



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Vorlesung SS 2001: “Sicherheit in offenen Netzen“

2.1 Internet Protocol - IP

Prof. Dr. Christoph Meinel

Informatik, Universität Trier & Institut für Telematik, Trier



2. Architektur von Internet und Intranet

- 2.1 **Internet Protocol - IP**
- 2.2 Transmission Control Protocol - TCP
- 2.3 User Data Protocol - UDP
- 2.4 Internetprotokolle für serielle Leitungen
- 2.5 Adressierung in IP Netzwerken
- 2.6 Internet Domain-Name Service - DSN
- 2.6 Internet Protocol Next Generation - IPv6
- 2.7 Absicherung auf der Vermittlungsschicht - IPSec
- 2.8 Netze mit mehreren Standorten
- 2.9 World Wide Web - WWW
- 2.10 Elektronische Post - E-Mail
- 2.11 Internet News
- 2.12 File Transport Protocol - FTP
- 2.13 Terminalemulation - Telnet
- 2.14 Verzeichnisdienst - LDAP
- 2.15 Multimedia



2.1 Internet Protocol (IP) (1 von ...)

(1) Internetprotokoll - zentrale Komponente der Internet-Protokollfamilie:

Anwendungen									NFS (Dateien)	PMAP	NIS (Yellow Pages)
									XDR		
	TELNET (Login)	FTP (Datei transfer)	SMTP (E-Mail)	HTTP (WWW)	Gopher (Gopher)	DNS (Do main- Name)	NTP (Zeit)	RIP (Routing)	RPC (Remote Applikationen)		
Transportschicht	TCP						UDP				
Netzwerkschicht	IP										
Sicherungsschicht	ISO 8802-2										
	Ethernet	ISO 8802-3/ IEEE 802.3	ISO 8802-5/ IEEE 802.5	ISO 9314/ ANSI ASC X 3T9.5	(ISO 3309, 8885)	HDLC (ITU X.25)	LAP-B	922 ITU Q 921/ITU Q	LAP-D (ITU Q 921)	SLIP	PPP RFC 1331
	CSMA/CD		Token- Ring	FDDI							
Bit- Übertragungs- schicht	unterschiedlich (Kupfer, Glasfaser, 9600 Bit/s – 1 GBit/s)										



2.1 Internet Protocol (IP) (2 von ...)

(2) Grundprinzipien des Internetprotokolls IP

Internetprotokoll IP ist

- **paketorientiert** - alle zu übertragenden Daten werden in Datenpakete „IP-Datenpaket“ zerlegt
- **verbindungslos** - Übertragung der einzelnen Datenpakete erfolgt unabhängig von vorhergehenden oder nachfolgenden Datenpaketen
- **nicht garantiert** - es gibt keinen Mechanismus, der für wiederholte Übertragung verlorener Pakete sorgt



2.1 Internet Protocol (IP) (3 von ...)

(3) Format eines IP-Datenpaket (1 von ...)

- Paketlänge abhängig vom
 - Typ des lokalen Netzwerkes, z.B. im Ethernet können Pakete höchstens eine Nutzlast von 1500 Bytes übertragen und
 - Type des Gateways, nach IP-Spezifikation muß jede Intersegmentkomponente (Router) Pakete einer Mindestlänge von 566 Bytes verarbeiten können
- Maximale Länge eines IP-Pakets: 64.535 Bytes



2.1 Internet Protocol (IP) (4 von ...)

(3) Format eines IP-Datenpaket (2 von ...)

Bits 0	4	8	16	19	31
Version		Header-länge	Service-Typ	Gesamtlänge (max. 65.535)	
Identifikation			Flags	Fragment-Offset	
Time To Live (TTL)		Protokoll		Header-Prüfsumme	
Sende-Adresse					
Empfangs-Adresse					
IP-Optionen				Füllbits	
....Daten					
....Daten....					



2.1 Internet Protocol (IP) (5 von ...)

(3) Format eines IP-Datenpaket (3 von ...)

- TTL-Byte („Time To Live“) beschränkt maximale Laufzeit des Pakets im Internet
Bei jedem Vermittlungsknoten wird TTL-Zähler um eins zurückgesetzt. Ist TTL-Zähler 0 vor Erreichen des Ziels, wird das Paket verworfen (um Endlosschleifen bei falschen Routing-Einträgen zu verhindern)
- Prüfsummenfeld zur Verifizierung der fehlerfreien Übertragung der Headerfelder



2.1 Internet Protocol (IP) (6 von ...)

(4) Fragmentierung eines IP-Datenpaket (1 von ...)

Zu lange IP-Pakete können fragmentiert werden:

- jedes Paket-Fragment hat Format eines IP-Pakets
- die Belegung der Felder *Identifikation*, *Flag* und *Fragment-Offset* macht Reassemblierung des ursprünglichen IP-Pakets am Ziel möglich
- Fragmentierung kann durch Flag-Bit 1 unterdrückt werden. (Achtung: Pakete, die nicht übertragen werden können, werden verworfen)



2.1 Internet Protocol (IP) (7 von ...)

(4) Fragmentierung eines IP-Datenpaket (2 von ...)

