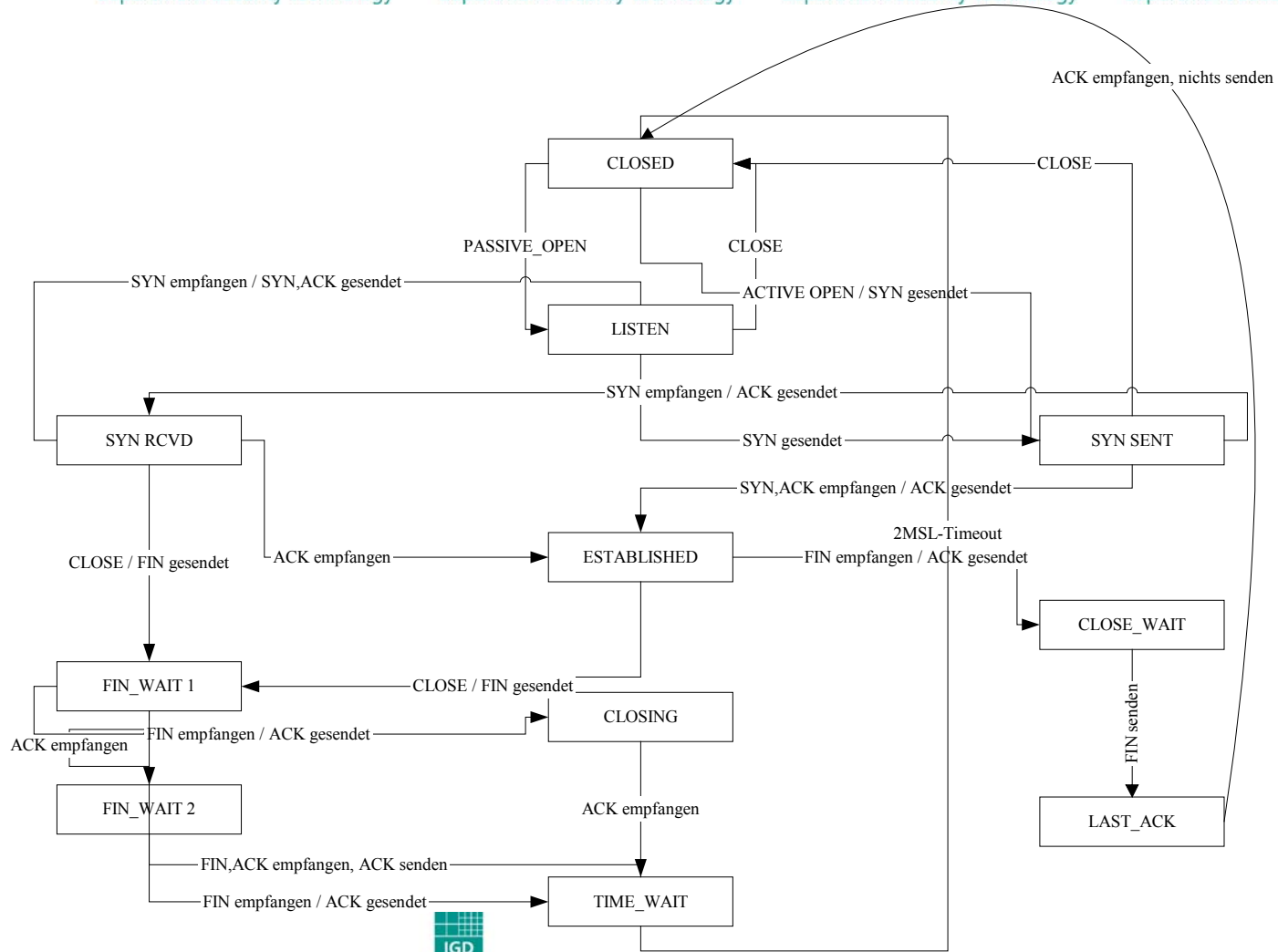
- Variante 1: 1 Byte Opcode
 - ▲ End of Option List
 - ▲ No Operation
- Variante 2: 1 Byte Opcode, 1 Byte Länge, Nutzdaten
 - ▲ Maximum Segment Size
 - △ Länge: 4 Bytes (16 Bit-Wert)
 - △ Maximale Segmentgröße, die Sender entgegennehmen will/kann





TCP-Zustandsautomat

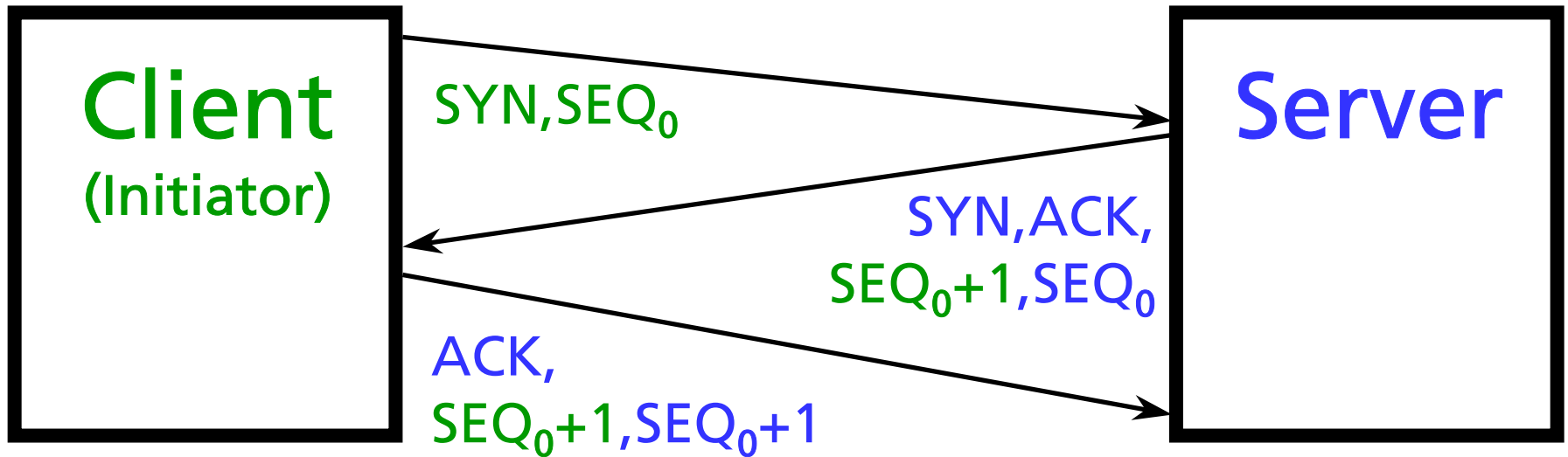
••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





TCP Open (normaler Vorgang)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





TCP Slow Start

... department security technology ... department security technology ... department security technology ... department security technology ...

- Sender muß Rücksicht auf Bandbreite der Verbindung und Pufferkapazitäten entlang der Route und des Ziels nehmen
- Slow start definiert CWND „congestion window“, Initialwert ist „Segment Size“ des Empfängers
- Mit jedem empfangenen ACK wird CWND um ein Segment Size erhöht
- Sender muß Minimum von CWND und Segment Size verwenden
- Implementierung ist zwar Pflicht, aber...





Initial Sequence Numbers, Sequenznummern

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Initiale Sequenznummern einer Verbindung können beliebig gewählt werden
 - Dienen der Unterscheidung von Datenströmen
 - Aufeinanderfolgende ISNs eines Hosts sollten möglichst zufällig sein
- Hohe Bandbreite stellt ein Problem dar
 - ▲ Sequenznummer muß für Lebensdauer im Netz eines Segmentes eindeutig sein
 - ▲ Es stehen nur 32 Bit zur Verfügung - bei Laufzeiten von 2-3s und Gbit/s („slow fat pipe“) ein Problem

