Internet Protokoll Version 6
die neue Generation

Lei Zhang
Xiaodong Wang

Übersicht

- Geschichte des Internet Protokolls
- Warum IPv6 ?
- Aufbau des IPv6s
- Sicherheit beim IPv6

Geschichte des Internet Protokolls

- In dem früher 70er Jahre entstand das ARPA-NET (Advanced Research Projects Agency Network) -das erste paket-orientierte Netzwerk.
- Ein paar Jahren später wurden die ARPA-Net-Protokolle durch die Protokoll-Familie TCP/IP verbessert.
- In dem früher 90er Jahre kam die neue Generation IPv6

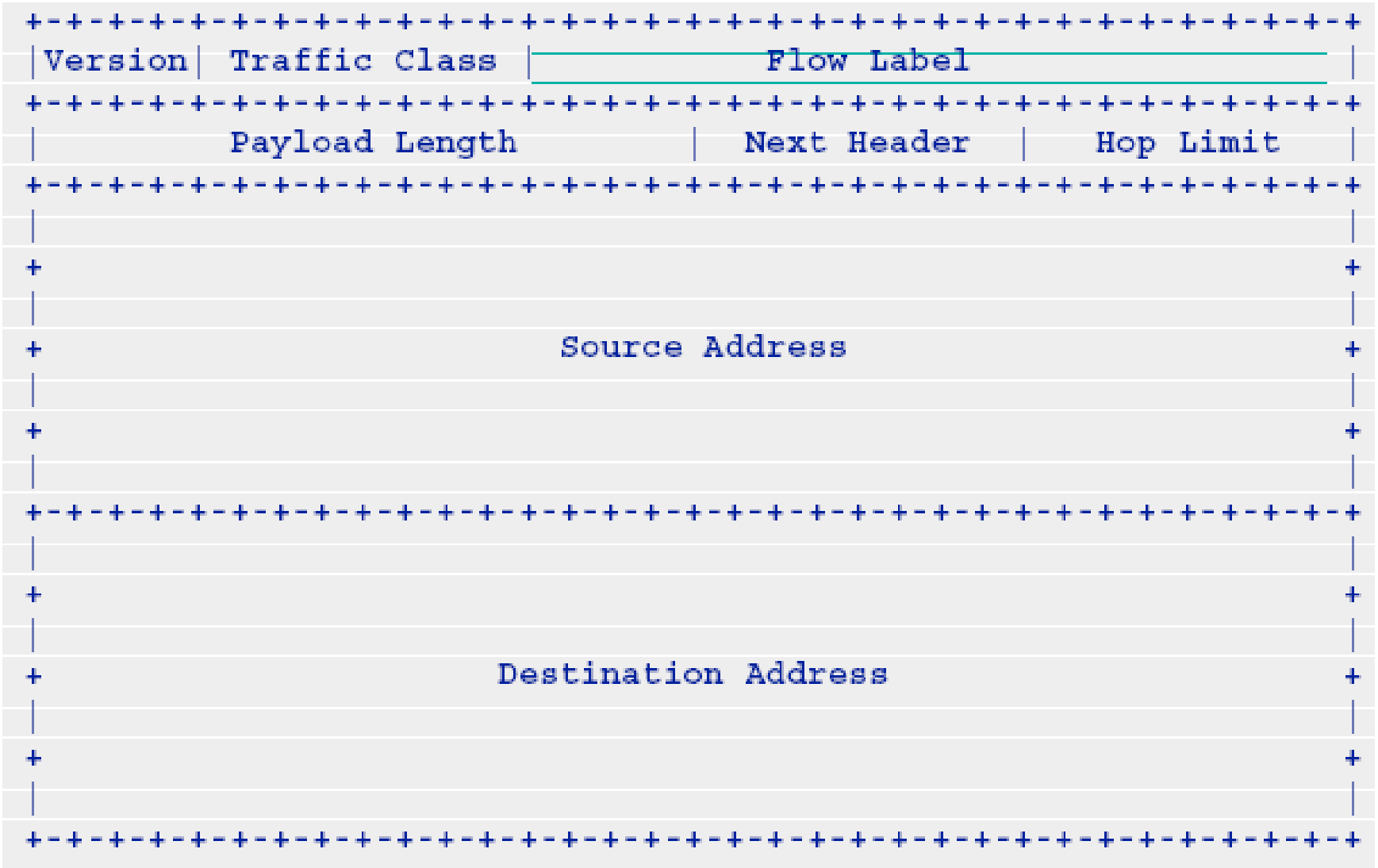
Warum IPv6 ?

- Knappheit im IPv4 Adressraum.
- Sicherheitsfunktionen sind obligatorisch und in jeder IPv6-Implementierung verfügbar
- Routen auf Basis von Flows möglich
- Wesentlich effizienteres Routing möglich
- Einfachere Verwaltung (Autokonfiguration von Knoten ohne irgend eine Einstellung möglich)
- …….

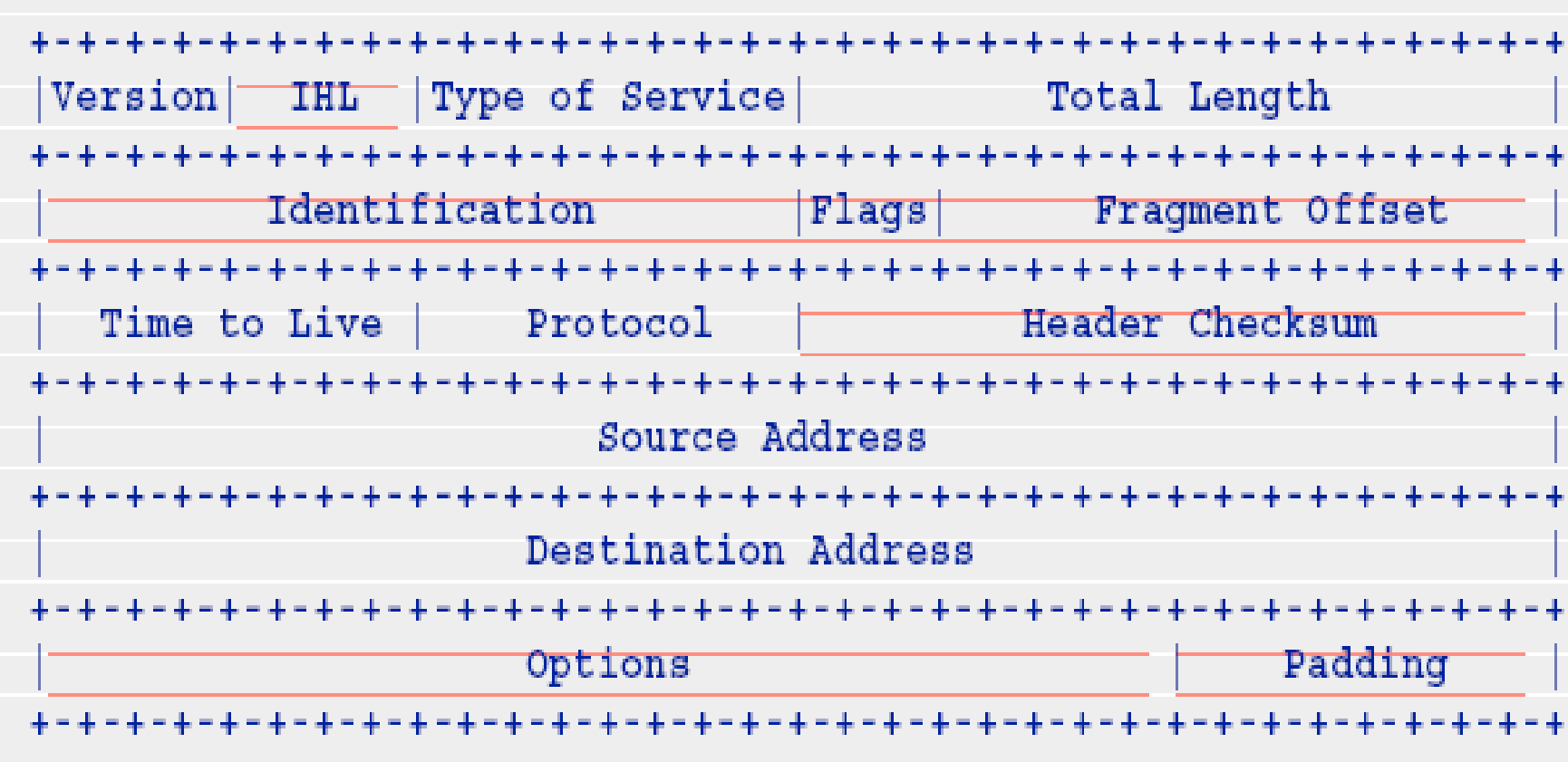
Aufbau des IPv6s

- IPv6-Header
- Adressearchitektur
- Erweiterungsheader

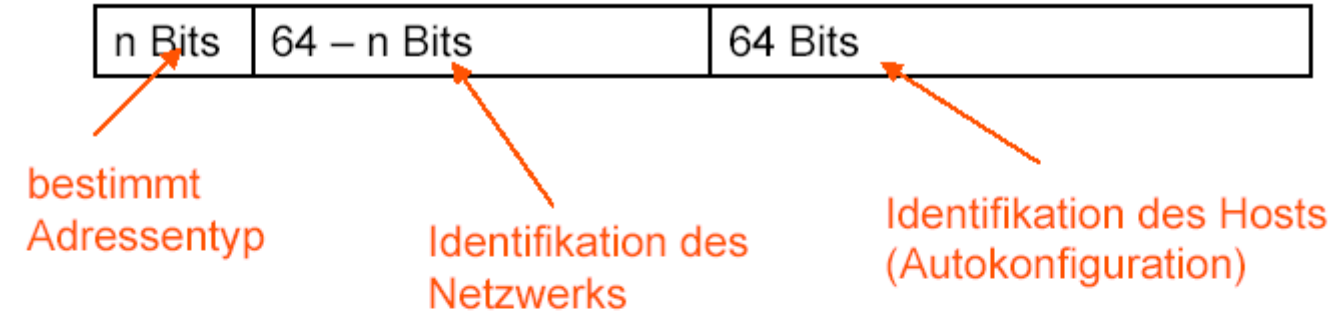
IPv6-Header


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

IPv4-Header


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

Adressearchitektur



ABCD:ABCD:ABCD:ABCD:ABCD:ABCD:ABCD:ABCD

mit A,B,C,D aus {0,1,2,....a,b,c,d,e,f}

Typen von Adressen

- Unicasting (one to one) *(Adresstyp: 001)*
- Anycasting (one to nearest)
- Multicasting (one to many) *(Adresstyp: 1111 1111)*

Erweiterungsheader

- Hop-by-Hop Optionsheader
- Routingheader
- Authentication Header
- ESP Header
- Zieloptionsheader

Sicherheit Grundlagen

- Sicherheit ist zentrales Thema bei IPv6
- IPSEC ist fester Bestandteil von IPv6
- Funktionsumfang von IPSEC
- Umfang des gesicherten Bereichs

Funktionsumfang von IPSEC

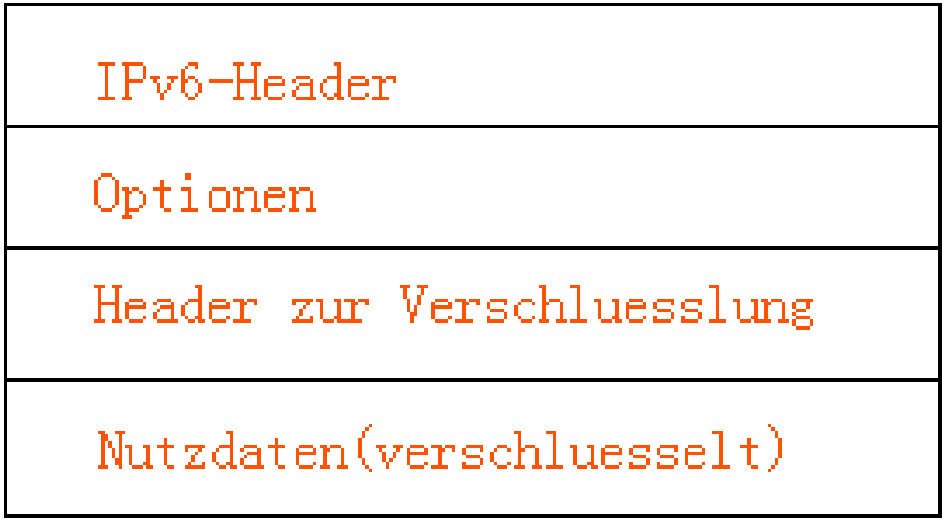
- Verschlüsselung als Sicherung gegen unbefugtes Mitlesen
- Authentisierung der Nachricht durch Prüfsumme zum Beweis der Unverfälschtheit
- Authentisierung des Absenders und der Herkunft durch digitale Signatur

Umfang des gesicherten Bereichs

- Zieladresse(IP-Adresse)
- gewähltes Verfahren zur Verschlüsselung oder Authentisierung
- aktüller(geheimer) Schlüssel für diese Beziehung
- weitere Parameter speziell für dieses Verfahren
- Zeitangabe, wie lange Schlüssel Gültigkeit haben

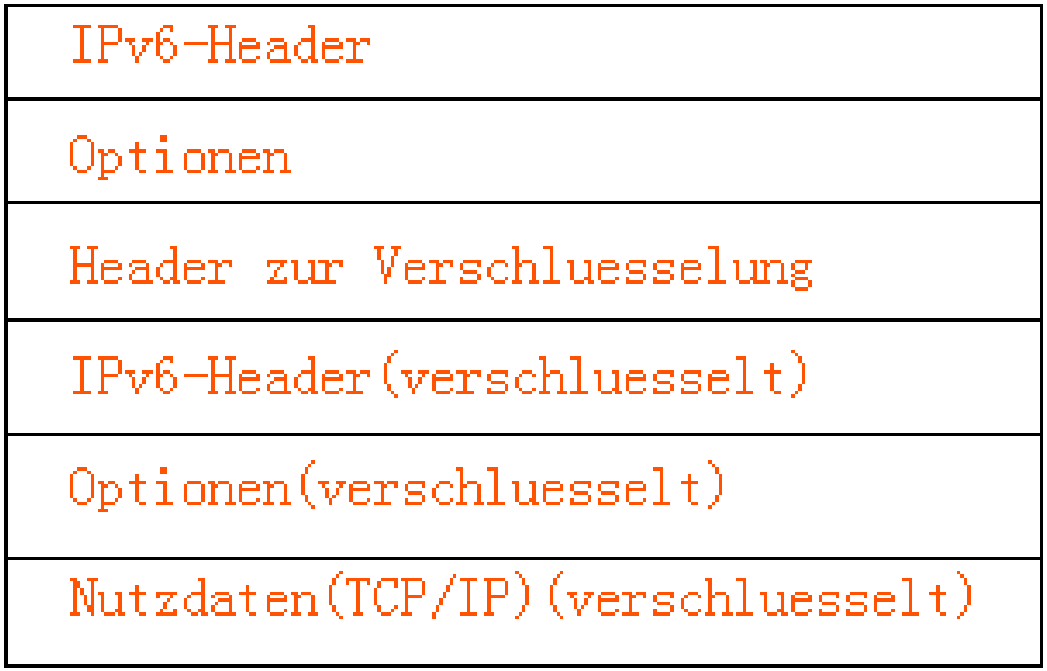
Verschlüsselung bei IPv6 (1)

- Verschlüsselung der Nutzdaten



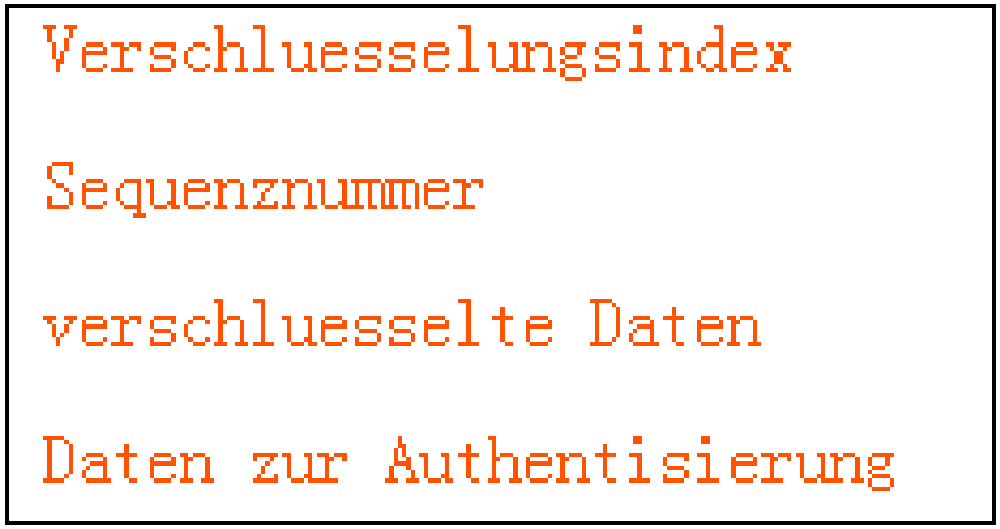
Verschlüsselung bei IPv6 (2)

- Verschlüsselung im Tunnelmodus



Verschlüsselung bei IPv6 (3)

- Header zur Verschlüsselung



Verfahren der Verschlüsselung bei IPv6

- DES-CBC-Verfahrens
- Triple-DES
- AES (Advanced Encryption Stardard)

Authentisierung bei IPv6 (1)

- Authentisierungsverfahren

  Es ist damit zu rechnen, dass in naher Zukunft bei Zugriffen auf DNS-Systeme Mechanismen zur Authentisierung vorgschrieben sei werden. Es ist auch im Standard nicht festgelegt, welche Verfahren zur Authentisierung. Allerdings müssen zumindest die Verfahren HMAC mit MD5 und HMAC mit SHA-1 in jeder Implementierung verfügbar sein.

Authentisierung bei IPv6 (2)

- Authentisierungsheader(AH)

Nächster Header	Nutzdatenlänge	Reserviert(16)
Sicherheitsparameter-Index(SPI)		
Folgenummern-Feld		
Authentifizierungsdaten(variable)		

Fazit

- Wegen der Adressknappheit wird IPv6 unbedingt eingesetzt.
- Der Basisheader wurde vereinfacht, Optionen können bei Bedarf durch Erweiterungsheader dem Datagramm hinzugefügt werden.
- Authentifizierung und Verschlüsselung dienen dem Bedarf nach Sicherheit und Datenintegrität im Internet.
- Die Standardisierung von IPv6 sowie die Standardisierung von Uebergangsstrategien ist weitgehend abgeschlossen.

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?