

Stream Control Transmission Protocol

Achim Friedland
<achim.friedland@stud.tu-ilmenau.de>

Technische Universität Ilmenau
Fakultät für praktische Informatik und Medieninformatik
Fachgebiet Telematik, Dr.- Ing. Werner Horn

30. April 2003

- 1. Hintergrund, Designziele**
- 2. SCTP Paketformat (PDUs)**
- 3. Verbindungsaufbau, Datentransport und -abbau**
- 4. SCTP Multihoming**
- 5. Erweiterungen zum RFC 2960**
- 6. Mögliche Anwendungsszenarien**
- 7. Implementierungen, Literatur, Links, RFCs**

1. Hintergrund

Entwickelt von der IETF Sigtran Working Group zum Transport von Telekom-Signalisierungsdaten (z.B. SS7) über IP Netze, da...

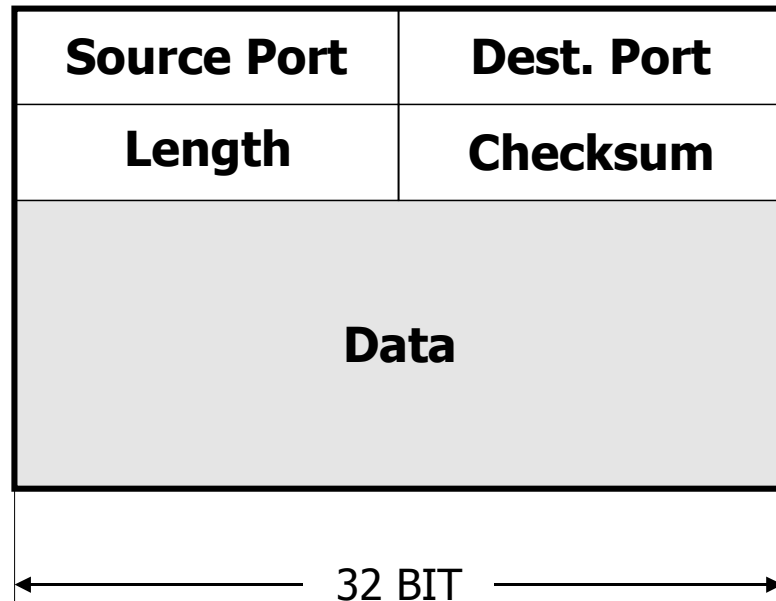
- UDP hierfür nicht mächtig genug ist (Reihenfolgesicherung, Paketverluste, ...)**
- TCP ein Protokoll zum zuverlässigen Transport von "großen" Byte-Streams ist und sich daher für kurze, sofort zu versendende Signalisierungsdaten, die keine strikte Reihenfolgesicherung benötigen, nicht eignet. (Blockierung von Daten, keine Unordered Delivery, zusätzliche Datenkapselung notwendig, kein Selektives-ACK).**
- TCP immense Probleme mit Mobile IP und DOS Attacken hat.**

1. Ziele des Protokolldesigns

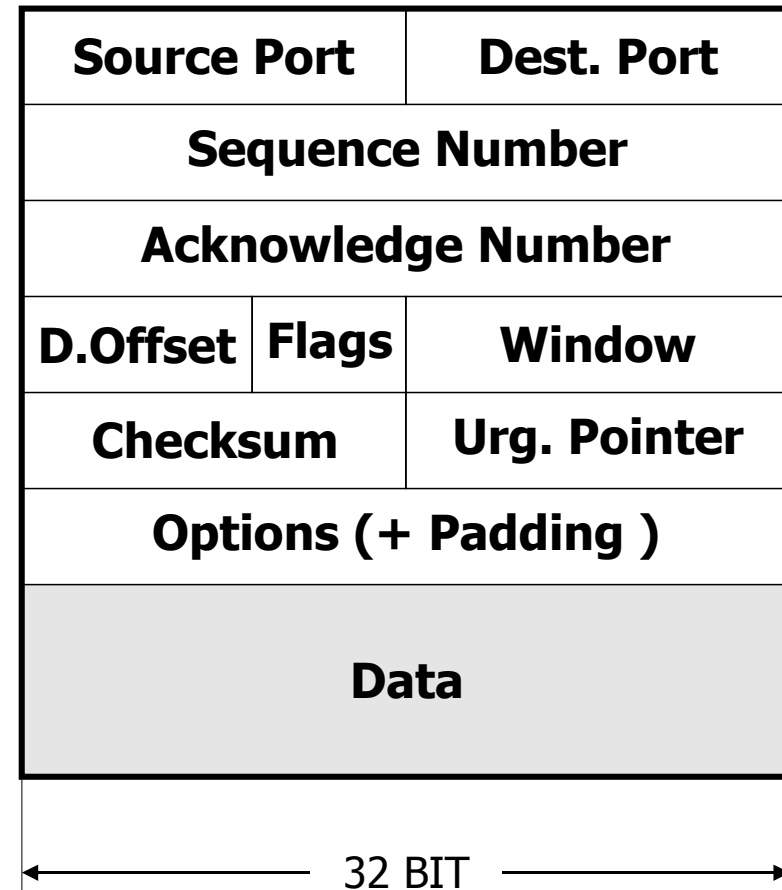
- **zuverlässiger (bestätigter, fehlerfreier, nicht-duplizierter) Transport von Nutzdaten, unabhängig vom:**
- **Reihenfolgegesicherten/-losen Transport in mehreren unabhängigen Streams**
- **Segmentierung der Daten gemäß der entdeckten Path MTU Größe**
- **Multiplexen mehrerer Nachrichten in einem SCTP-Datagramm**
- **Netzwerkstauerkennung/-vermeidung durch "Sliding Window"**
- **Fehlertoleranz auf Netzwerkebene durch Multihoming**
- **Bessere Unterstützung von Selektiven-ACKs und Mobile IP**
- **Schutz gegen Standardangriffe (Denial-of-Service, IP-Spoofing)**

2. Bisherige Protokolle

UDP (IP-Proto: 0x11)

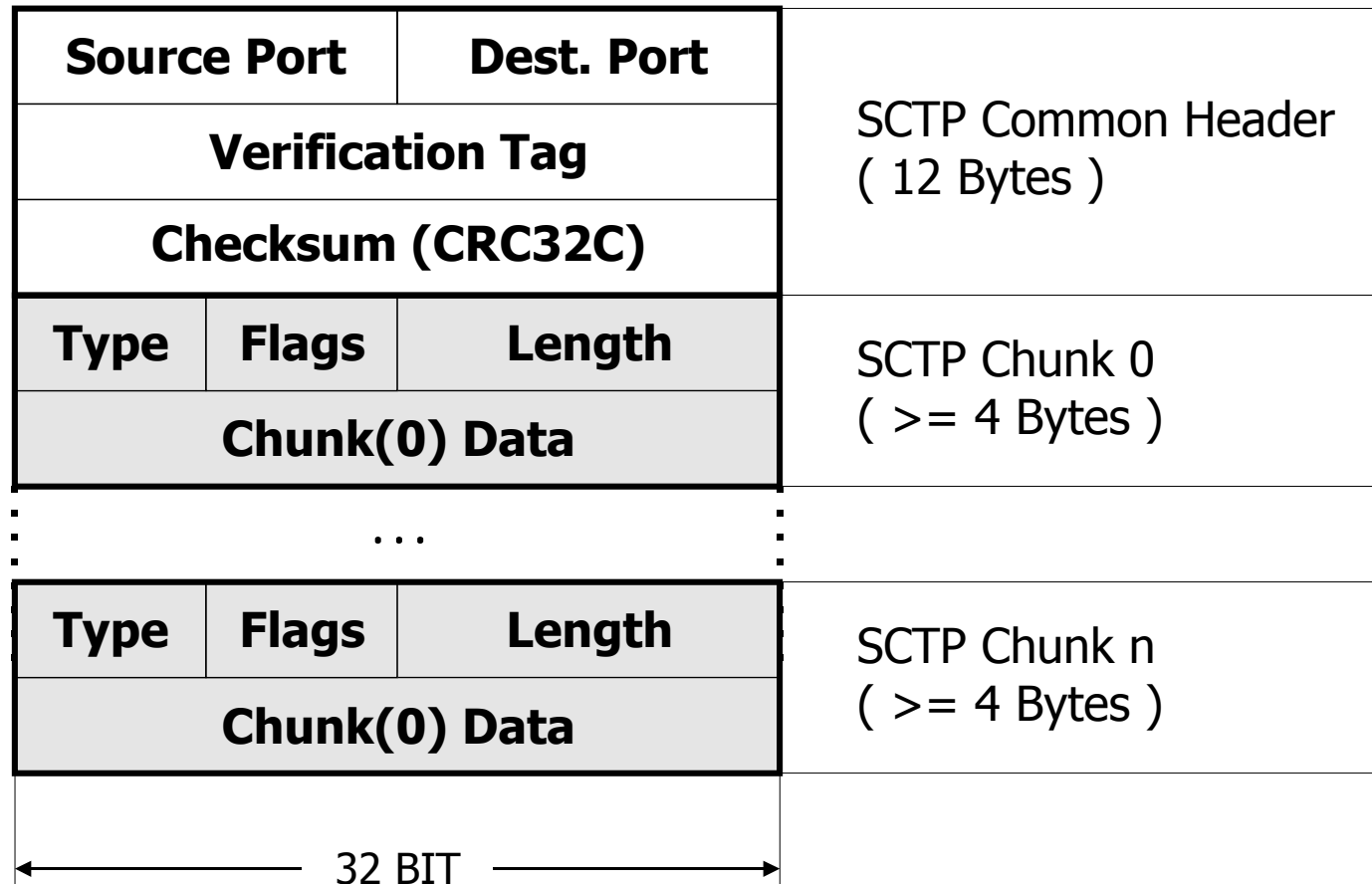


TCP (IP-Proto: 0x06)



2. SCTP Paketformat

SCTP (IP-Proto: 0x84)



2. "Chunk Type" Feld

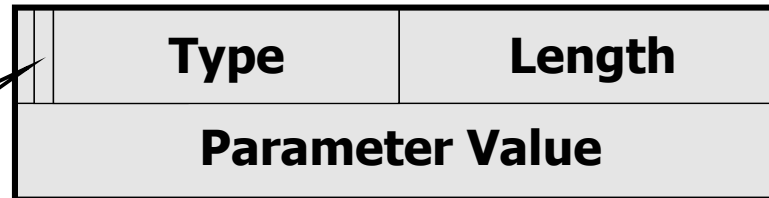


"Unknown Chunk Type" Behavior

- 00 Stop processing this SCTP packet and discard it, do not process any further chunks within it.
- 01 Stop processing this SCTP packet and discard it, do not process any further chunks within it, and report the unrecognized parameter in an 'Unrecognized Parameter Type' (in either an ERROR or in the INIT ACK).
- 10 Skip this chunk and continue processing.
- 11 Skip this chunk and continue processing, but report in an ERROR Chunk using the 'Unrecognized Chunk Type' cause of error.

- 0 Payload Data
- 1 Initiation
- 2 Initiation Acknowledgement
- 3 Selective Acknowledgement
- 4 Heartbeat Request
- 5 Heartbeat Acknowledgement
- 6 Abort
- 7 Shutdown
- 8 Shutdown Acknowledgement
- 9 Operation Error
- 10 Cookie Echo
- 11 Cookie Acknowledgement
- 12 Reserved for Explicit Cong. Notification Echo
- 13 Reserved for Congestion Window Reduced
- 14 Shutdown Complete

2. TLV-Encoded Parameters

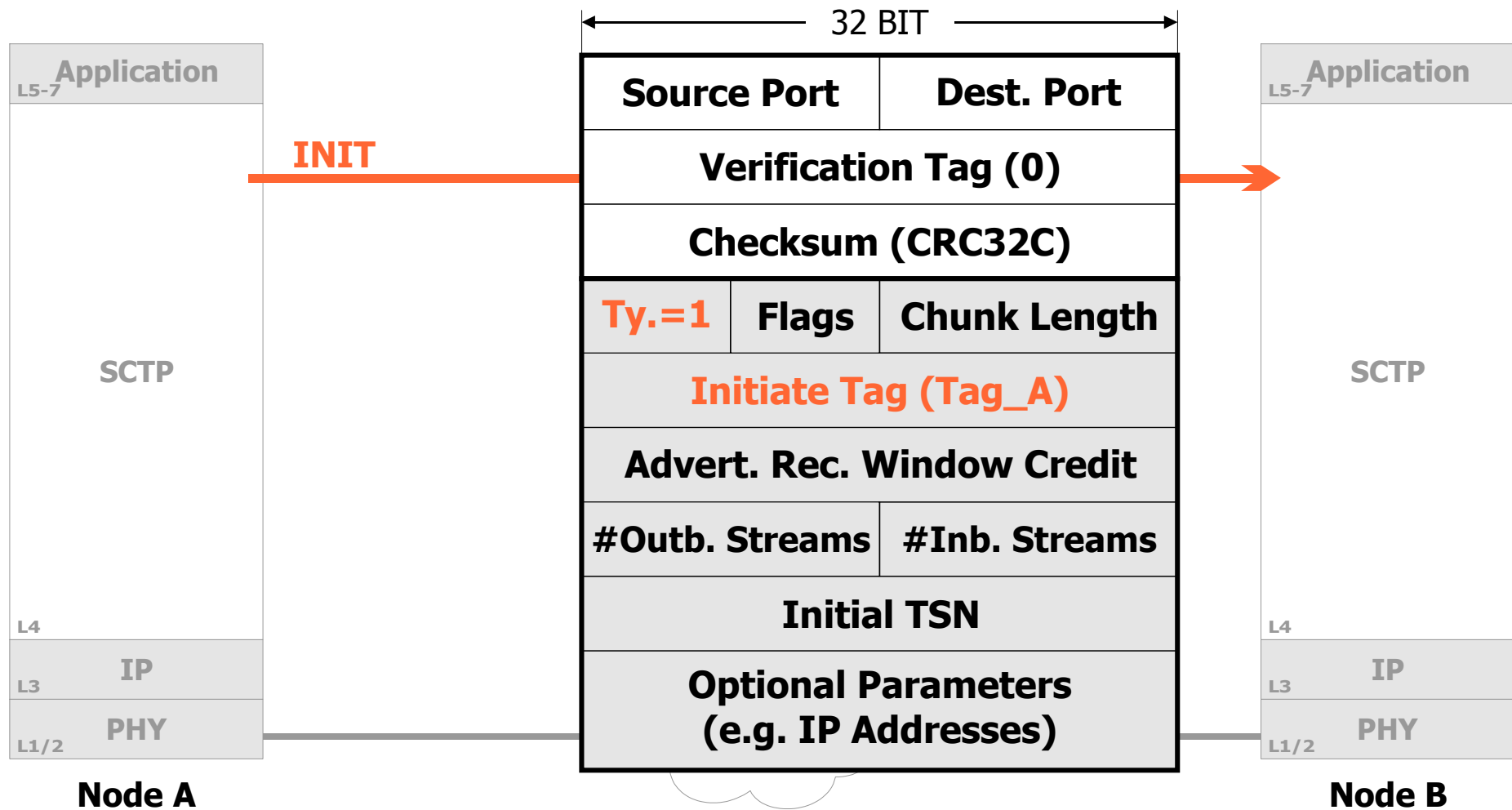


"Unknown Parameter Type" Behavior

- 00 Stop processing this SCTP packet and discard it, do not process any further chunks within it.
- 01 Stop processing this SCTP packet and discard it, do not process any further chunks within it, and report the unrecognized parameter in an 'Unrecognized Parameter Type' (in either an ERROR or in the INIT ACK).
- 10 Skip this chunk and continue processing.
- 11 Skip this chunk and continue processing, but report in an ERROR Chunk using the 'Unrecognized Chunk Type' cause of error.

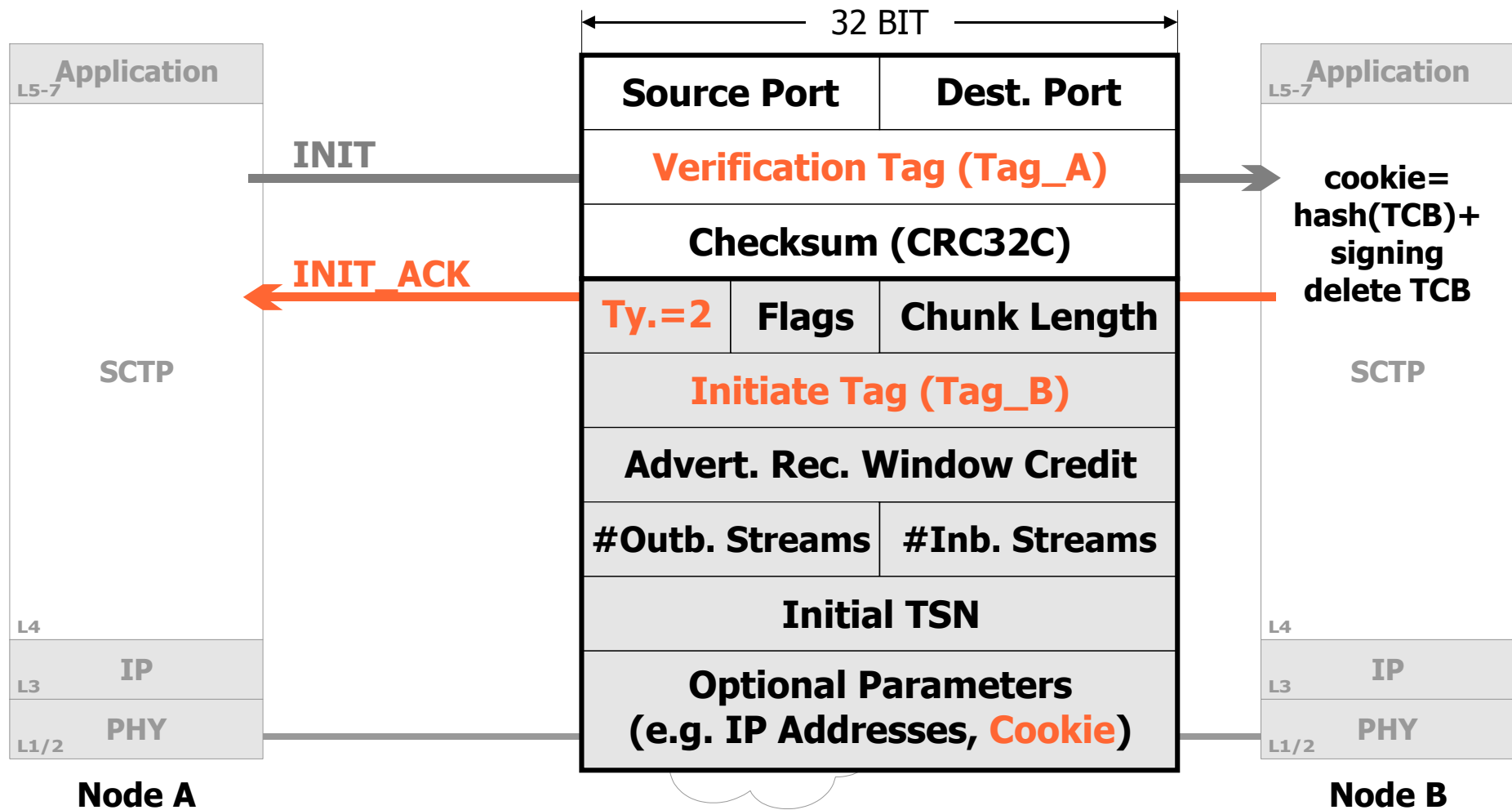
3. Verbindungsaufbau

Schwachpunkt: IP Adressen im "Payload" -> ernste Probleme mit multihomed NAT



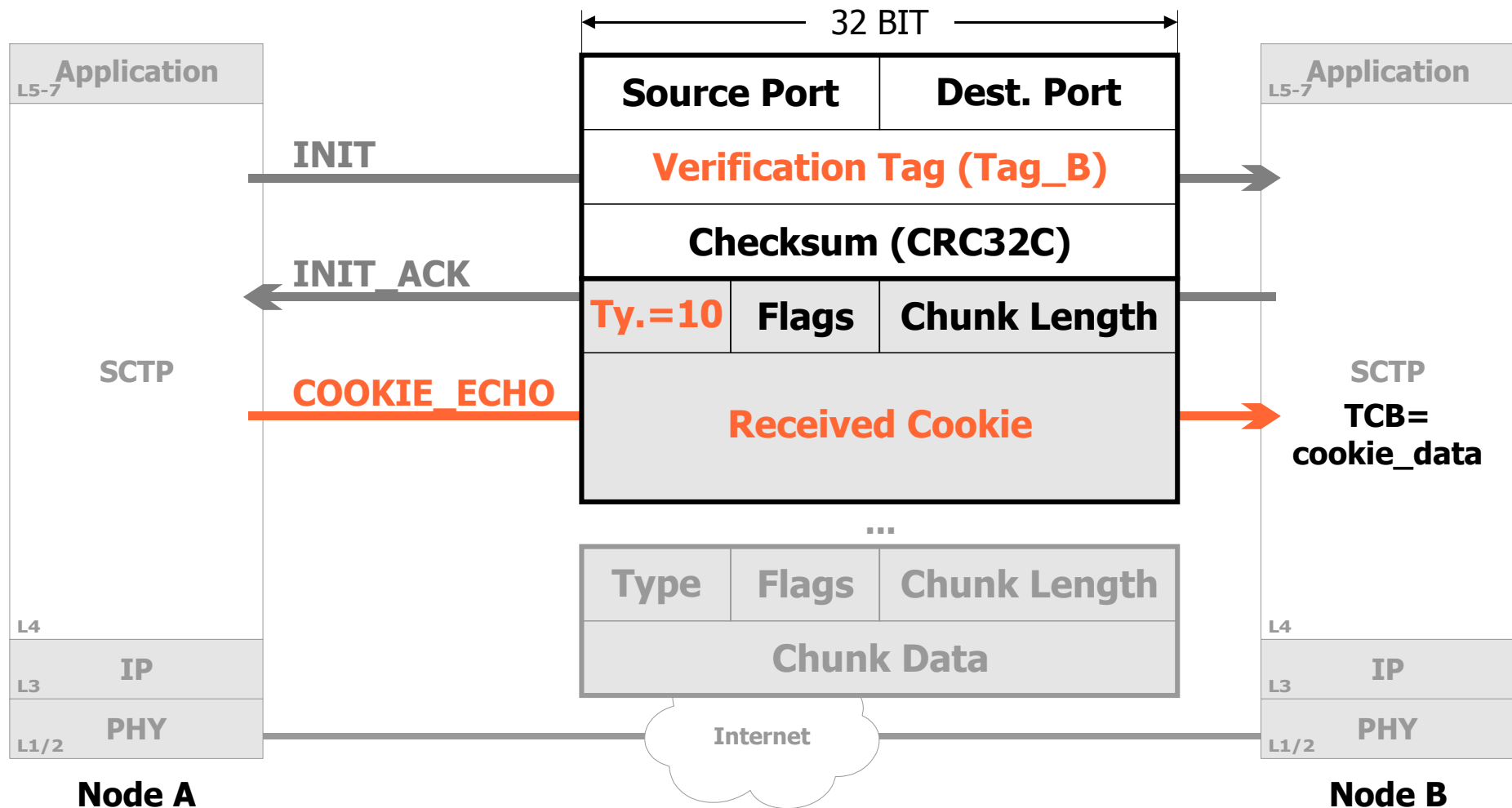
3. Verbindungsaufbau

"SYN Cookies" nach Karn and Simpson (rfc2522)...

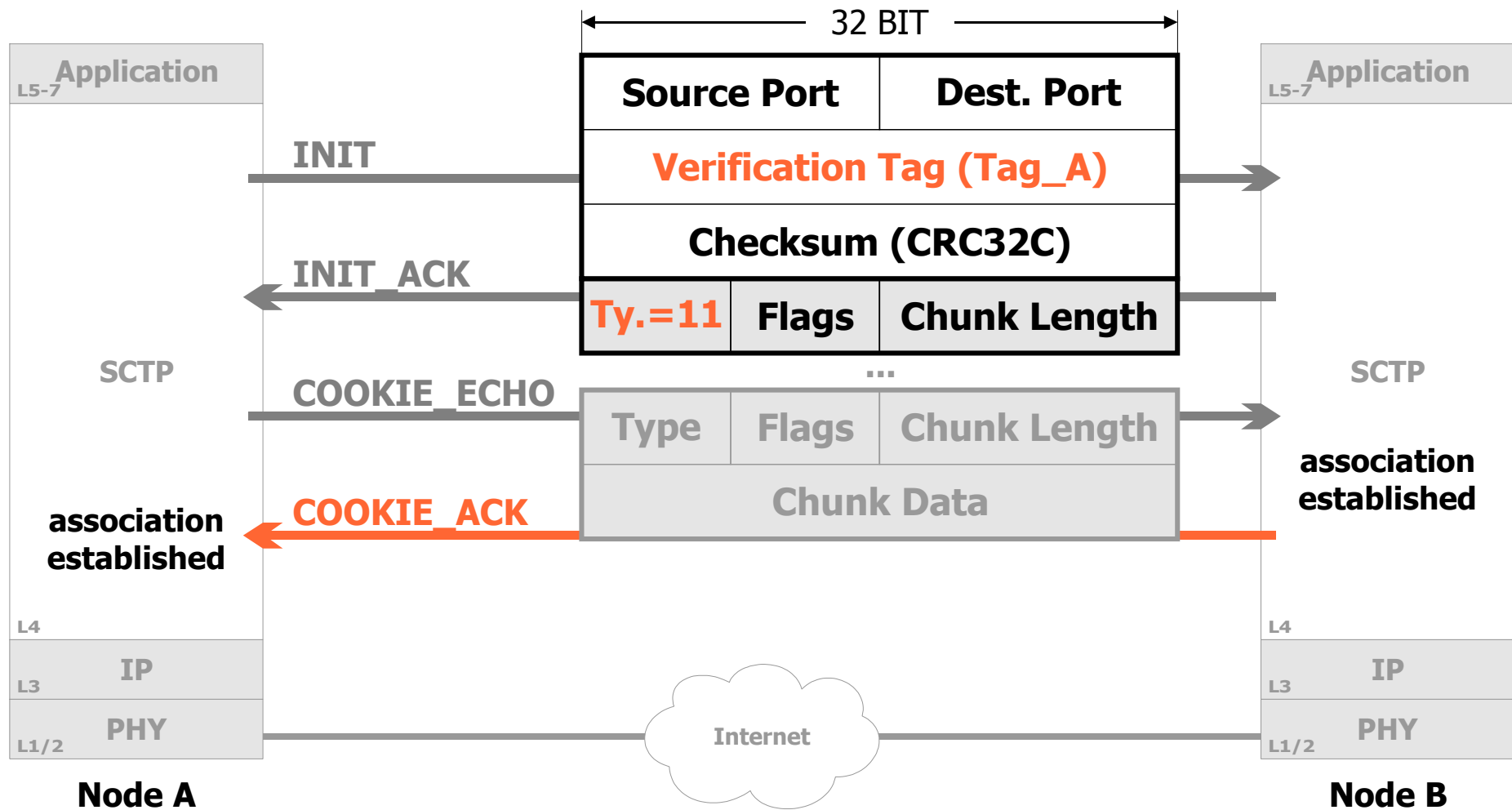


3. Verbindungsaufbau

Transport von Chunks mit Nutzerdaten ö.ä. ist ab hier möglich...



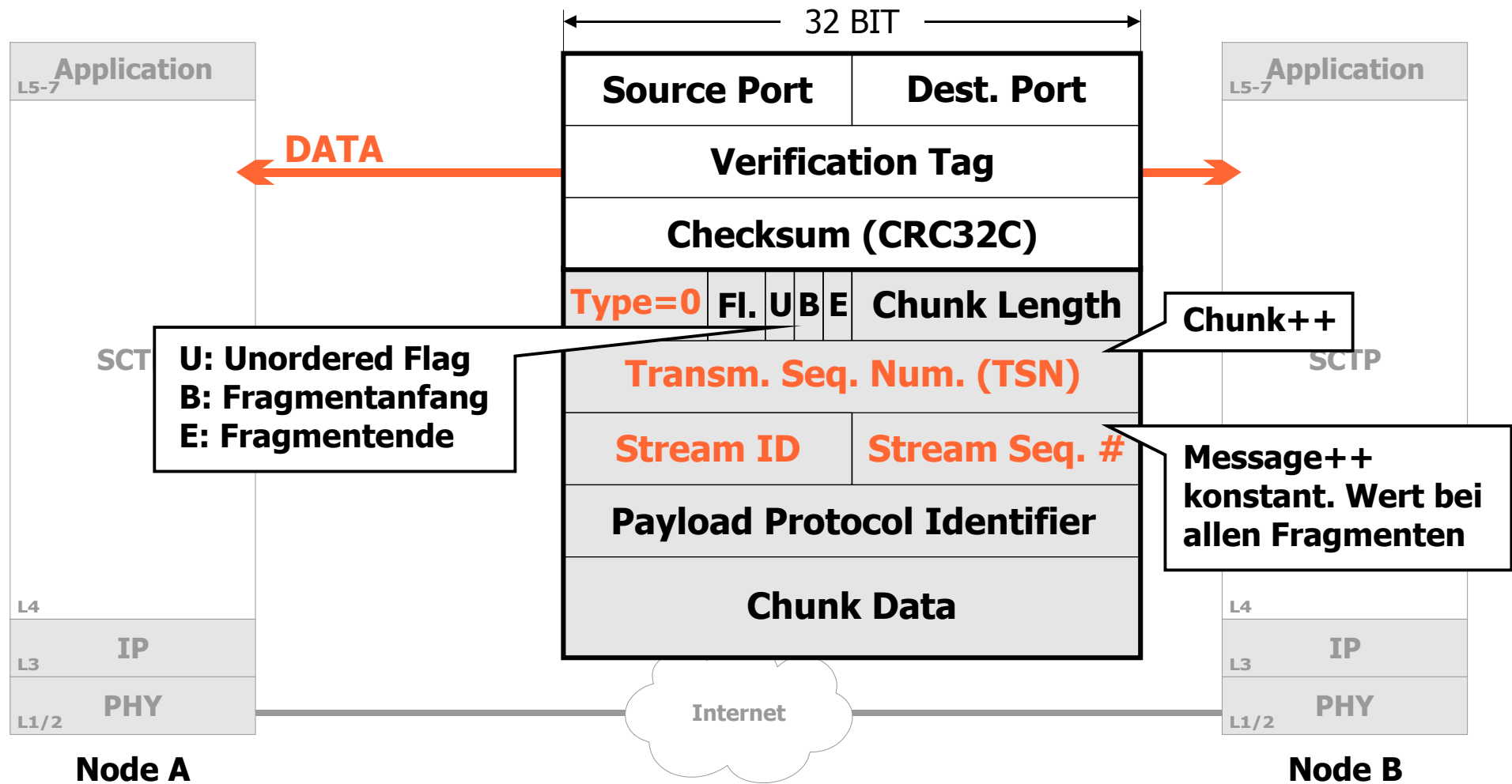
3. Verbindungsaufbau



3. Verbindungsaufbau - Resümé

- **4-Wege Handshake bei dem im 3./4. Bein bereits Daten übertragen werden können**
- **Aushandeln der Zahl der Inbound/Outbound-Streams, der TSN- und der Window Credit Werte**
- **Kryptographischer Cookie Mechanismus zum Schutz gegen DOS Att.**
- **Verification Tag zum Schutz gegen Blind Attacken**
- **Im Resultat schneller als 3-Wege TCP, langsamer als UDP, T/TCP**

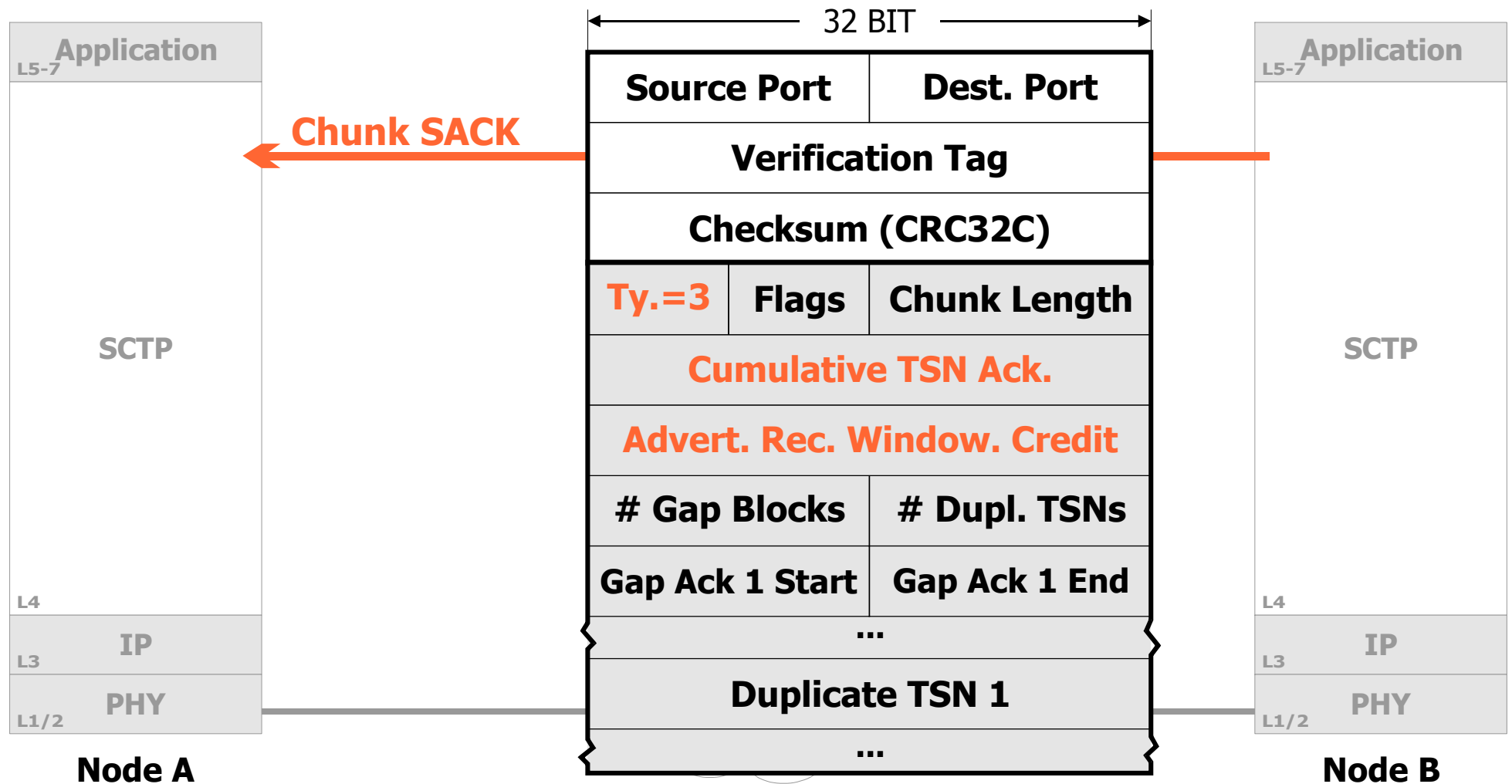
3.1. Datentransport - Data Chunk



3.1. Datentransport - Data Chunk

- **Streams sind uni-direktionale, voneinander unabhängige Verbindungskanäle zwischen den SCTP Endpunkten. Entgegengesetzte Streams gleicher Stream-ID bilden einen bi-direk. Stream.**
- **Reihenfolgesicherung der Datenpakete nur innerhalb eines Streams**
- **"Transmission Sequence Number" nummeriert die Data Chunks
"Stream Sequence Number" nummeriert Nachrichten**
- **"Payload Protocol Identifier" findet heute noch keine Anwendung,
in Zukunft als Ersatz/Erweiterung für Portnummern**

3.2. Datentransport - Selective-ACK Chunk



3.2. Datentransport - Selective-ACK Chunk

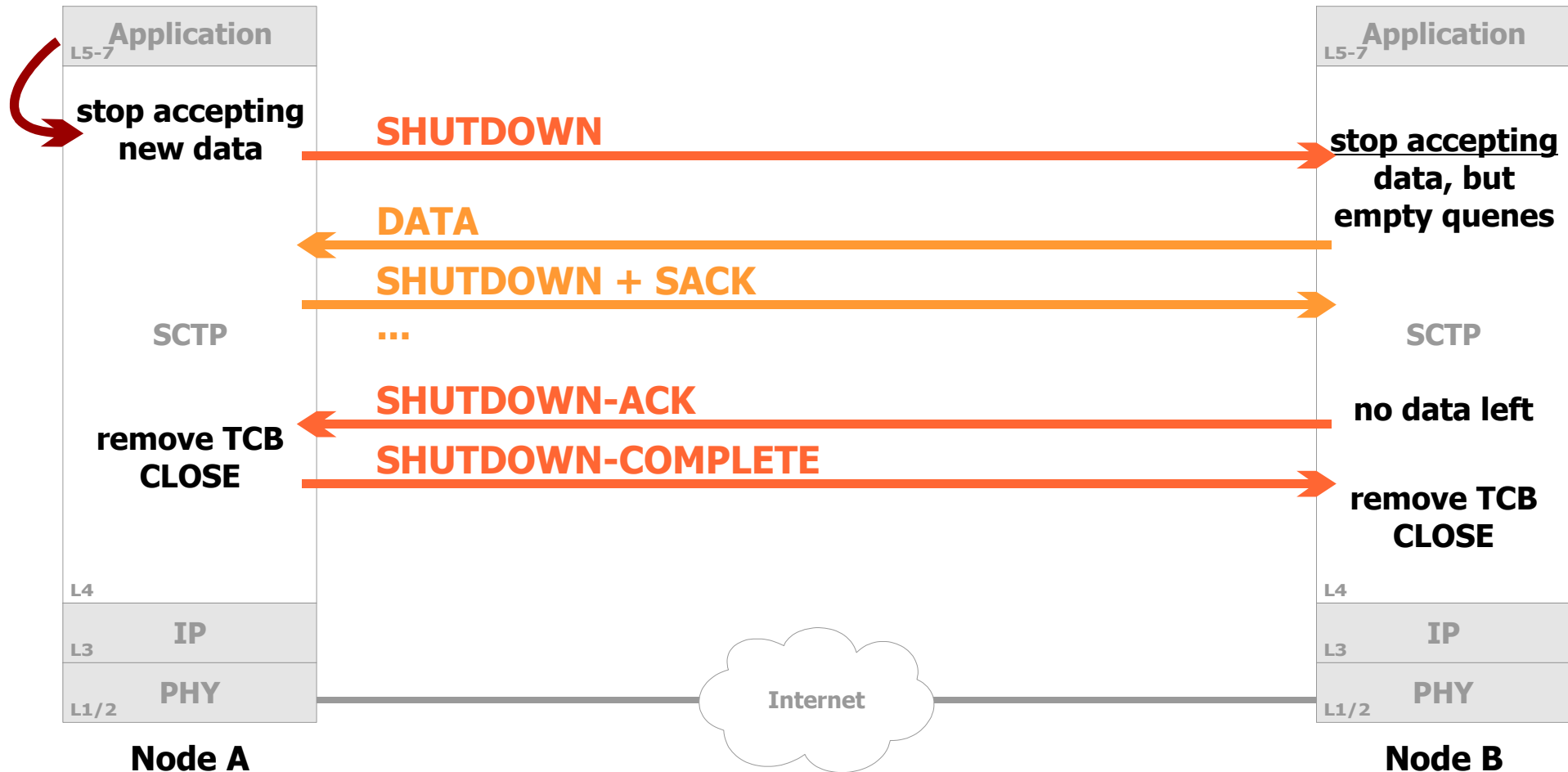
- **"Cumulative TSN Ack"** bestätigt den Empfang aller Chunks bis zu dieser TSN
- **"Adv. Rec. Window Credit"** zeigt die aktuelle Empfangspuffergröße an
- **"Gap Ack Blocks"** bestätigt Blöcke von Daten die nicht in der original Reihenfolge empfangen wurden (relativer Wert bzgl. TSN Ack)
- **"Duplicate TSNs"** zeigt doppelte TSN an (unklarer Nutzen)

3.3. Datentransport - Congestion Control

- **SCTP Congestion Control ist, um eine faire Koexistenz zu gewährleisten, an die von TCP (rfc2581) angelehnt
=> Additive Increase, Multiplicative Decrease (AIMD)**
- **Congestion Control wird immer auf die ganze Association (eigentlich Pfad -> draft), nicht nur auf einen Stream, angewendet.**
- **Path MTU Discovery (rfc1191) z.B. via Heartbeats die das IPv4 Flag "Don't-Fragment" gesetzt haben**

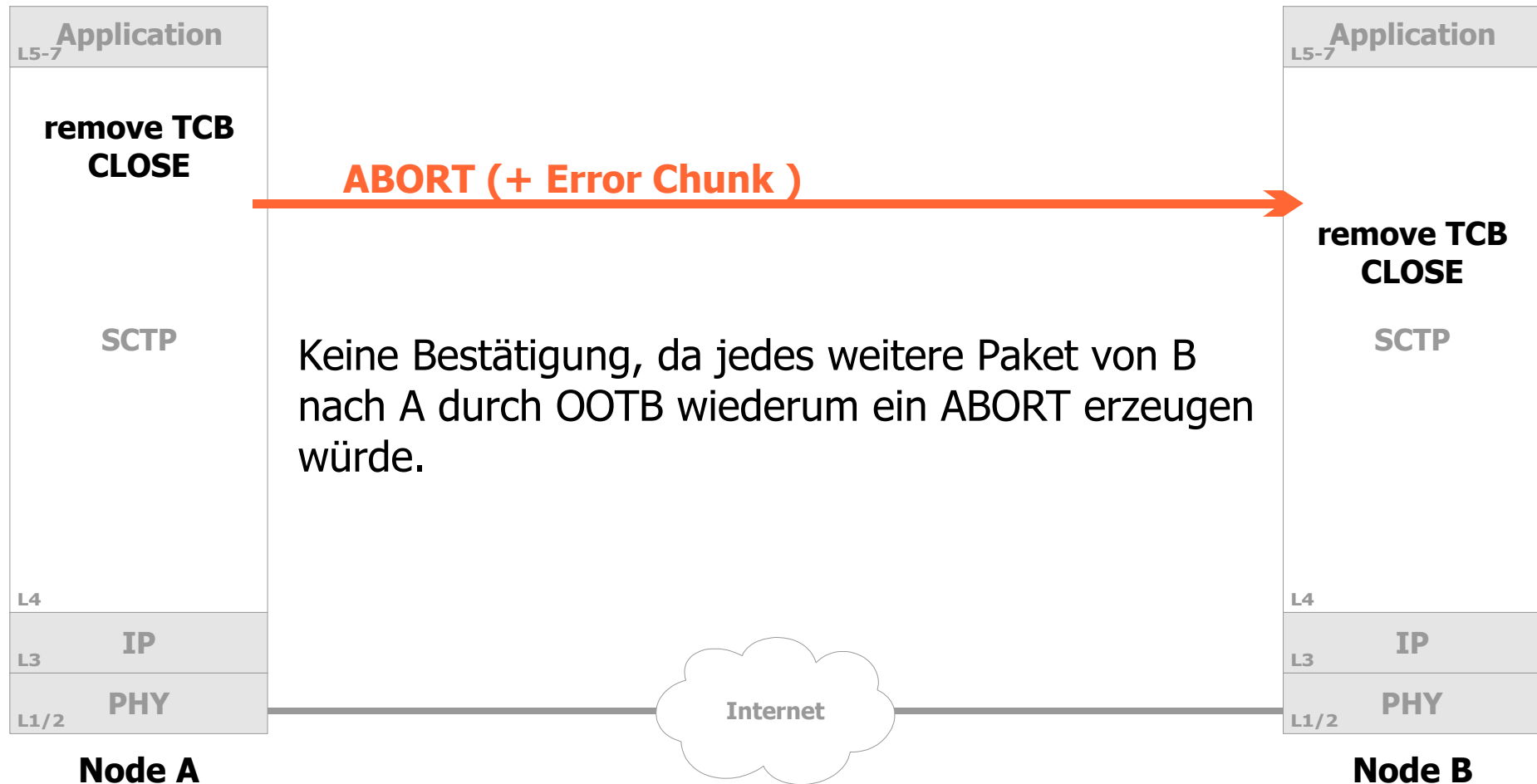
3.4. Verbindungsabbau - Graceful Shutdown

Nur von der Applikation aufrufbar, kein TCP HALF-OPEN...

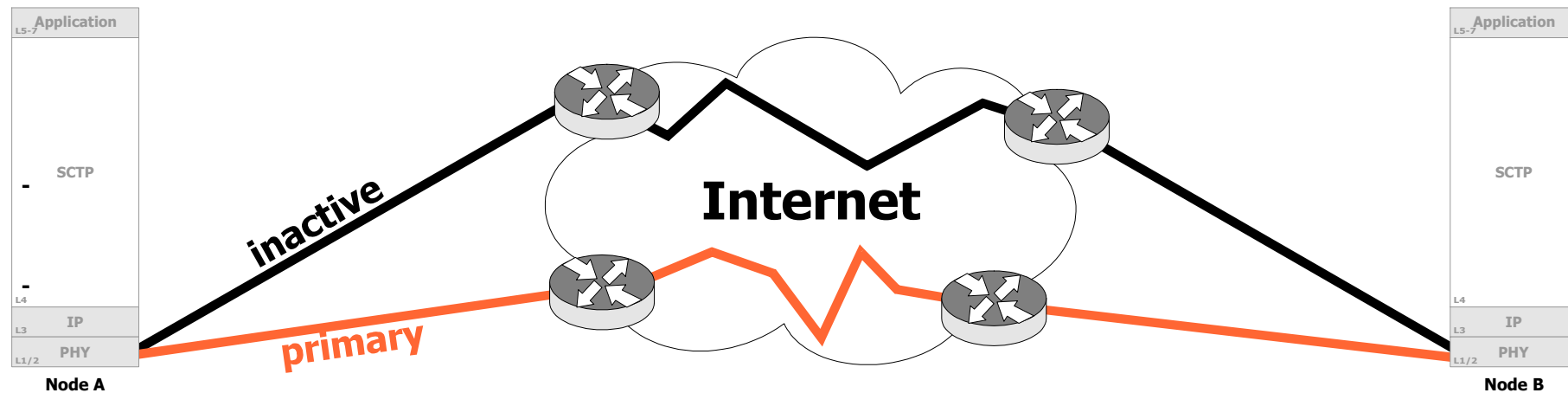


3.5. Verbindungsabbau - Abort

Vom SCTP Stack aber auch von der Applikation aufrufbar...



4. Multihoming



- Mehrere IP Adr. (gleicher Port !) beim Aufbau der Association möglich
- Hiervon bildet eine den "primary path"
- Ziel ist bislang reine Redundanz und kein Load-Sharing
- Inaktive Pfade werden regelmässig mittels Heartbeat überprüft
- IETF Draft beschreibt, das dynamische Hinzufügen neuer IP Adressen (z.B. für Mobile IP)

5. Erweiterungen zu den RFCs

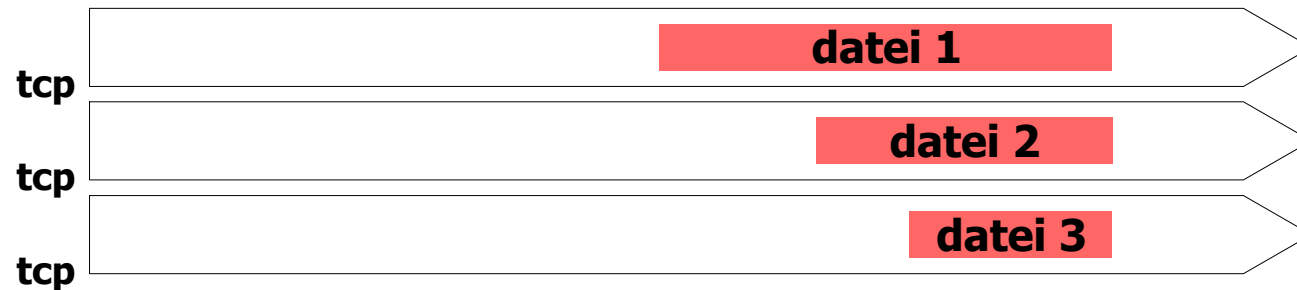
- **"Partially reliable transport with congestions control" (ietf draft)**
z.B. für **SCSI-over-SCTP/IP**
- **"Dynamic IP Addressconfiguration" (ietf draft)**
z.B. für **Internet via Dial-up Verbindungen oder Mobile IP**
- **"Stream-bases flow limiting" (ietf draft)**
Einzelene Streams dürfen nicht die ganze Übertragungsrate nutzen
- **Höhere Performance durch SACK und Retransmits über alternative Pfade (z.B. Satellitenverbindung mit ISDN Kanal).**
- **SCTP-over-IPSec, TLS-over-SCTP (Transport Layer Security)**
- **Explicit Congestion Notification (ECN)**

6. Mögliche Anwendungsszenarien

- **Transport von Signalisierungsdaten in Mobilfunknetzen der 3ten Generation (3rd Generation Partnership Project (3GPP))**
- **Transport von Authentication, Authorization, Accounting (AAA-) Informationen z.B. Diameter (ehemals Radius) (IETF)**
- **Multimedia (Unicast) Streaming (IETF)**
- **Multicast SIP (Session Initiation Protocol) (IETF)**
- **FTP-Protokoll: Mehrere Streams statt mehrerer TCP Verbindungen**

6.1. Mögliche Anwendungsszenarien - HTTP

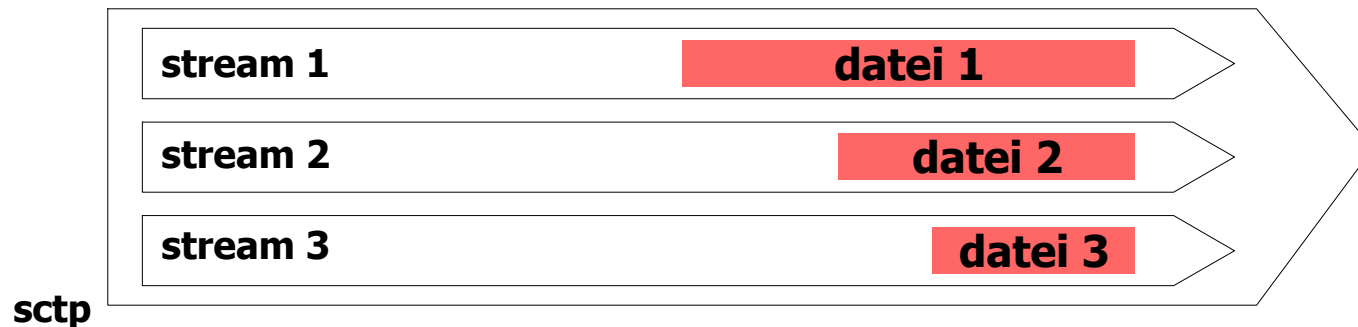
- HTTP/1.0 over TCP: Teure Ressourcen, kein HOL-Blocking



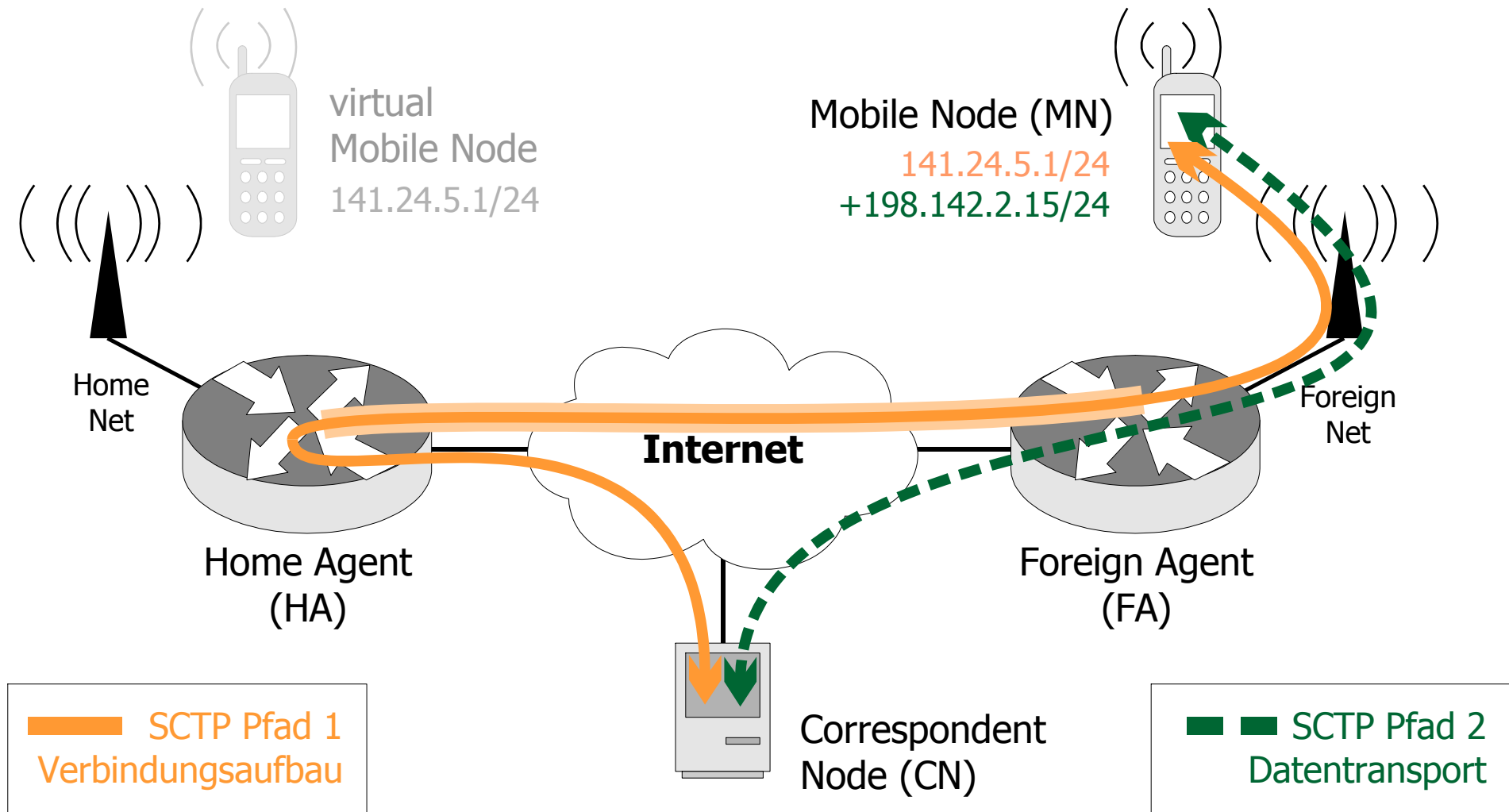
- HTTP/1.1 over TCP: Sparsam mit Ressourcen, HOL-Blocking



- HTTP/1.x over SCTP: Sparsam mit Ressourcen, kein HOL-Blocking

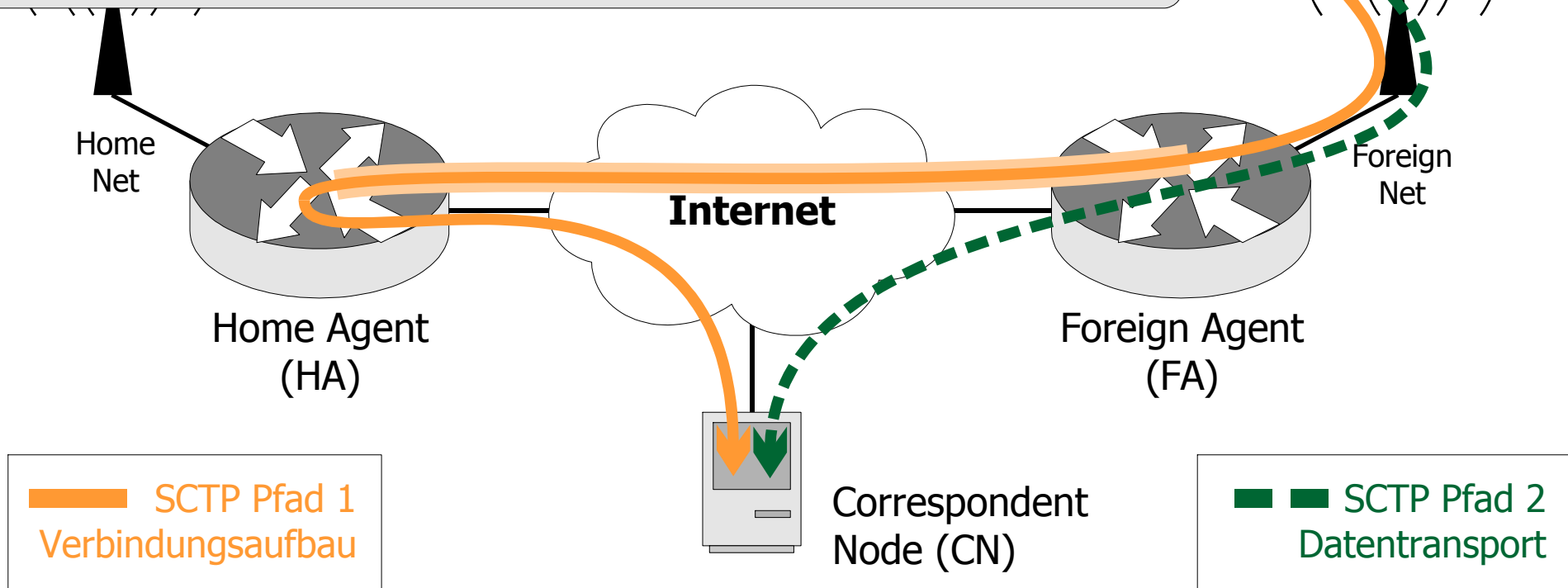
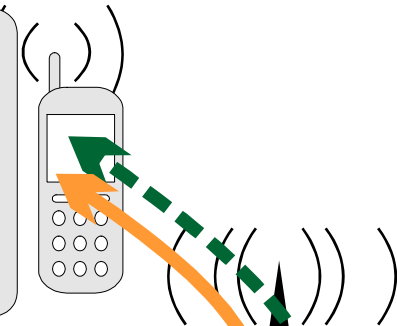


6.2. Mögliche Anwendungsszenarien: Mobile IP und SCTP



6.2. Mögliche Anwendungsszenarien: Mobile IP und SCTP

- Pro:**
- Problemloser Verbindungsaufbau
 - CN lernt neue IP Adresse durch dyn. Addr.conf.
 - Keine "Umwege" beim Datenpfad, keine Tunnel
- Contra:**
- Langsamer als Redirects vom Home Agent



7. Implementierungen, Literatur, Links, RFCs

rfc2960 <http://www.ietf.org/rfc/rfc2960.txt>

rfc3286 <http://www.ietf.org/rfc/rfc3286.txt>

Webseiten <http://www.sctp.de>

<http://www.sctp.org>

Masters Thesis <http://www.sctp.org/IvanAriasRodriguezMastersThesis.pdf>

SCTP4Beginners http://tdrwww.exp-math.uni-essen.de/inhalt/forschung/sctp_fb/index.html

LinuxKernel <http://sourceforge.net/projects/lksctp>
(2.5.x patch)

Solaris 8, HP-UX, ...

Stream Control Transmission Protocol (SCTP)

Vielen Dank

http://www.ahzf.de/itstuff/Hauptseminar_SCTP_Folien.pdf