IETF 92 Report
spud (BoF)

2015.4

NTTコミュニケーションズ株式会社
技術開発部
中原　悠希

Spud(BoF)の開催の経緯

■ IABの“IP Stack Evolution(IPSE)”プログラムにおいて、1月26,27日に“Stack Evolution in a Middlebox Internet(SEMI)”ワークショップが開催され、IETFにおけるSPUD BoF開催が提案、承認された。

IP Stack Evolutionプログラムのスコープ

“The IP Stack Evolution program covers various topics in the evolution of IPv4 and IPv6, the transport protocols running over IP, and the overall protocol stack architecture.”

- 現状多くのアプリが HTTP/TCP/IPを利用。この原因は、
  - 他のプロトコルのインターフェースは乏しく、アプリ開発者からの利用が難しい。
  - MiddleboxがTransparencyを制限している。

  の2点。
- そこでIPSEでは以下の2つを主なフォーカスとしている。
  ①SOCK_STREAMやSOCK_DGRAMを改善したI/Fを作る。
  ②Middlebox存在下でのTransparencyを改善する。

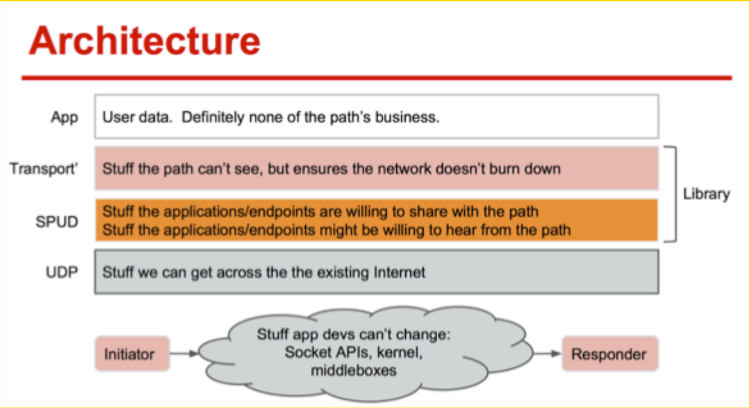
Stack Evolution in a Middlebox Internetワークショップ

- インターネットのトランスポートは、古いI/Fに縛られていること、およびMiddleboxがパケットを書き換えてしまう問題のせいで硬直化しており、トランスポートレイヤのイノベーションを阻害している。
- これを解決し、E2E原理を取り戻すための方策を考えるのが本ワークショップの目的。
- 20件のポジションペーパーが提出され、議論が行われた。
- Spud BoFの開催が決定され、これに向けたDraftの執筆、プレゼン発表のアサインがされた。

http://tools.ietf.org/bof/trac/wiki/BofIETF92
https://www.iab.org/activities/programs/ip-stack-evolution-program/
https://www.iab.org/activities/workshops/semi/
https://www.iab.org/wp-content/IAB-uploads/2014/09/stackevo-cfp.pdf

SPUD(Substrate Protocol for User Datagrams) BoF サマリ

- IABのWorkshop「Stack Evolution」が開催され、IETF#92でのSPUD BoF開催が計画された。
- SPUDのスコープは、Middleboxがあってもe2E通信が可能な新しいトランスポートプロトコルをUDP上に作る事。
- IETF#92の段階では、要求条件分析・プロトコルの草案が提案された状態。新プロトコルの作成には、参加者は前向き。
- 「tube」という概念でUDPパケットをセッション管理する。
- 今後の取り組みについての議論の結果、SPUDはまだWG化されず、BoFとして継続議論される見通し。
- 関連情報
  - 議長:
    Mirja Kühlewind氏 (チューリッヒ工大)
    Eliot Lear氏 (Cisco)
  - 所属エリア: Transport Area
  - BoF参加人数: 200人程度



https://datatracker.ietf.org/meeting/92/agenda/spud/

(参考) 進め方に関しての議論

■ 進め方について主な議論

- WGを作ってCharterを書き始めるか、WGを作るためのBoFを開くか、もっと議論が必要か、それともRGを作る方が良いのか、話し合われた。
- Rapid deploymentとCareful Designのどっちを優先するか、という問いに対して「とにかく立ち止まらずに仕様を作ろう」派と「プロトコルは長年使われるものだから慎重にやろう」派の意見があった。
- 以下、参加者からの主な意見
  - まだまだオープンな場で議論したいので、BoFを続けるべき。(多数)
  - 問題領域が広いので、BoFをまた開いて議論すべき。
  - WG化、WG Charterを書くのは時期尚早である。
  - BoFを続ける以前にStackEvolution programの中で議論を継続して、まとまったらIETF BoFの場に持ってくるべき。
  - いろんな意見があるけど、Charterは早く書くべき。
  - これをResearchだととらえるべきで無い。ここはIRTFではなくてIETF。WG化して実験的プロトコルを作ってみるべき。
- BoF継続が多数派であり、次回IETFでもBoFが開かれると思われる。

SPUD BoF アジェンダ

- Chair's slides & Agenda Bashing (Chair)
  - 本BoFの目的について
- Introduction (Brian Trammell氏)
  - SPUDの背景および主な方針について概説。
- SPUD Requirements (Ted Hardie氏)
  - SPUDのハイレベル要求条件について。
- SPUD Prototype (Joe Hildebrand氏)
  - 試作したSPUDプロトコルについて紹介。当日急遽追加。
- DTLS as Subtransport protocol (Christian Huitema氏)
  - 下位プロトコルとしてDTLSを用いることのメリットを紹介。

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

https://www.ietf.org/proceedings/92/agenda/agenda-92-spud

プレゼン1 Introduction

■ 要旨

- SPUD BoF開催の経緯を、IABでの「Stack Evolution in a Middlebox Internet(SEMI)」ワークショップの結果と説明。
- 現在のNWは、NAT/FW等のMiddleboxが経路上にあると、帯域・レイテンシの面でボトルネックになったり、パケットを止めてしまうという問題がある。
- SPUDの最初のユースケースとして、UDP firewall traversalを提案。

現状の問題(WebRTC DataChannelを例に)

History (in other words)

- This problem was effectively referred to us by the RTCWEB working group.
  - What draft-ietf-rtcweb-data channel says: "The encapsulation of SCTP over DTLS over ICE/UDP provides a NAT traversal solution together with confidentiality, source authentication, and integrity protected transfers."
  - What I read: "The stack is broken, please help!"

ユースケース: UDP Firewall Traversal

Initial Use Case: UDP firewall traversal

- Today UDP is often blocked ("99% of UDP is garbage") but volume of (good) UDP traffic grows, e.g. RTCWEB uses UDP for data and media.
- Hard to establish session/flow state at firewalls: block rules are stateless
- Need an *explicit* contract to establish state along the path (as today's *implicit* contract does with TCP)

Approach

- Use of identifiers ("tubes") beyond the five-tuple to link packets together
- Explicit signaling/negotiation of tube start/end
  - Indicate start/stop to middlebox
  - Confirm connection establishment by receiver

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

https://datatracker.ietf.org/meeting/92/agenda/spud/

プレゼン2 SPUD Requirements

■ 要旨

- SPUDのハイレベルの要求条件を提案。
- プライバシー問題があるので、DPIが無くてもMiddleboxを通過出来る事が必要。
- NW装置が、同一セッションに属する複数のUDPパケットを認識出来るよう「tube」という概念を導入。

経路上のNW装置は、UDPパケットをグルーピングできる

Application to path semantics

We need to be able to tell the path which UDP packets are part of the same group (tube).

We need to be able to tell the path about flow starts and stops for that grouping, so that boxes along the way can maintain state for it without heartbeats.

We may experiment with more, but these are essential. Ordinal priority among multiple groups on the same 5-tuple is one example extension.

アプリケーションは、経路上のNW装置から情報をもらえる(副効用)

Path to application semantics

The primary requirement is for advisory messages similar to ICMP, but scoped to a grouping (tube) instead of to the destination address.

This may include information from the path on resource constraints, on available MTU, noting address family conversion, and flagging congestion.

All should be advisory, with a "trust but verify" approach.

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

https://datatracker.ietf.org/meeting/92/agenda/spud/

プレゼン4 SPUD Prototype

■ 要旨

- SPUDのプロトタイプを作ったので、その紹介。(GitHubで公開中)

パケットヘッダ案(再掲)

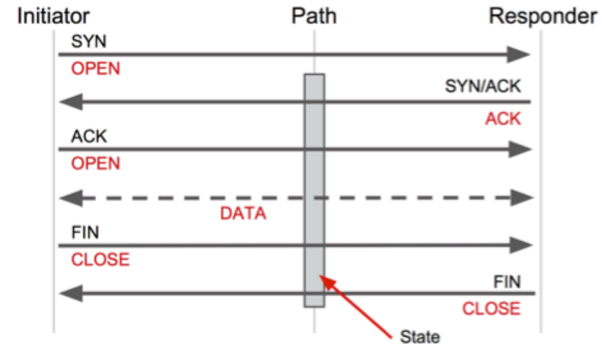
Current Packet Layout

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	magic = 0xd80000d8																															
4	32	tube id																															
8	64																																
12	96	cmd		adec	pdec	resv				CBOR map ...																							

Magic: Constant
Command: Data, Open, Close, Ack
Application Declaration: CBOR contains information for the path bound to the tube ID
Path Declaration: CBOR contains information from the path bound to the tube ID
CBOR (RFC 7049): { 0: [application data], "something else": "for the path!" }

TCPのシーケンスとの対比

Example TCP over SPUD mapping



https://datatracker.ietf.org/meeting/92/agenda/spud/ https://github.com/iptube

//developer.cisco.com/site/ietf-hackathon/

Log In | Register | Subscribe | Solution Partner | Marketplace

cisco DevNet

Browse · Sandbox · Community · Events · Support

IETF Hackathon at IETF 92, March 21-22, Dallas, TX

The firrst ever IETF Hackathon was held March 21-22, the weekend before IETF 92 in Dallas, Texas. It took place just before IETF 92, and was free for both newcomers and grey beards to get involved.

All you needed was a knowledge of networking technologies, and you were guaranteed to learn something new and have fun!

As a supporter and active member of IETF standards development, Cisco was pleased to be supporting this initiative through the Cisco DevNet program.

Many thanks to all involved, bringing the emphasis on 'running code' back into the IETF

Which technologies were included?

The hackathon featured six technology areas, representing a mix of existing IETF working groups, proposals with BoFs (Birds of a Feather sessions) occurring later in the week, and a combination of new and established open source projects.

- BIER (Bit Index Explicit Replication)
- NETVC and Daala (Internet Video Code)
- I2RS/OpenDaylight + NETCONF/YANG
- Services Function Chaining (SFC) in OpenDaylight (ODL)
- SPUD (Substrate Protocol Underneath Datagrams)
- STUN/DISCUSS (Dierentiated prIorities and Status Code-points Using Stun Signaling)

What projects were created, using which technologies?

- BIER powered HOMENET multicast routing
- NETVC/Daala: new contributor added, video analyzer created
- OpenDaylight ietf-syslog model: used to congure Linux rsyslog daemon
- OpenDaylight developer VM: created, used, and rened to provide complete development environment for I2RS, SFC, ietfsyslog project, and others projects involving OpenDaylight
- SFC traceroute: draft implemented, revealing error in the specication fixed by a new version of draft
- NETCONF integration for SFC
- YANG model inventory; tool that produces RFC/internet draft template from YANG model
- SPUDlib open source project contributors increased 200%
- SPUD prototype: draft implemented, used as input in BoF later in week
- STUN/DISCUSS: demo created

"People were so engrossed in their projects that lunch sat untouched for half an hour. Fresh cookies provided as an afternoon snack did not distract" said

Find out exactly why lunch remained untouched in the two day hackathon!

Read the DevNet blog post

"I got to learn a lot and meet talented folks. I do not know why such an event never happened till 2015, it should have been a part of IETF since day one."

Sunil Vallamkonda, F5

"My personal thanks for helping out in the IETF Hackathon and plugging me to right group to contribute. I should say I had a good time hacking as a first time IETFer"

Hariharan Ananthakrishnan

Packet Design

プレゼン3 DTLS as Subtransport protocol

■ 要旨

- 新プロトコルを作るにおいて、暗号化の仕組みをイチから新しく作ると大変なので、DTLSを用いることを推奨。
- プレゼン2(要求条件)に対して、MiddleBoxでのセッションStart/Stopが検知可能、NW情報の収集が可能、という点をDTLSが満たしていると主張。

DTLSを下位に使う事のメリット

Gaps: DTLS as efficient sub-transport

- Zero RTT setup
  - Zero RTT setup will be supported in TLS/1.3
- Low overhead
  - 13 bytes of header, out of 1500 bytes UDP packet, maybe too much
  - Could use compression per draft-modadugu-dtls-short-00
- DOS resilience – without TCP 3 ways handshake
  - Resource at server: use DTLS cookies mechanism
  - DOS amplification: require padding of initial packet
- Context-ID
  - Additional 8 byte identifier would allow MP-TCP like functionality
  - Discuss – do we need to multiplex many connections per 5-tuple?

DTLSとmiddlebox

Gaps: DTLS and being middle-box friendly

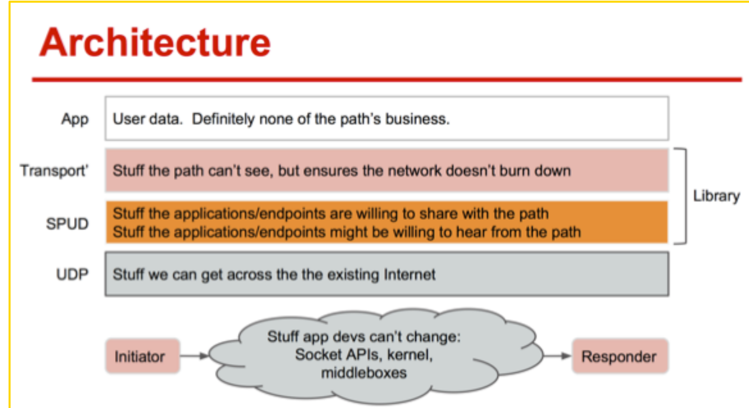
- Protocol detection
  - Have middle box understand what protocol is being used
  - Some minimal support in DTLS – pattern matching clear text headers
  - But generally goes against the whole point of encryption
- Start-Stop indication
  - Suggested to help resource control at middle box
  - Start is obvious – first packet does it
  - Plausible Stop heuristic, monitor "Alert" content type in clear text header
- Accepting indications from the network
  - For example, "congestion detected" or "PMTU supported"
  - Goes against the grain of DTLS – not encrypted, not secure
  - Heuristics are possible, but not obvious
  - End-to-end evaluation of MTU, congestion seems more plausible

https://datatracker.ietf.org/meeting/92/agenda/spud/

再掲

SPUD(Substrate Protocol for User Datagrams) BoF サマリ

- IABのWorkshop「Stack Evolution」が開催され、IETF#92でのSPUD BoF開催が計画された。
- SPUDのスコープは、Middleboxがあっても E2E通信が可能な新しいトランスポートプロトコルをUDP上に作る事。
- IETF#92の段階では、要求条件分析・プロトコルの草案が提案された状態。新プロトコルの作成には、参加者は前向き。
- 「tube」という概念でUDPパケットをセッション管理する。
- 今後の取り組みについての議論の結果、SPUDはまだWG化されず、BoFとして継続議論される見通し。
- 関連情報
  - 議長:
    Mirja Kühlewind氏 (チューリッヒ工大)
    Eliot Lear氏 (Cisco)
  - 所属エリア: Transport Area
  - BoF参加人数: 200人程度



https://datatracker.ietf.org/meeting/92/agenda/spud/