



# Introdução ao Protocolo de Controle de Fluxo de Transmissão (SCTP), A próxima geração do Protocolo de Controle de Transmissão (TCP)

**Introdução** Nós passamos por varreduras de segurança no aeroporto e então partimos em uma rápida caravana de veículos. Chegando ao mundo semi-secreto dos grupos de trabalho da Internet Engineering Task Force (IETF), atravessamos a porta de vidro que marcava o ponto de onde não haveria mais volta. Entramos em um labirinto de corredores e, por fim, chegamos a uma porta comum. Por trás dela, entre os ternos azul-marinho, existe o Stream Control Transmission Protocol (SCTP). Organizamo-nos para ter uma visão melhor e podemos observar o AIX da IBM, três variantes diferentes do BSD, o Cisco IOS, Linux, o sistema operacional da Microsoft e o Sun Solaris. Cada um implementou sua interpretação deste protocolo padronizado. Nós contemplamos o que pode ser o Santo Graal das telecomunicações e multimídia IP. Passando por entre os cubículos, entramos por uma porta com uma indicação curiosa: "Área de testes/Laboratório".

Nos limites do laboratório, os distintivos nos trajes de sala limpa indicam que o SCTP é resultado dos esforços dos grupos de trabalho de Signaling Transport (SigTran) da IETF. Seu objetivo é produzir algo similar à rede de comutação telefônica com Signaling System 7 (SS7), capaz de transmitir por redes IP. Simplificando, o SCTP foi criado para transportar sinais de controle de chamadas usando redes IP. O SCTP não é novo; ele foi criado em 2000 e está demorando algum tempo para crescer além de seu confinamento nas interconexões das grandes companhias de telecomunicações.

Discretamente, somos informados de que o sigilo foi criado para prevenir uma corrida em massa para a implementação SCTP quando todos descobrirem as capacidades do protocolo. Com mais de vinte anos de experiência no currículo, o Transmission Control Protocol (TCP) e o User Datagram Protocol (UDP) não estavam, individualmente, à altura da tarefa, mas cada um forneceu peças e idéias para tornar o SCTP possível. Nem o TCP nem o UDP podem trabalhar em multi-homing e eles não têm a capacidade de enviar informações para um endereço alternativo, se o principal não puder ser alcançado. O TCP, concorrente mais próximo do SCTP, terá de ser melhorado ou se tornará uma relíquia.

Segundo as especificações do IP Multimedia System (IMS), o SCTP oferece conexões entre vários servidores do Session Initiated Protocol (SIP) e servidores proxy, um cenário coletivamente chamado de Call Session Control Function (CSCF). O sigilo parece ser em torno do fato que as comunicações que transitam entre ou através do Proxy-CSCF e outras partes da infra-estrutura IMS serem gerenciadas no plano de controle em vez de no plano de dados. (O plano de dados contém os dados de telecomunicações sendo realmente enviados para um assinante/usuário, e o plano de controle oferece o controle e a conectividade para o plano de dados). Como o SCTP fica oculto por trás das cortinas das redes de plano de controle, não recebeu a mesma publicidade ou atenção dedicadas às outras especificações IMS. O SIP e o RTSP saíram de trás da cortina, com a capacidade de processar telecomunicações de Voz sobre IP (VoIP) no espaço corporativo. Porém, a notoriedade do SIP e do RTSP pode ter vida curta quando o SCTP estreiar no espaço corporativo.

E esse é o ponto crucial: Sem as capacidades do SCTP, o IMS não poderá transmitir a sinalização de controle de chamada de forma confiável para os vários sistemas, e



não será possível usar o TCP ou UDP. Você poderia usá-los, se permitir apenas vinte sessões simultâneas, o que é irrelevante, pois a maioria dos provedores de serviços têm milhões de assinantes. Um exame das especificações do SCTP revela muitas funções ou serviços similares aos do TCP.

### Serviços e funções do SCTP

Observando a Tabela 1, você pode facilmente identificar as vantagens do SCTP em relação ao TCP ou UDP. (Veja o *Apêndice 1* para uma explicação das funções/serviços.) É essa a próxima geração do TCP? Poderia ser, pois o SCTP é poderoso e, quando implementado, pode oferecer inúmeros benefícios às comunicações orientadas a conexões.

Função/Serviço	SCTP	TCP	UDP
Permite conexões half-closed	Não	Sim	N/A
Agrupamento de PDU por aplicativo	Sim	Sim	Não
Fragmentação de PDU por aplicativo	Sim	Sim	Não
Controle de congestionamento	Sim	Sim	Não
Orientado à conexão	Sim	Sim	Não
Capaz de usar ECN	Sim	Sim	Não
Controle de fluxo	Sim	Sim	Não
Full duplex	Sim	Sim	Sim
Multi-homing	Sim	Não	Não
Multistreaming	Sim	Não	Não
Distribuição ordenada de dados	Sim	Sim	Não
Transferência parcial confiável de dados	Opcional	Não	Não
Descoberta do MTU do caminho	Sim	Sim	Não
Preserva limites da mensagem	Sim	Não	Sim
Protege contra ataques de inundação SYN	Sim	Não	N/A
Pseudocabeçalho para o checksum	Usa vtags	Sim	Sim
Verificação de acessibilidade	Sim	Sim	Não
Transferência confiável de dados	Sim	Sim	Não
Acks seletivos	Sim	Opcional	Não
Estado de tempo de espera	para vtags	para 4-tuple	N/A
Distribuição de dados não-ordenada	Sim	Não	Sim

(N/A = não aplicável)

*Tabela 1: Comparação entre SCTP, TCP e UDP*

### Benefícios principais do SCTP

O SCTP amplia as capacidades do TCP e do UDP, integrando componentes de ambos. Mas os criadores do SCTP não pararam por aí. Eles adicionaram dois novos conceitos: multi-homing e multistreaming.



**Multi-homing**

O SCTP foi criado para gerenciar a sinalização de telecomunicações sobre IP. Como as telecomunicações são muito suscetíveis a atrasos, cada milissegundo conta. O Multi-homing permite que os sistemas que possuem múltiplas interfaces para redundância usem uma interface em lugar de outra, sem ter de esperar. No SCTP, uma interface é estabelecida como primária e as outras se tornam secundárias. Se a primária falhar por qualquer motivo, uma secundária é escolhida e utilizada. Quando a interface primária estiver disponível novamente, as comunicações podem ser transferidas de volta sem que o aplicativo sequer saiba que houve um problema. Ao estabelecer as conexões, as interfaces primária e secundária são verificadas e modificadas usando um processo de reconhecimento de heartbeats que valida os endereços e mantém um cálculo de tempo de ida e volta (round trip time - RTT) para cada endereço. O RTT pode mostrar que a interface primária está mais lenta do que a secundária, permitindo que as comunicações migrem da primeira para a segunda.

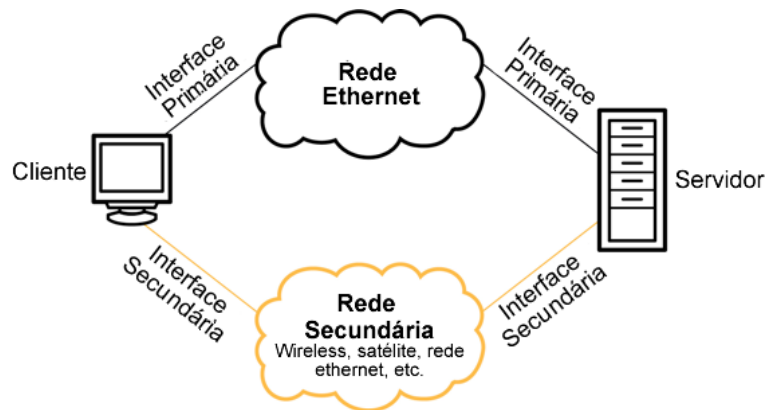


Figura 2: Multi-homing

**Multistreaming**

Usando o TCP, somente um fluxo de dados é permitido por conexão. A informação completa deve ser passada por meio daquele fluxo. O SCTP permite múltiplos fluxos simultâneos de dados em uma conexão ou associação. Cada mensagem enviada para um fluxo de dados pode ter um destino final diferente, mas todas precisam manter os limites das mensagens. Por exemplo, os sistemas não podem mandar partes da mesma mensagem por fluxos diferentes - uma mensagem deve ser enviada pelo mesmo fluxo. Ao executar um sistema de distribuição ordenada de dados, se um dos pacotes estiver avariado ou faltando, o fluxo é bloqueado até a resolução da ordem. É o processo conhecido como "Bloqueio Head-of-Line". Com o uso de fluxos múltiplos, somente o fluxo afetado seria bloqueado; os outros fluxos continuarão funcionando normalmente.

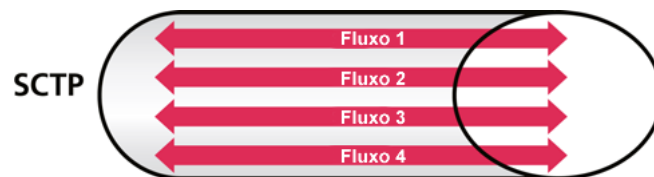


Figura 3: Multistreaming

Usando o multistreaming com SCTP, desaparece o problema com os navegadores web que só podem gerenciar duas conexões simultâneas. O cliente ou servidor web poderia abrir imediatamente fluxos adicionais e enviar imagens, texto, etc. por cada fluxo, reduzindo a latência geral. Isso também poderia reduzir o over-head que



normalmente afeta os servidores com várias conexões separadas, necessárias para atender a um pedido.

O multistreaming do SCTP também pode ajudar em infra-estruturas que conectam múltiplos meios de comunicação simultaneamente. Por exemplo, se analisarmos a figura 3 acima, o Fluxo 1 pode ser comunicação de voz, o Fluxo 2 poderia ser vídeo, o Fluxo 3, um aplicativo compartilhado e assim por diante. Ao possibilitar que o SCTP atenda às demandas do futuro, o grupo de trabalho SIGTRAN simplificou a conectividade para desenvolvedores. Eles só precisarão acessar os fluxos adequados para fornecer as informações aos aplicativos.

**Benefícios adicionais do SCTP em comparação ao TCP**

**Permite conexões half-closed**

As conexões half-closed podem ocorrer quando um lado da comunicação acredita que a conexão foi fechada e o outro pensa que ela ainda está aberta. O TCP usa um comando de encerramento de quatro etapas que consiste de mensagens FIN e FIN-ACK bidirecionais. A conexão half-open pode existir se as mensagens vermelhas não são enviadas (veja a figura abaixo). O SCTP remove essa possibilidade implementando um encerramento de três etapas que consiste de SHUTDOWN, SHUTDOWN-ACK e SHUTDOWN-COMPLETION. Quando esse processo é iniciado, ambos os lados encerram imediatamente a comunicação. Caso seja necessário o envio de mais informações, uma nova conexão terá de ser feita.



**Preservação dos limites das mensagens**

Se um cliente envia uma mensagem com 100 bytes e outra com 50, a informação é oferecida ao servidor com os limites de mensagem preservados. Com SCTP e UDP, as mensagens são enviadas como 100 bytes e 50 bytes. Com o TCP, as mensagens podem ser enviadas/recebidas como uma mensagem de 150 bytes. No exemplo abaixo, as mensagens foram recebidas como uma única mensagem. Isso força o aplicativo a separar as mensagens novamente em seu formato original. Com SCTP e UDP, os limites das mensagens são mantidos e o aplicativo não tem de dividi-las.



**Protege contra ataques de inundação SYN**

Para entendermos como funcionam os ataques de inundação SYN, temos de olhar como uma conexão normal é estabelecida. Com o TCP, o cliente inicia a comunicação com um pedido de sincronização - o pacote SYN. O servidor responde confirmando com um pacote SYN-ACK e, por fim, o cliente verifica a confirmação com um pacote ACK. Isso é conhecido como o "handshake de três etapas". Quando

todos os três passos forem completados, as comunicações podem começar. Em contraste, o SCTP usa um handshake de quatro passos, mas pode começar a enviar informações no terceiro passo. Então, o cliente SCTP inicia a comunicação com um pacote INIT. O servidor confirma com um pacote INIT-ACK e um cookie (um contexto único que identifica a conexão). O cliente então manda o cookie de volta para o servidor; o cliente também pode enviar informações adicionais após o COOKIE-ECHO. O servidor então confirma o recebimento do COOKIE-ECHO com um COOKIE-ACK.



Um ataque de inundação SYN ocorre quando um ou vários clientes enviam pacotes SYN para um servidor. Isso faz que o alvo comprometa seus recursos e, eventualmente, sobrecarregará o servidor, fazendo que ele reinicie ou algo pior. Com o TCP, o servidor alocou recursos para a conexão. Em uma conexão TCP, ambos os terminais devem dedicar portas, memória e ciclos de processamento para cada nova conexão. Para fins de atribuição de recursos, as conexões TCP começam com o recebimento de pacotes SYN. Como o UDP é um protocolo não orientado à conexão, isso não se aplica a ele. Usando o SCTP, os servidores não alocam recursos para a conexão até que o COOKIE-ECHO seja recebido. Isso significa que o cliente SCTP deve alocar os recursos inicialmente para poder enviar informações.



### Acks seletivos

No TCP padrão, cada mensagem ou pacote de informação deve ser considerado, reenviado se necessário, e processado na ordem em que foi enviado. O SCTP tem a capacidade de confirmar seletivamente a recepção ou não de mensagens duplicadas, perdidas ou fora de ordem. Em função da natureza das telecomunicações, a maioria dos aplicativos acabaria por descartar qualquer mensagem não-sincronizada. Portanto, a necessidade do envio e recebimento da informação é abandonada. Isso significaria que parte de uma palavra, vídeo ou imagem seria "pulada". Os aplicativos e usuários podem perceber leves saltos na transmissão de voz, vídeo ou imagens. No mundo das telecomunicações, nos referimos a esse fenômeno como "jitter", e uma pequena quantidade dele pode ser preferível a ter os pacotes reenviados e reprocessados, o que acabaria por aumentar o jitter, tornando-o mais perceptível aos usuários.

### Distribuição de dados não-ordenada

Por conta da natureza das redes, nem todos os pacotes podem trafegar pelo mesmo caminho. Se houver um atraso de tempo no uso de um caminho em relação a outro, a mensagem original poderá estar fora da ordem ao ser recebida. A distribuição de



dados não-ordenada permite isso e pode corrigir o problema simplesmente reordenando as mensagens da forma correta. O uso da função de transferência confiável to TCP exige que os pacotes sejam processados em ordem. Se um pacote for perdido ou estiver fora da ordem, precisará ser reordenado novamente antes que o processamento possa prosseguir. Por exemplo, no diagrama abaixo, se estivéssemos usando o TCP, quando a Mensagem 3 for recebida, todo o processamento será interrompido, enquanto aguardamos a chegada da Mensagem 2, para que ela possa ser processada e só então a Mensagem 3 será, por fim, submetida ao processamento. O SCTP permite a distribuição de dados não-ordenada. Como ele possui múltiplos fluxos, somente aquele afetado é bloqueado temporariamente. No diagrama abaixo, o SCTP processaria as mensagens na ordem de chegada, sem esperar que elas sejam numericamente ordenadas. Com a transferência confiável do SCTP, muitas soluções de discos de rede já oferecem serviços de ordenamento; a capacidade do SCTP de simplesmente transmitir os dados alivia os servidores da carga desnecessária da reorganização.

### **Resumo**

O intuito deste documento é familiarizar o leitor com o conceito e a necessidade do SCTP. Embora, atualmente, ele tenha um uso limitado, suas capacidades são muito atraentes e, em breve, a adoção do SCTP crescerá rapidamente. Na arquitetura IMS, o SCTP fornece a sinalização de chamadas sobre IP. O multi-homing e multistreaming, benefícios principais do SCTP, permitirão o desenvolvimento de inúmeros dispositivos novos que incluirão o suporte a esse novo protocolo.



## Apêndice 1. Definições de funções/serviços

Função/Serviço	Definições
<b>Permite conexões half-closed</b>	As conexões half-closed podem ocorrer quando um lado da comunicação acredita que a conexão foi fechada e o outro pensa que ela ainda está aberta.
<b>Agrupamento de PDU por aplicativo</b>	Os pacotes PDU (Protocol Data Unit) dos aplicativos são agrupados antes da transmissão.
<b>Fragmentação de PDU por aplicativo</b>	Os pacotes PDU (Protocol Data Unit) dos aplicativos são desagrupados após a transmissão.
<b>Controle de congestionamento</b>	O controle de congestionamento significa que a rede é verificada antes da transmissão para ajudar a evitar o congestionamento dos links.
<b>Orientado à conexão</b>	A orientação à conexão é baseada nas duas pontas de uma comunicação, estando ambas conscientes de que estão transmitindo dados.
<b>Capaz de usar ECN</b>	A Notificação Expressa de Congestionamento (Explicit Congestion Notification - ECN) faz notificações de congestionamento ao entrar ou sair de uma conexão.
<b>Controle de fluxo</b>	Capacidade de ajustar a transmissão de dados, especificamente, a quantidade. Veja MTU para mais informações sobre tamanho/volume
<b>Full duplex</b>	A capacidade de enviar e receber simultaneamente.
<b>Multi-homing</b>	Capacidade de ter múltiplos endereços IP e usar qualquer deles (ou todos) simultaneamente, conforme necessário. É como ter um telefone que suporta várias linhas, com o qual você pode atender a diversas chamadas ao mesmo tempo.
<b>Multistreaming</b>	A capacidade de enviar/receber múltiplos fluxos de dados em uma única conexão.
<b>Distribuição ordenada de dados</b>	Isso significa que, quando os pacotes 1, 2 e 3 são enviados, eles precisarão ser processados em ordem, mesmo se o pacote 3 chegar antes do 2.
<b>Transferência parcial confiável de dados</b>	Permite que o usuário especifique, mensagem a mensagem, as regras que definirão o quanto o serviço de transporte deverá ser persistente nas tentativas de enviar a mensagem ao destinatário.
<b>Descoberta do MTU do caminho</b>	Unidade Máxima de Transmissão (Maximum Transmission Unit - MTU). O maior tamanho de pacote que pode ser enviado pelo remetente ao destinatário, sem a necessidade de fragmentação.
<b>Preserva limites da mensagem</b>	Os limites das mensagens são definidos pelo aplicativo. É aqui que o protocolo de transmissão mantém ou não os limites.
<b>Protege contra ataques de inundação SYN</b>	Os ataques de inundação SYN ocorrem quando vários sistemas enviam pedidos para estabelecer conexões, mas nenhuma outra transmissão de dados. Esse é um método de ataque.
<b>Pseudocabeçalho para o checksum</b>	Um cabeçalho adicional contendo um checksum dos dados contidos no pacote. Eles foram adicionados ao TCP e UDP.
<b>Verificação de acessibilidade</b>	Capacidade de confirmar se um dispositivo remoto está funcionando ou não, antes de enviar dados.
<b>Transferência confiável de dados</b>	Garantia de que os dados enviados, em várias partes, foram todos recebidos sem corrupção.
<b>Acks seletivos</b>	Capacidade de notificar o remetente do recebimento de pacotes duplicados, perdidos e fora de ordem.
<b>Estado de tempo de espera</b>	Depois que uma conexão é encerrada, esse é o período de tempo que um sistema esperará antes de reutilizar aquela porta e o endereço IP.
<b>Distribuição de dados não-ordenada</b>	A capacidade de receber pacotes fora da ordem em que foram enviados.

Randall Stewart, Paul D. Amer. "Why is SCTP needed given TCP and UDP are widely available? (Por que o SCTP é necessário quando o TCP e o UDP estão amplamente disponíveis?)" REUNIÃO Nº 17 DOS MEMBROS DO ISOC, Junho de 2004.