Using Session Control Transmission Protocol (SCTP) for VPN Transport

-Joseph Hill-
VPN Concept
Data Encapsulation

- Original IP packet becomes payload
- Adds overhead
Session Control Transmission Protocol (SCTP) Features

- Reliable
- Connection Oriented
- Message Based
  - Independent Ordering
- Multiple Streams
- Optional Ordering
  - Per message
- Multi-Homing

SCTP Common Header

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification Tag</td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td></td>
</tr>
</tbody>
</table>

SCTP Chunk Header

<table>
<thead>
<tr>
<th>Type</th>
<th>Flags</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission Sequence Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stream Identifier</td>
<td>Stream Seq Num</td>
<td></td>
</tr>
<tr>
<td>Payload Protocol Identifier</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12 Bytes
16 Bytes
Data Encapsulation Comparison

- UDP
  - Message Based
  - Unordered
  - Unreliable
Data Encapsulation Comparison

- **TCP**
  - Stream Based
  - Ordered
  - Reliable
Data Encapsulation Comparison

- **SCTP**
  - Message Based (Chunks)
  - Flexible Ordering
  - Reliable
Test Setup

- Tunnels Created Between Virtual Servers in various locations
  - Each Protocol used for each pair
    - SCTP Ordered & Unordered
  - FreeBSD 10.2 Servers
Performance Results

[Bar chart showing Absolute Protocol Performance with data points for Amsterdam & Frankfurt, London & New York, and San Francisco & Singapore for TCP, UDP, SCTP, and SCTP (Unordered).]
Performance Results

![Performance Relative to UDP](image)

- **TCP**
- **UDP**
- **SCTP**
- **SCTP (Unordered)**

Locations:
- Amsterdam & Frankfurt
- London & New York
- San Francisco & Singapore
Problems Encountered

- Not all Implementations created Equal
  - Microsoft Windows
    - No builtin support for SCTP
  - Linux
    - Performance Issues?
  - FreeBSD
    - Driver Issues
    - Problems with IPv4?
Conclusions

● Use UDP
  ○ Except when it doesn’t work
    ■ Not connection oriented

● SCTP viable alternative to TCP
  ○ Except when it doesn’t work
    ■ Connection oriented, but is it supported?
Future Work

- Investigate Linux implementation
- Investigate SCTP support
  - in Firewalls
  - in devices performing NAT
  - in mobile devices
- Potential of SCTP extensions
  - RFC 3758 - Partial Reliability Extension
References

- Mastering OpenVPN by Eric F Crist and Jan Just Keijser
- Quantifying Head-of-Line Blocking in TCP and SCTP by Michael Scharf and Sebastian Kiesel
- RFC 768 - User Datagram Protocol by J. Postel
- RFC 793 - Transmission Control Protocol by J. Postel
- RFC 4960 - Stream Control Transmission Protocol by R. Stewart
- SCTP Performance Tests by Asim Iqbal
- The State of Enterprise Network Traffic in 2012 by David Murray and Terry Koziniec
- Why TCP Over TCP Is A Bad Idea by Olaf Titz