SCTP

Dr. G. Omprakash

Assistant Professor, ECE, KLEF

Stream Control Transmission Protocol (SCTP)

SCTP is designed to combine some features of UDP and TCP in an effort to create a better protocol for multimedia communication

SCTP Services

- **Process-to-Process Communication**
  - SCTP provides process-to-process communication using port numbers.
- **Multiple Streams**
  - TCP client and a TCP server involves one single stream.
    - Problem: Loss at any point in the stream blocks the delivery of the rest of the data.
  - SCTP allows multistream service
  - If one of the streams is blocked, the other streams can still deliver their data.
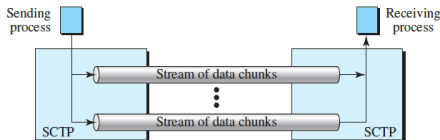

Figure: Multiple-stream concept

- **Reliable Service**: SCTP uses an acknowledgment mechanism to check the safe and sound arrival of data

SCTP Services

- **Multihoming**:
    - TCP connection involves one source and one destination IP address (data from either WiFi or Ethernet)
    - SCTP supports multihoming service. (data from WiFi and Ethernet)
        - sending and receiving host can define multiple IP addresses in each end for an association.
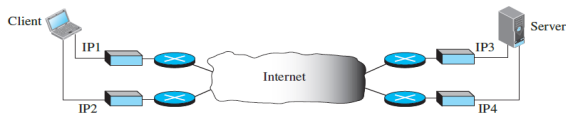   - Also called *inverse multiplexing*

Figure: Multihoming concept

- **Full-Duplex Communication**
    - Like TCP, SCTP offers full-duplex service, where data can flow in both directions at the same time.
- **Connection-Oriented Service**: In SCTP, a connection is called an **association**.

SCTP Features

- **Transmission Sequence Number (TSN)**
  - Data transfer in SCTP is controlled by numbering the data chunks
  - SCTP uses a *transmission sequence number* to number the data chunks
  - TSN in SCTP plays the analogous role as the sequence number in TCP.
  - TSNs are 32 bits long: Randomly initialized between 0 and $2^{32} - 1$.

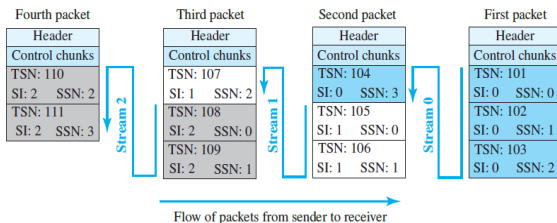- **Stream Identifier (SI)**:
  - There may be several streams in each association
  - Each stream is identified using a **stream identifier**.
  - SI is a 16-bit number starting from 0
  - Each data chunk must carry the SI in its header

- **Stream Sequence Number (SSN)**
  - SCTP defines each data chunk in each stream with a stream sequence number.
  - When a data chunk arrives at the destination SCTP, it is delivered to the appropriate stream and in the proper order

SCTP Example

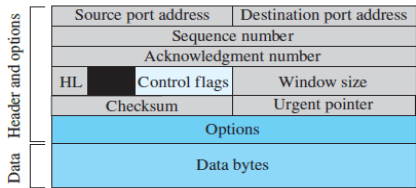Flow of packets from sender to receiver

- Process A needs to send 11 messages to process B in three streams
  - Assume that each message fits into one data chunk
- 1,2,3,4 $\implies$ First stream; 5,6,7 $\implies$ Second stream; 8,9,10,11 $\implies$ Third stream
- Each data chunk needs three identifiers
  - TSN: Transmission Sequence number: Cumulative number used for error and flow control
  - SI: Stream Identifier: Defines the stream to which the chunk belongs
  - SSN: Stream Sequence Number: Defines the chunk's order in a particular stream
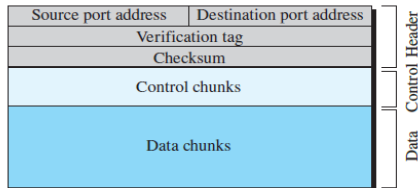
TCP vs SCTP

TCP	SCTP
It is low in usage	It is mostly used
Sequence number is used to number the data bytes.	**Transmission sequence number** is used to number the data chunks
Each connection between a TCP client and a TCP server involves **single stream service**	SCTP allows **multistream service** in each connection
Data are carried as a collection of bytes	Data are carried as data chunks
Control information: Defined by six control flags in the header	Control information is carried as control chunks
A TCP connection involves one source and one destination IP address	In SCTP, sending and receiving host can define multiple IP addresses in each end for an association **(multihoming)**

A segment in TCP   A packet in SCTP

SCTP Packets

- Data are carried as data chunks
- Control information is carried as control chunks
- Several control chunks and data chunks can be packed together in a packet
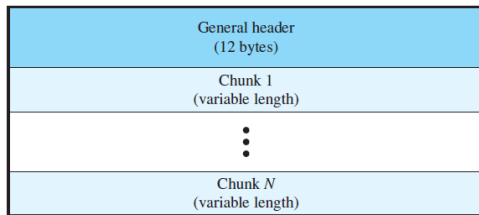- A packet in SCTP plays the same role as a segment in TCP.

Figure: SCTP Packet Format

SCTP General Header

Source port address 16 bits	Destination port address 16 bits
Verification tag 32 bits	
Checksum 32 bits	

- Defines the endpoints of each association to which the packet belongs
- **Source port number** : 16-bit field that defines the port number of the application program in the host that is sending the packet
- **Destination port number**: 16-bit field that defines the port number of the application program in the host that is receiving the packet.
- **Verification tag** is a 32-bit field that matches a packet to an association.
  - This prevents a packet from a previous association from being mistaken as a packet in this association (Resolves duplicate problem)
- Size of the checksum is increased from 16 bits (in UDP, TCP, and IP) to 32 bits in SCTP to allow for the use of the CRC-32 checksum

Acknowledge various sources for the images.
Thankyou