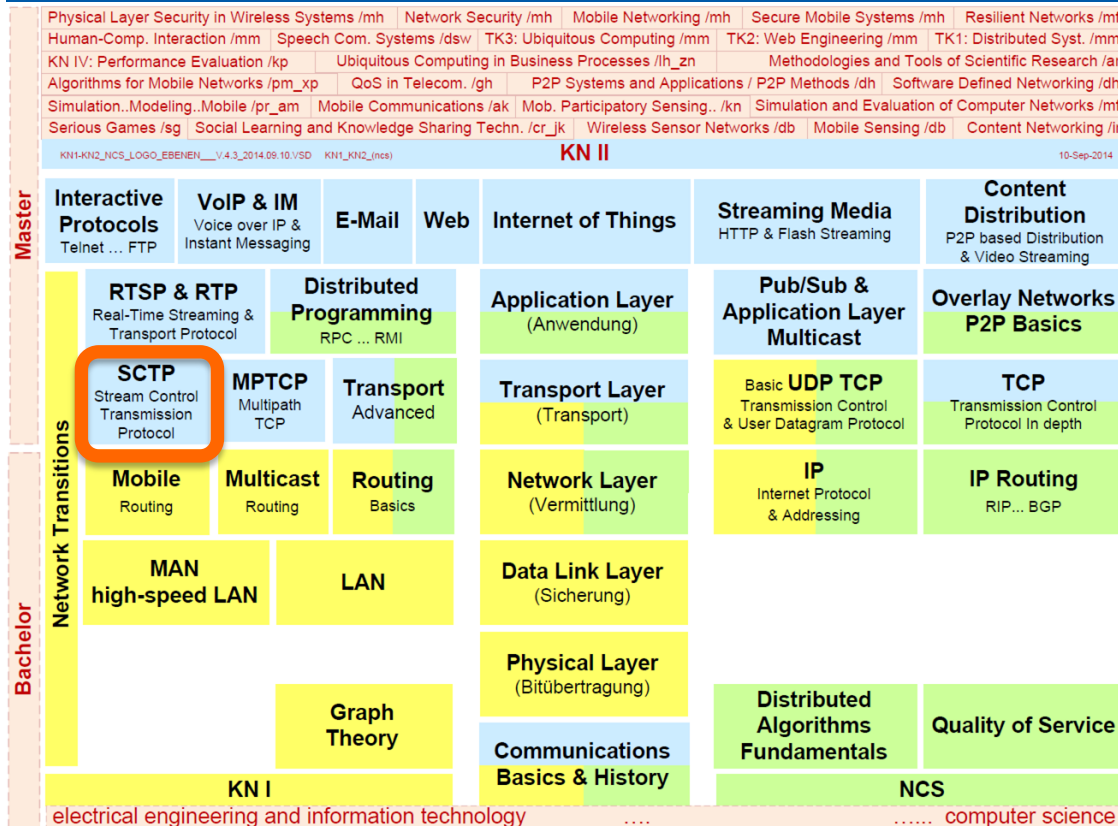


Communication Networks II

Stream Control Transmission Protocol (SCTP)



TECHNISCHE
UNIVERSITÄT
DARMSTADT



10. September 2014

Prof. Dr.-Ing. Ralf Steinmetz
KOM - Multimedia Communications Lab

Physical Layer Security in Wireless Systems /mh	Network Security /mh	Mobile Networking /mh	Secure Mobile Systems /mh	Resilient Networks /mf
Human-Comp. Interaction /mm	Speech Com. Systems /dsw	TK3: Ubiquitous Computing /mm	TK2: Web Engineering /mm	TK1: Distributed Syst. /mm
KN IV: Performance Evaluation /kp	Ubiquitous Computing in Business Processes /lh_zn		Methodologies and Tools of Scientific Research /ar	
Algorithms for Mobile Networks /pm_xp	QoS in Telecom. /gh	P2P Systems and Applications / P2P Methods /dh	Software Defined Networking /dh	
Simulation..Modeling..Mobile /pr_am	Mobile Communications /ak	Mob. Participatory Sensing.. /kn	Simulation and Evaluation of Computer Networks /mf	
Serious Games /sg	Social Learning and Knowledge Sharing Techn. /cr_jk	Wireless Sensor Networks /db	Mobile Sensing /db	Content Networking /ir

KN1-KN2_NCS_LOGO_EBENEN___V.4.3_2014.09.10.VSD KN1_KN2_(ncs)

KN II

10-Sep-2014

Master

Interactive Protocols Telnet ... FTP	VoIP & IM Voice over IP & Instant Messaging	E-Mail	Web	Internet of Things	Streaming Media HTTP & Flash Streaming	Content Distribution P2P based Distribution & Video Streaming
--	---	---------------	------------	---------------------------	--	---

RTSP & RTP Real-Time Streaming & Transport Protocol	Distributed Programming RPC ... RMI	Application Layer (Anwendung)	Pub/Sub & Application Layer Multicast	Overlay Networks P2P Basics
---	---	---	--	--

SCTP Stream Control Transmission Protocol	MPTCP Multipath TCP	Transport Advanced	Transport Layer (Transport)	Basic UDP TCP Transmission Control & User Datagram Protocol	TCP Transmission Control Protocol In depth
---	-------------------------------	---------------------------	---------------------------------------	---	--

Mobile Routing	Multicast Routing	Routing Basics	Network Layer (Vermittlung)	IP Internet Protocol & Addressing	IP Routing RIP... BGP
-----------------------	--------------------------	-----------------------	---------------------------------------	---	---------------------------------

MAN high-speed LAN	LAN	Data Link Layer (Sicherung)
---------------------------	------------	---------------------------------------

Physical Layer (Bitübertragung)	Distributed Algorithms Fundamentals	Quality of Service
---	--	---------------------------

Graph Theory	Communications Basics & History	NCS
---------------------	--	------------

electrical engineering and information technology computer science

Overview

1 Introduction

2 SCTP – Basics

2.1 SCTP Concepts: Association and Streams

2.2 SCTP Concepts: Strict vs. Partial Order

2.3 SCTP: Further Concepts

2.4 SCTP: 4-way Handshake

3 SCTP – Packet Format and Chunks

4 SCTP – Comparison to other Transport Protocols

5 SCTP – Main Features and Extensions

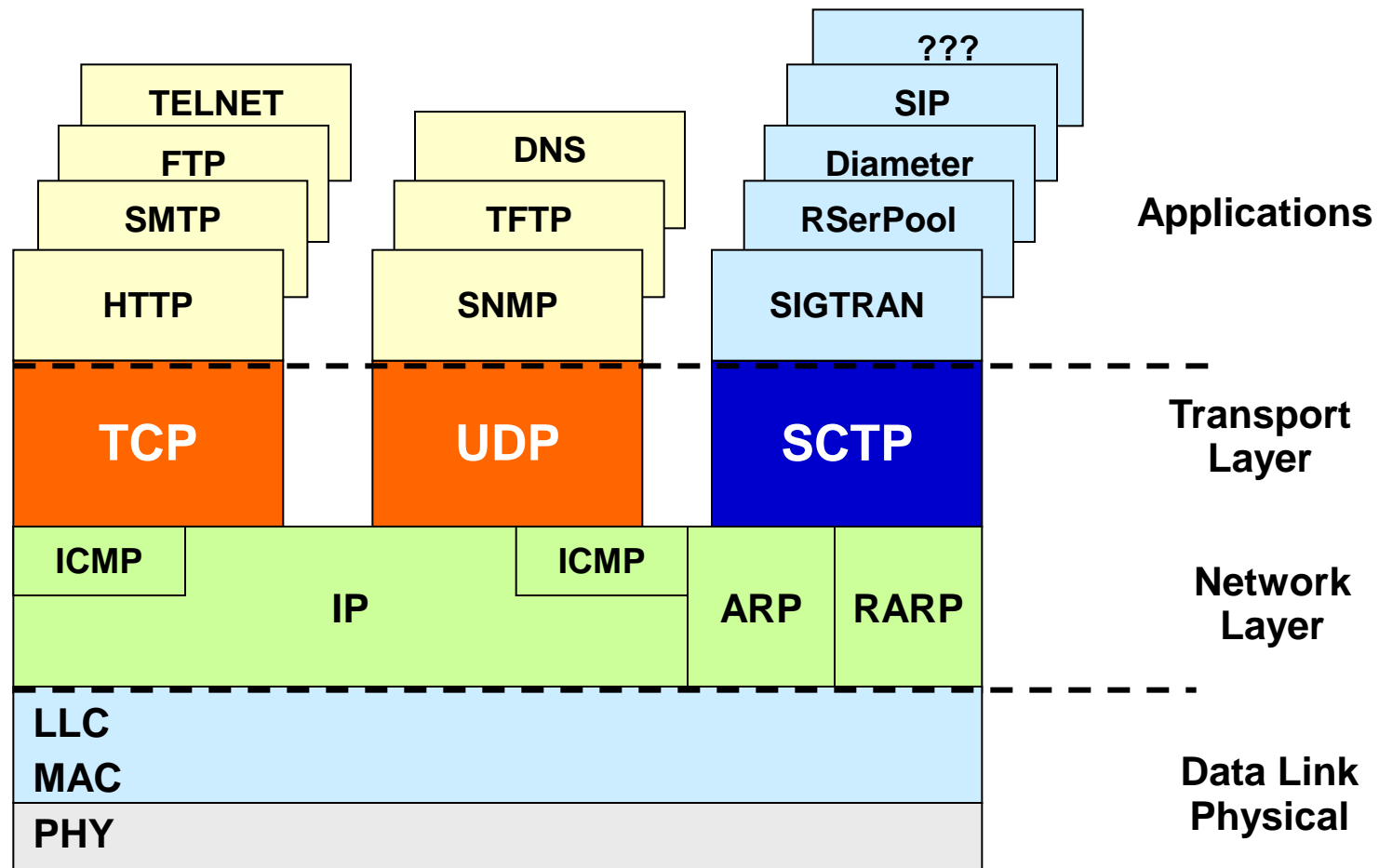
6 Main SCTP Application Scenarios

7 Conclusion and Outlook

1 Introduction

SCTP – Stream Control Transmission Protocol

- see also <http://www.sctp.de>



and: source of very many Slides

- Prof. E.Rathgeb, Duisburg-Essen .. thanks

Motivation

For signaling with high reliability but, low overhead

- Additional transport protocol from IETF
- TCP too limited for some applications:
 - e.g., transport signaling from PSTN networks (SS7) over IP-based networks

Goals

- initial goal
 - to replace SS7 signaling in PSTN with SCTP
- now:
 - SCTP as a universal transport protocol (e.g., for SIP)
- future:
 - To replace TCP (in some cases)

Examples:

- Strict order-of-transmission delivery of data with multiple streams
 - partial order within a stream of multiplexed streams sufficient
- Stream-orientation of TCP inconvenient
 - application must set record markings
 - better: message-orientation
- TCP cannot deal with multi-homing
 - i.e., one server with several IP addresses
- TCP is vulnerable to DoS attacks
 - e.g., SYN flooding

Specification in

RFC 2960

- Stream Control Transmission Protocol

RFC 2719

- Architectural Framework for Signaling Transport

RFC 3057

- ISDN Q.921-User Adaptation Layer

see also

- <http://www.sctp.de/>
- <http://www.tdr.wiwi.uni-due.de/forschung/forschungsprojekte/sctp/#c11432>

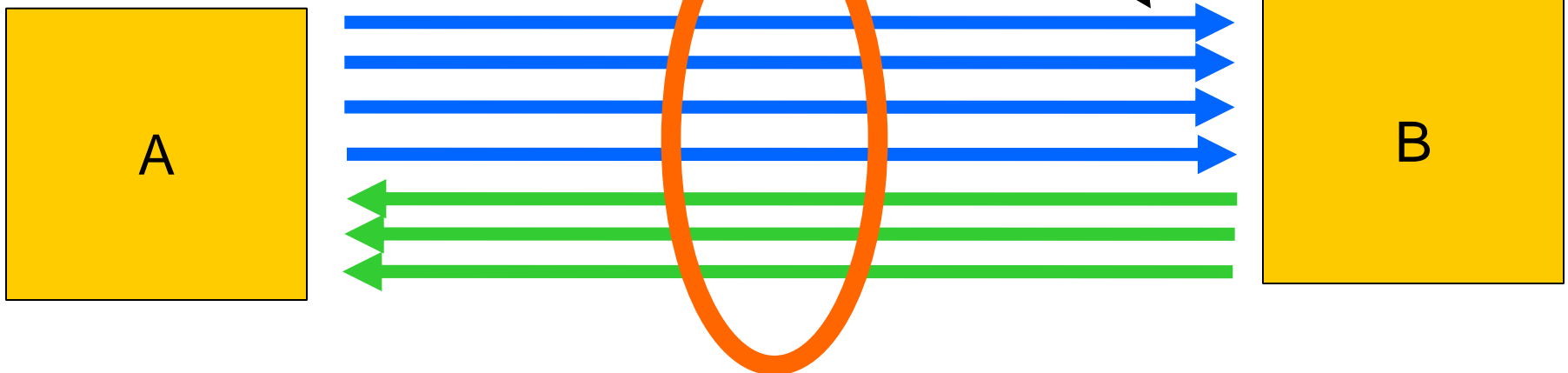
2 Sctp – Basics

SCTP association

- analogous to TCP connection

SCTP Streams

- unidirectional channels for message transmission (up to 2^{16} per direction)
- Number of streams negotiated at connection initiation
- streams

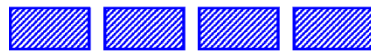


2.1 SCTP Concepts: Association and Streams

Connection-oriented:

- concept of ‘association’
 - bi-directional
- generalization of TCP-connections:
 - each association endpoint can have several IP addresses (multi-homing)
 - each association can contain several streams (multi-streaming)

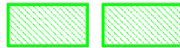
Stream A:



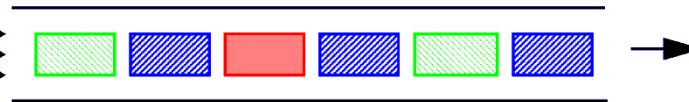
Stream B:



Stream C:

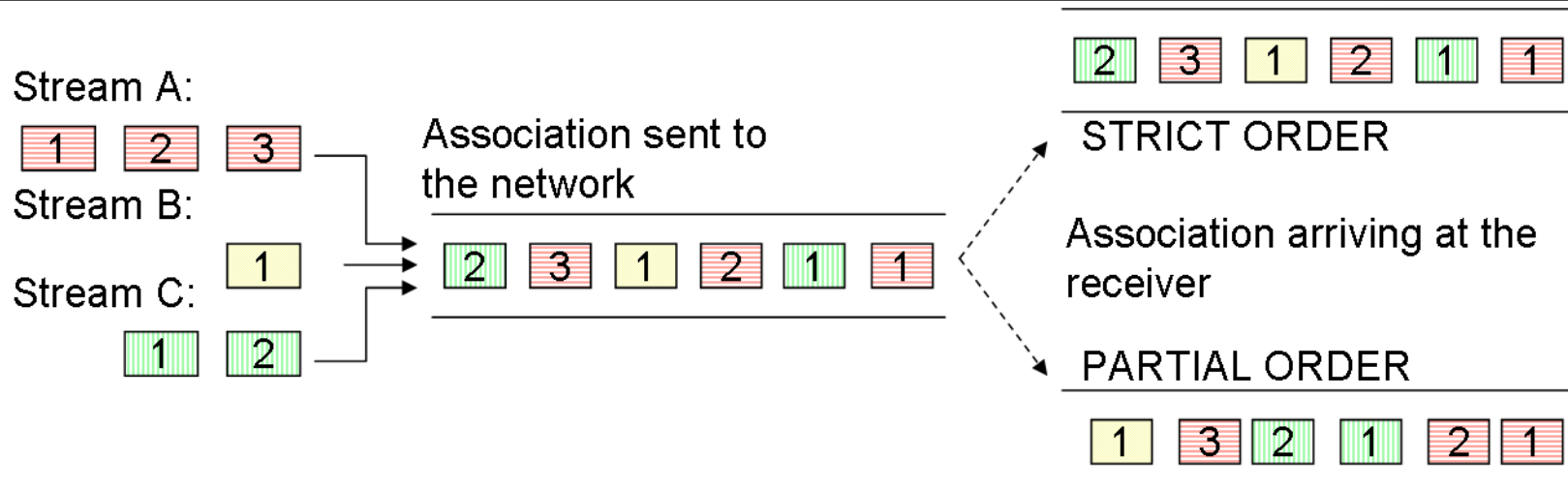


Association



- Stream: sequence of user messages to be delivered in order
 - up to 2^{16} per direction
 - → in contrast to the notion of ‘stream’ of TCP
- Reliable data transfer
 - confirmed, no duplicates, error-free

2.2 SCTP Concepts: Strict vs. Partial Order



Strictly ordered delivery optional

- packets of a stream within an association are delivered in order
 - partial order
- optional:
to retain order between packets of all streams
 - strict order

effects

- strict order:
 - data transmission stalled if one stream is stalled
- partial order:
 - transmission for non-stalled streams can continue

Example:

HTTP with multiple embedded files (images)

- Order of arrival of image data not relevant
- Retrieving the text can continue even if loading the image is blocked
 - e.g., if the image is located on a different server which is highly loaded

2.3 SCTP: Further Concepts

Message segmentation according to path-MTU

- Path-MTU:
 - maximum transfer unit supported on the path between the endpoints
- Path-MTU discovery mechanism as specified in RFC 1191

Test whether the communication partner is alive:

- Heartbeats

Flow control and congestion control similar to TCP (Selective Ack,...)

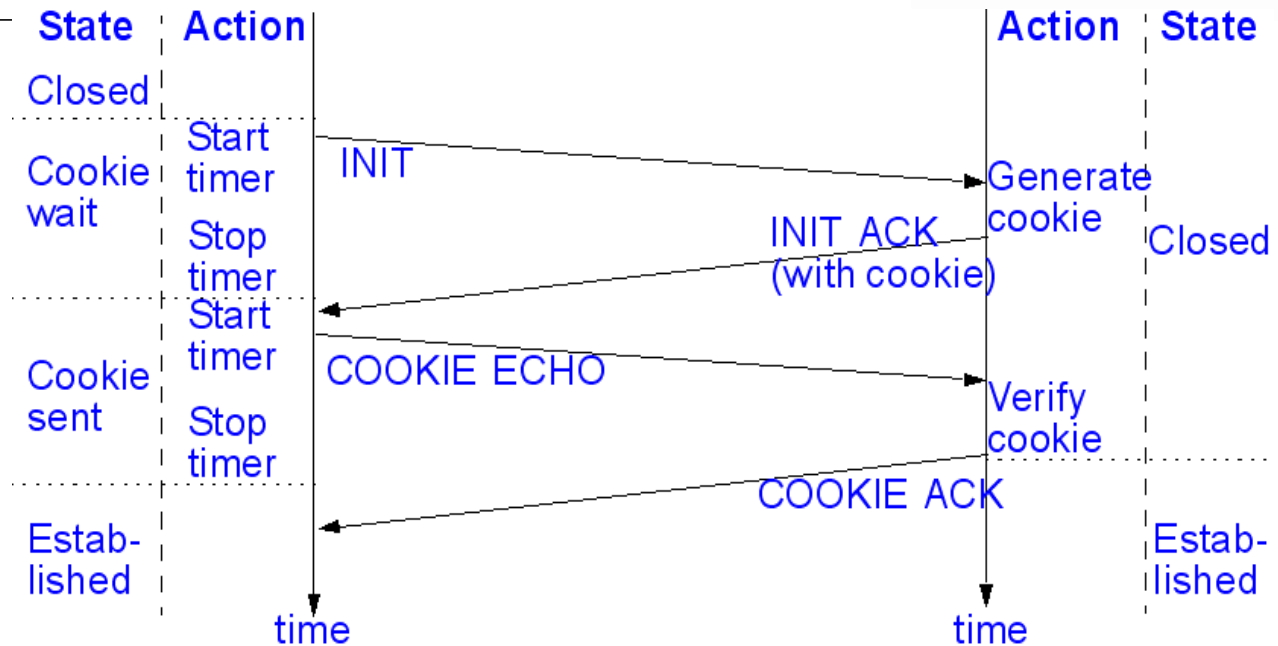
- Coexistence with TCP

Security means:

- 32-bit checksum (like e.g. Adler-32, CRC-32)
- 4-way handshake using cookies against DoS attacks

2.4 SCTP: 4-way Handshake

Association Set-up:



No state information kept at the station receiving the 'INIT' message

- no vulnerability for SYN flooding
- state information established only after the third step,
 - the 'COOKIE' message

To increase efficiency

- user data can be sent already with the 'COOKIE ECHO' and 'COOKIE ACK' messages

Association Teardown

- Additional feature of SCTP disconnect
 - No half-open states as in TCP
 - Due to asymmetric disconnect

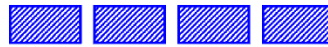
3 SCTP – Packet Format and Chunks

Terminology:

Endpoint

- Logical sender/receiver

Stream A:



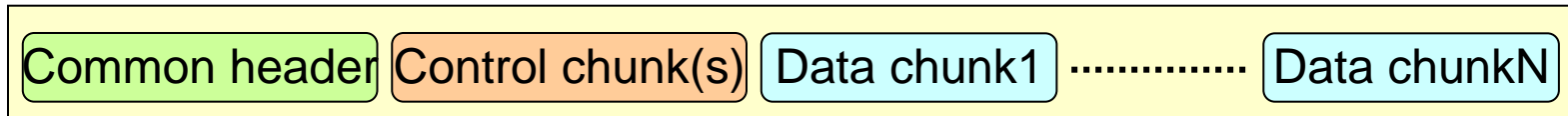
Stream B:



Stream C:



Association



Association

- SCTP connection between two endpoints

Stream

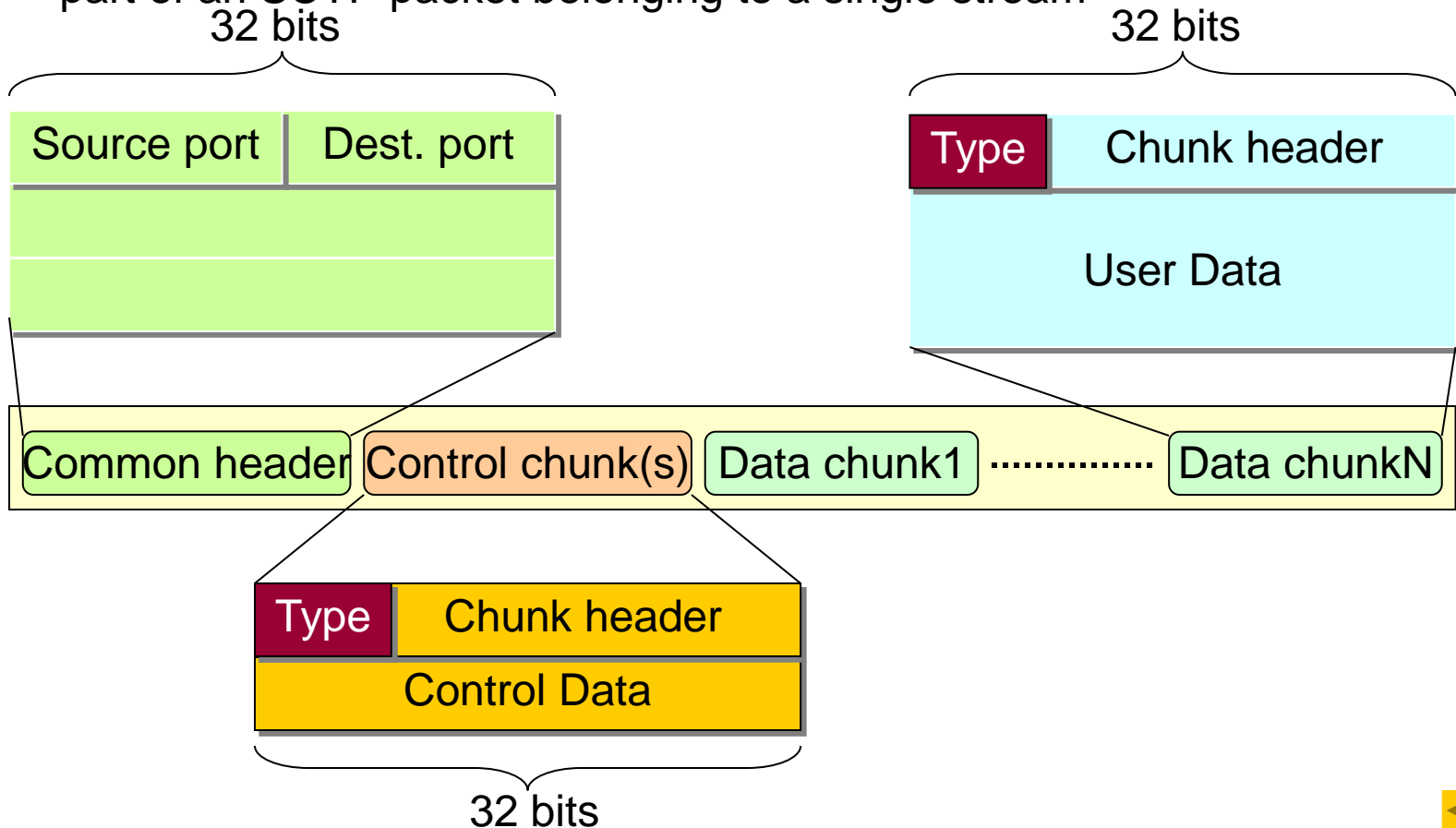
- Unidirectional logical channel

Chunk

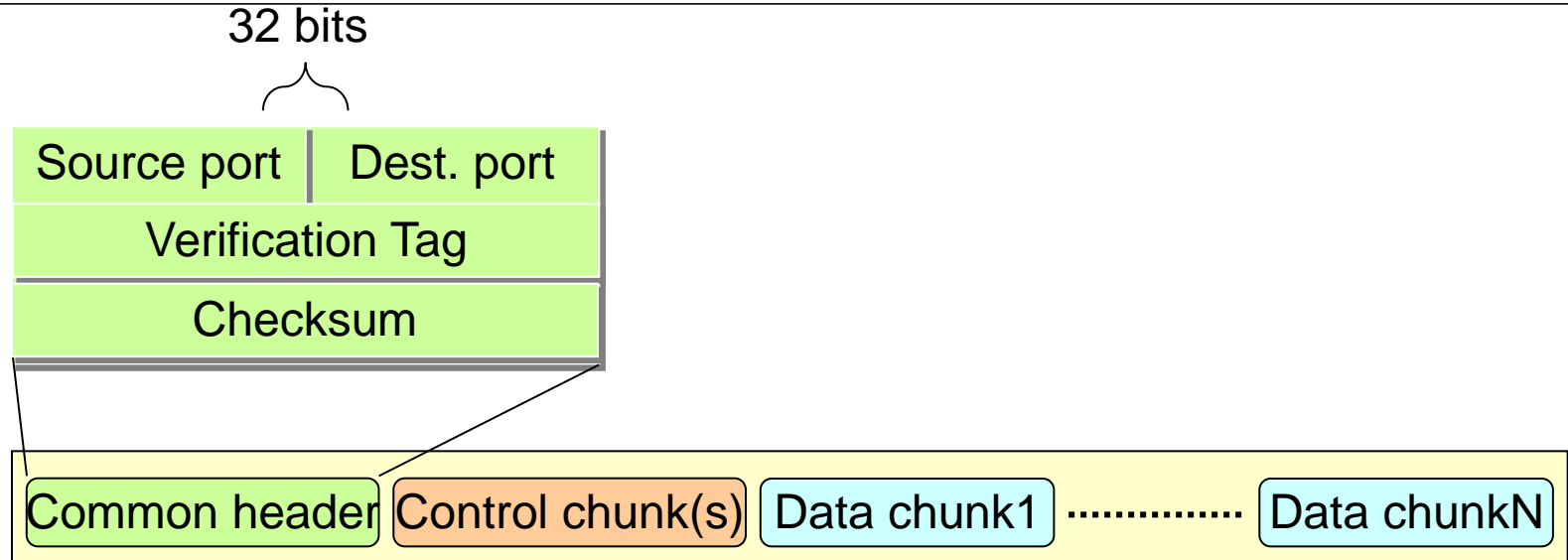
- Unit of information within an SCTP packet,
- consisting of
 - a chunk header and
 - specific content

Multiplexing of several user messages: Chunk Bundling

- Chunk:
 - part of an SCTP packet belonging to a single stream



SCTP – Packet Format: Common Header



source port / destination port (2 Byte each):

- As in TCP or UDP

verification tag: for validation of the sender of the SCTP message

- protection against blind attacks (unauthorized shutdown of association)

checksum:

- Adler-32: currently proposed in the RFC
- CRC-32: proposed recently, better error detection properties for small packets
- RFC 3309: Stream Control Transmission Protocol (SCTP) Checksum Change

SCTP - Packet Format: INIT Chunk Format

Type=1	Flags: None	Chunk Length
Initiate Tag		
Advertised Receiver Credit Window		
Number of outbound streams	Number of inbound streams	
Initial Transmission Sequence Number		
Optional/Variable-Length Parameters		

Initiate Tag: random number used in all subsequent messages

- protect against blind attacks

Advertised Receiver Credit Window:

- dedicated buffer space reserved for the association

Number of outbound streams:

- the sender of this INIT chunk wants to open

Number of inbound streams:

- maximum the sender of this INIT message can support

Variable-Length parameter

- among others.: list of IP addresses (multi-homing!) being part of the association

4 SCTP – Comparison to other Transport Protocols



Table I. Comparison of Transport-Layer Protocols

FEATURE	SCTP	TCP	UDP
Connection-oriented	Yes	Yes	No
Half-closed connections	No	Yes	N/A
Protection against blind DoS attacks	Yes	No	N/A
Dynamic address manipulation	Optional ^a	No	N/A
Reliable data transfer	Yes	Yes	No
Partially reliable data transfer	Optional ^b	No	No
Preservation of application message boundaries	Yes	No	Yes
Application PDU fragmentation/bundling	Yes	Yes	No
Ordered data delivery	Yes ^c	Yes	No
Unordered data delivery	Yes	No	Yes
Full-duplex data transmission	Yes	Yes	Yes
Flow and congestion control	Yes	Yes	No
Selective acknowledgments	Yes	Optional	No
Path max. transmission unit discovery	Yes	Yes	No
Explicit congestion notification support	Yes	Yes	No
Multistreaming	Yes	No	No
Multihoming	Yes	No	No

^aCovered with DAR extension, see RFC 5061 [Stewart et al. 2007].

^bCovered with PR-SCTP extension, see RFC 3758 [Stewart et al. 2004].

^cThe data within a stream is delivered in order.

from
ACM Computing Survey Aug. 2012

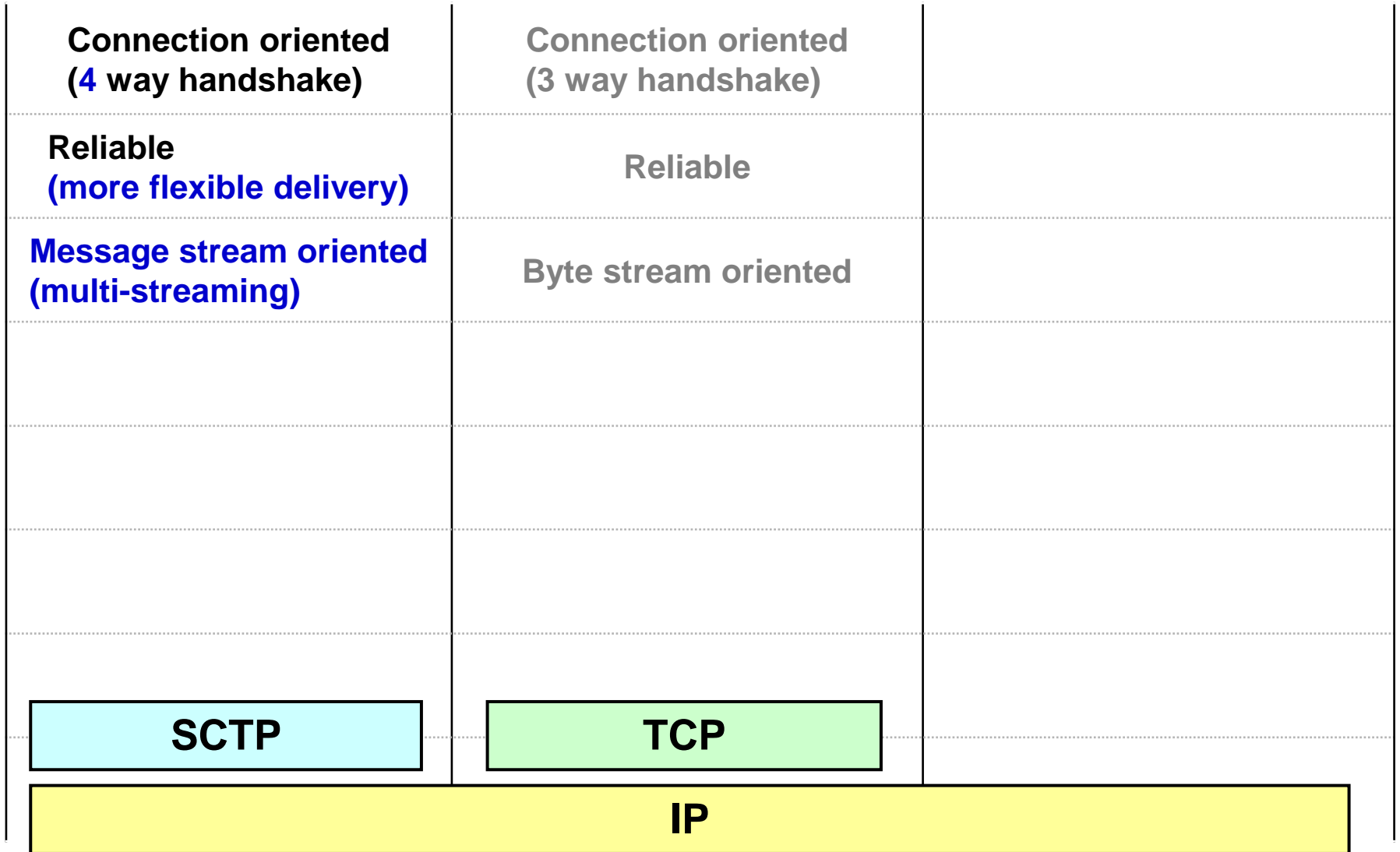
- A Taxonomy and Survey of SCTP Research
 - LUKASZ BUDZISZ, Technische Universität Berlin
 - JOHAN GARCIA and ANNA BRUNSTROM, Karlstad University
 - RAMON FERRUS, Universitat Politècnica de Catalunya

SCTP – Comparison to other Transport Protocols




Connection oriented (4 way handshake)	Connection oriented (3 way handshake)	Connectionless
Reliable (more flexible delivery)	Reliable	Unreliable
Message stream oriented (multi-streaming)	Byte stream oriented	Message oriented
Adaptive flow control	Adaptive flow control	
Multi-homing		
Overhead : 28 bytes (data)	Overhead: 20-32 bytes	Overhead: 8 bytes
Extensible		
SCTP	TCP	UDP
IP		

Example of TCP vs. SCTP




5 SCTP – Main Features and Extensions

Multi-Streaming

- Multiplexing of several independent application flows
 - within one SCTP association via multiple streams
- Avoids head of line blocking 

Multi-Homing


- SCTP endpoints support multiple IP addresses
 - to create redundant network paths between SCTP endpoints
- Compensates network failures 

Flexible delivery

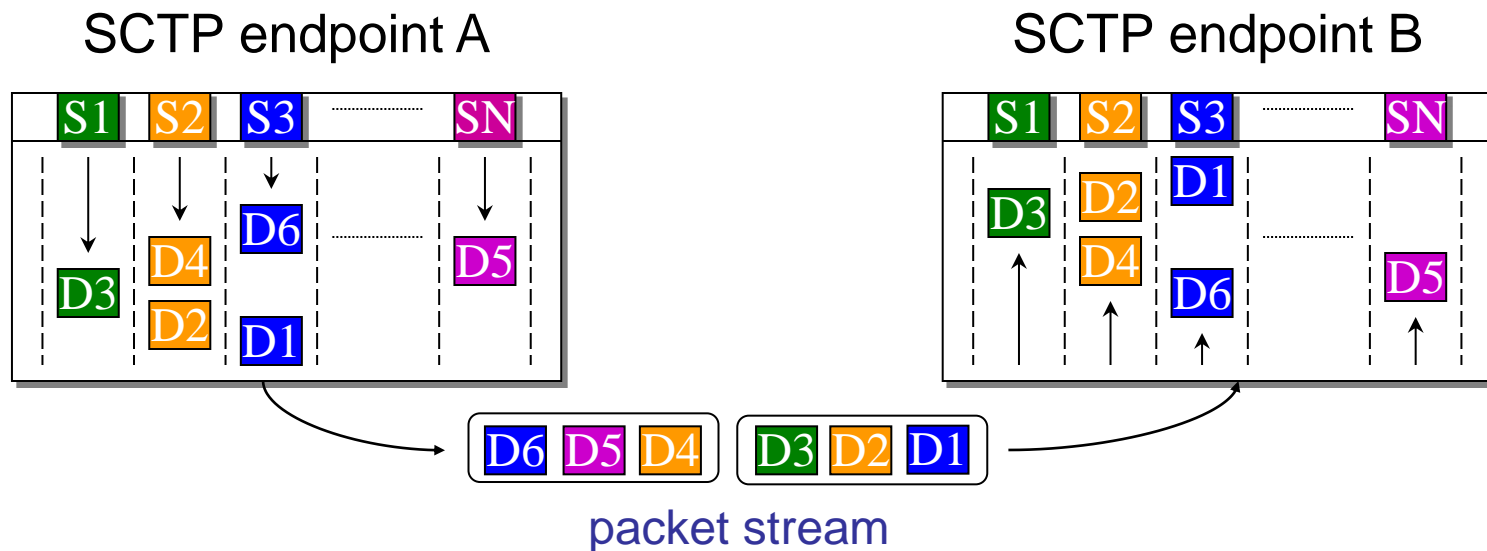
- SCTP provides ordered delivery and unordered delivery 

TCP-friendly adaptive flow control

SCTP protocol extensions

- Partial reliability extension (<http://tools.ietf.org/html/draft-ietf-tsvwg-prsctp-03>)
 - Retransmission can be limited for some transported messages
- Dynamic address reconfiguration (<http://tools.ietf.org/html/draft-ietf-tsvwg-addip-sctp-08>)
 - Add and drop IP addresses of established associations dynamically 

Multiplexing of multiple message streams within one association



S1, S2, S3, . . . , SN – SCTP streams

D1 – D6 – SCTP data chunks

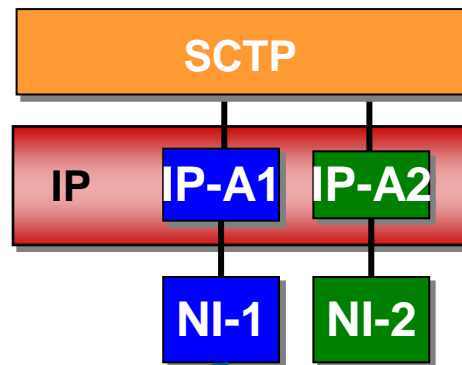


SCTP main Features – Multi-Homing

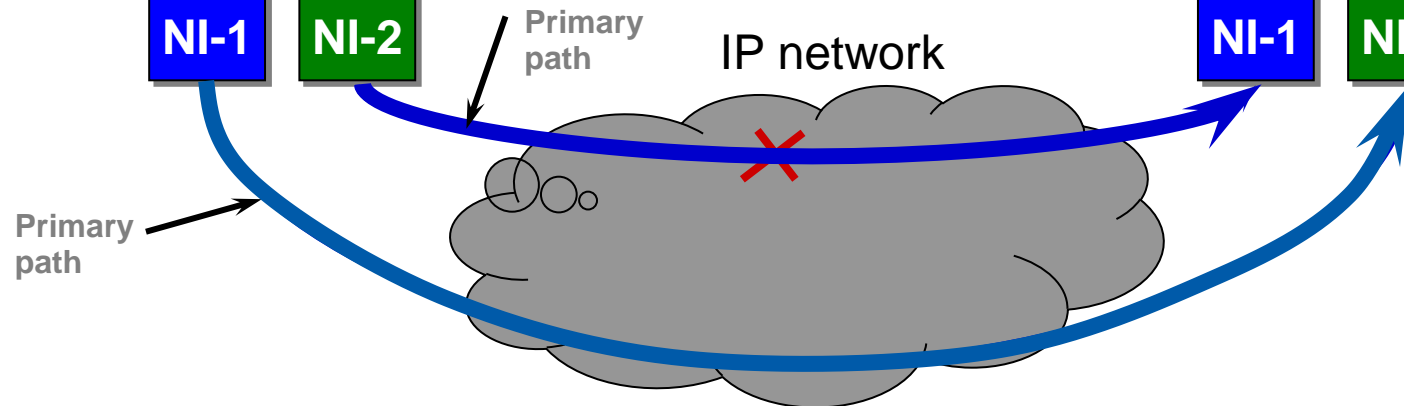
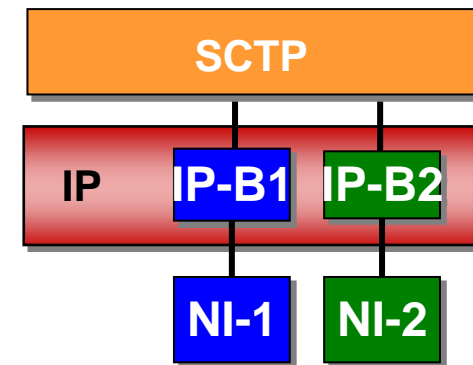
Multi-Homing

- SCTP endpoints support multiple IP addresses
 - to create redundant network paths between SCTP endpoints
- Compensates network failures

SCTP Endpoint A



SCTP Endpoint B



Only primary path carries data traffic,
other paths used for retransmissions only

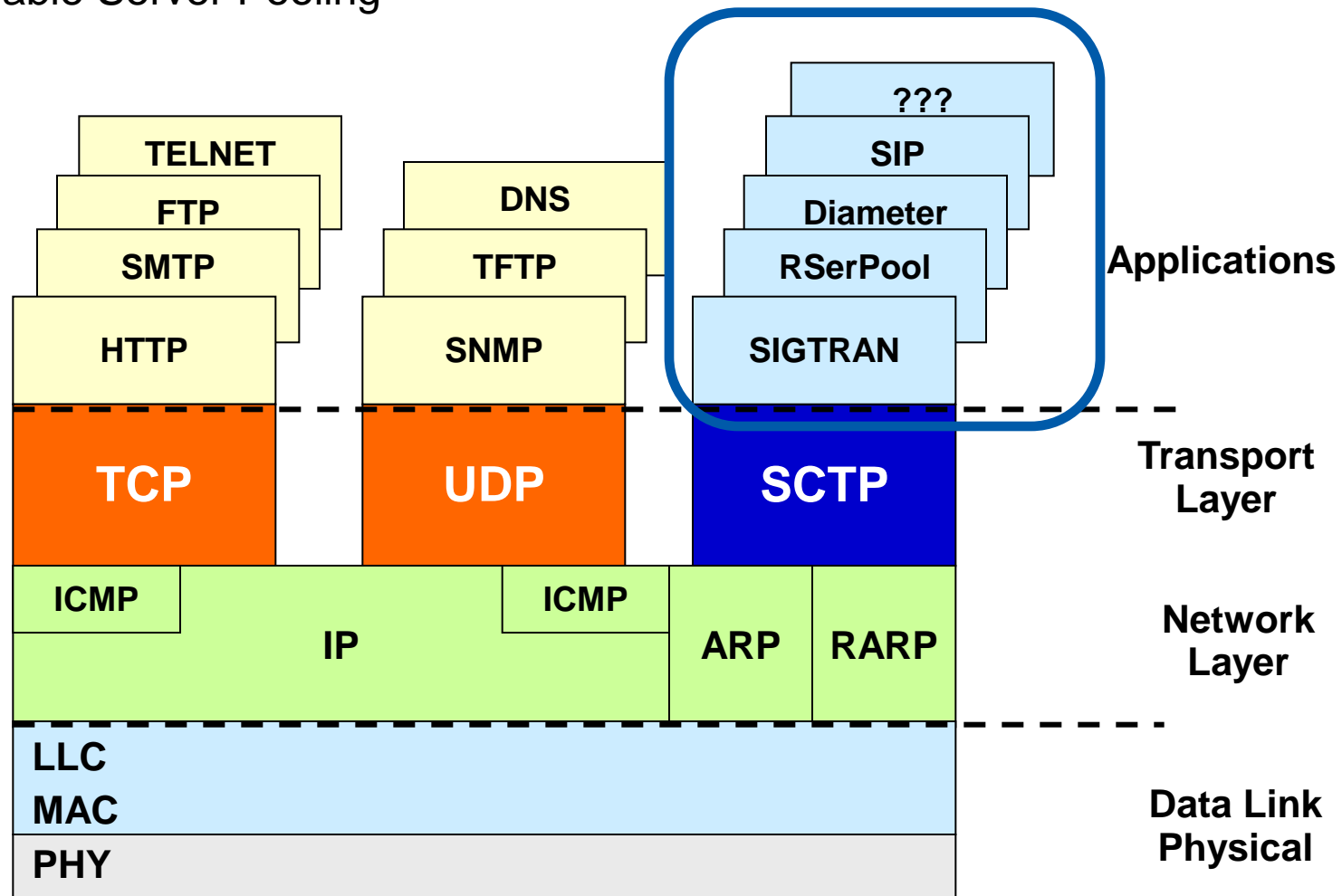
Inactive paths are monitored by heartbeats

NI – Network interface

6 Main SCTP Application Scenarios



- IP-based transport of signaling information
- Reliable Server Pooling



Reliable Server Pooling (RSerPool)

Primary Motivation: Signaling Transport (SS7)

- Strict availability requirements
- Availability by component redundancy
- Usage of inexpensive standard IP-based (SCTP) components
- Software layer for redundancy

Reliable Server Pooling (by IETF RSerPool WG)

- Lightweight (also usable for small embedded devices)
- Real-time (time constraints)
- Scalable (up to large company networks, not the global Internet)
- Extendable (e.g. new server selection policies)
- Simple (automatic configuration)

Additional Application Scenarios for RSerPool:

- GRID Computing / Distributed Computing
- Mobility Management
- Load Balancing (e.g. web servers; applications actively discussed at 60th IETF)

SCTP is a promising multi-purpose IETF transport protocol

- Incorporated already in SIGTRAN, RSerPool and Diameter protocols
- Other potential applications have been identified (SIP, mobility, ...)
- It can be deployed easily because it is TCP friendly

Multi-homing feature of SCTP is highly beneficial

- To cope with network failures (fast failover)
- To improve data throughput in critical scenarios

Standard security protocols (IPSec, TLS) can be used with SCTP

- Some limitations and potential performance issues
- Secure-SCTP extension avoids these drawbacks
 - Not standardized