# 14 билет. Транспортный протокол SCTP

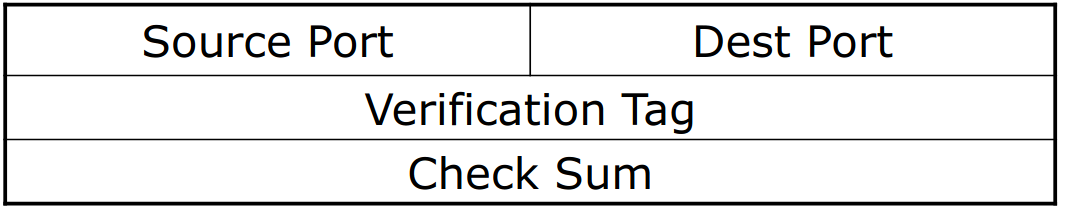
SCTP – Stream Control Transmission Protocol (протокол передачи с управлением потоком). Относительно новый транспортный протокол.  
Первым его стандартом был RFC2960, 2002г.  
Нынешний стандарт RFC4960, сентябрь 2007г.

Основная идея создания протокола была объеденить в себе достоинства и исправить недостатки двух других известных транспортных протоколов (TCP и UDP).

Одними из главных нововведений SCTP были многопоточность, защита от DdoS атак и multi-homing(синхронное соединение между двумя хостами по двум и более независимым физическим каналам) (дополнительно после формата пакетов).

Целый пакет состоит из общего заголовка(12 байт=64 бита) и субпакетов (чанков). Каждый чанк же в свою очередь состоит из своего заголовка и данных.

### Формат общего заголовка:

Где:

- Verification tag – метка для проверки  
отправителя пакета (32-битное случайное значение, созданное во время инициализации, чтобы отличать устаревшие пакеты от предыдущего соединения)  
- Check Sum – контрольная сумма

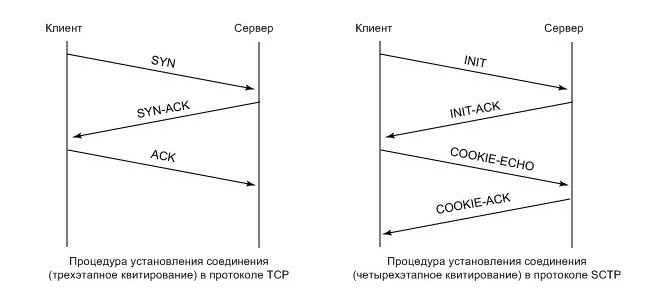
### Формат чанков:

Под тип выделен один байт,значит возможно 255 различных типов. На данный момент в RFC определены 15 типов. 0 означает, что чанк несет полезные данные, остальные — служебные.

Под флаги тоже 8 бит, состав флагов определяется типом чанка.

Длинна чанка — 0..65535, общая длина субпакета с заголовками.

### Безопасное установление соединения:

В TCP трехэтапный хэндшейк, в чем есть одна потенциальная уязвимость, обусловленная тем, что нарушитель, устанавливая фальшивые IP-адреса отправителя, может послать серверу множество пакетов SYN. При получении пакета SYN сервер выделяет часть своих ресурсов для установления нового соединения. Обработка множества пакетов SYN рано или поздно затребует все ресурсы сервера и сделает невозможной обработку новых запросов. Такой вид атак называется «SYN-флуд».

Протокол SCTP защищён от подобных атак с помощью механизма четырёхэтапного квитирования (four-way handshake) и вводом маркера (cookie). По протоколу SCTP клиент начинает процедуру установления соединения, посылая пакет INIT. В ответ сервер посылает пакет INIT-ACK, который содержит маркер (уникальный ключ, идентифицирующий новое соединение). Затем клиент отвечает посылкой пакета COOKIE-ECHO, в котором содержится маркер, полученный от сервера. Только после этого сервер выделяет свои ресурсы новому подключению и подтверждает это отправкой клиенту пакета COOKIE-ACK.

### Многопоточность

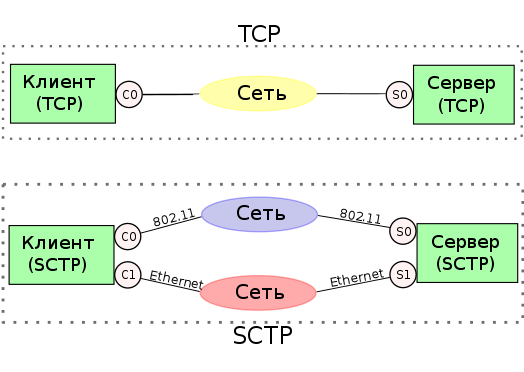


Термин «многопоточность» (англ. *multi-streaming*) обозначает способность SCTP параллельно передавать по нескольким независимым потокам *сообщений*. Например, мы передаём несколько фотографий через HTTP-приложение (например, браузер). Можно использовать для этого связку из нескольких TCP-соединений, однако также допустима *SCTP-ассоциация* (англ. *SCTP-association*), управляющая несколькими потоками сообщений для этой цели. Потоки являются однонаправленными, то есть передают информацию только в одном направлении (картинка выше является неточной).

TCP достигает правильного порядка байт в потоке, абстрактно назначая порядковый номер каждой отосланной единице, а упорядочивая принятые байты, используя назначенные порядковые номера, по мере их прибывания. С другой стороны, SCTP присваивает различные порядковые номера сообщениям, посылаемым в конкретном *потоке*. Это разрешает независимое упорядочивание сообщений по разным потокам. Так или иначе, многопоточность является опцией в SCTP. В зависимости от желаний пользовательского приложения, сообщения могут быть обработаны не в порядке их отправления, а в порядке их поступления.

## Другие достоинства SCTP:

**Multihoming** (Использование множественных интерфейсов, мультидомность по Ицыксоновски) - Допустим, у нас есть два хоста. И хотя бы один из них имеет несколько сетевых интерфейсов, и соответственно несколько IP-адресов. В TCP, понятие «соединение» означает обмен данными между двумя точками, в то время, как в SCTP имеет место концепция «ассоциации» (англ. *association*), обозначащая всё происходящее между двумя хостами

**Механизмы валидации и проверки подлинности -** Защита адресата от flood-атак (технология 4-way handshake), и уведомление о потерянных пакетах и нарушенных цепочках.

## Из недостатков

Бóльшая занимаемая полоса, то есть относительный объём служебного трафика больше, чем при использовании TCP/UDP.

