IETF 99 (プラハ) 報告会
RTG Area トピックス

2017/9/1

栃尾　祐治(富士通研究所)

[RTG Area]現在の構成

Area Directors: Alvaro Retana, Alia Atlas, Deborah Brungard

- *BABEL*
- BESS
- BFD
- *BIER*
- **CCAMP**
- **DETNET**
- I2RS
- IDR
- *ISIS*
- *L2TPEXT*
- *LISP*
- *MANET*
- **MPLS**
- **NVO3**
- OSPF
- PALS
- **PCE**
- *PIM*
- *ROLL*
- **RTGWG**
- SFC
- *SIDR*
- SPRING
- **TEAS**
- *TRILL*

青: 今回参加、黒: 時間があえば参加、
斜体: 関与薄、灰色: 今回未開催

参考
https://trac.ietf.org/trac/rtg/wiki/IETF99summary

今回の報告事項

RTG中心に出席した最近の話題を紹介

- MPLS WG などにみる最近のMPLS
  - MPLS over UDP with SR
  - RTG WG (, SPRING WG) も含む
  - さらに DC routing & VPN+ も含む
- DetNet WG
  - Encapsulation, Security…
  - Psuedowire control word に関わる問題
    - 一部PALS WGにも関連
- IDEAS (BoF)
  - Identifier vs Identity
  - LISP and HIP

- 参考までに、先週から話題(!?)のBGPを扱うIDRの状況は…
  - Route Leak Prevention, BGP Tunnel attributes , FlowSpec(rfc5575bis)の継続議論
  - BGP extended communityでのcongestion status 定義、LLDP peer discovery の議論が中心のようで、例の件でMLが盛り上がった形跡もなし…

先に OPS Area すこしだけ…

- NETCONF/YANG(NETMOD)
  - NETCONF/YANGに関しての大きな進展は、前回合意された NMDA/Datastore更新(operationalサポート)に伴うYANG更新が中心
    - draft-ietf-netmod-revised-datastores
    - 前回報告した、Old Train → Train 1/2　の件
  - YANG pushのソリューションの進展は思ったほどなし
  - 他:
    - Yang-mount ドラフトがカムバック
    - Notification for UDP(←TCP)について議論(反応そこそこあり)
- ANIMA
  - 基本となるプロトコル(GRASPなど)はかなり熟したので今後について議論
  - professionally-managedをベースにしたネットワーク自動構築技術を検討するというコンセプト中、(1) 現在のANI (Autonomic Networking Infrastructure) をてこ入れする、(2) ANIをさらに拡張する (3) ASA (Autonomic Service Agent)を掘り下げるという3案が示された
- SUPA, LIME, L2SM
  - 開催されず…

MPLS WG

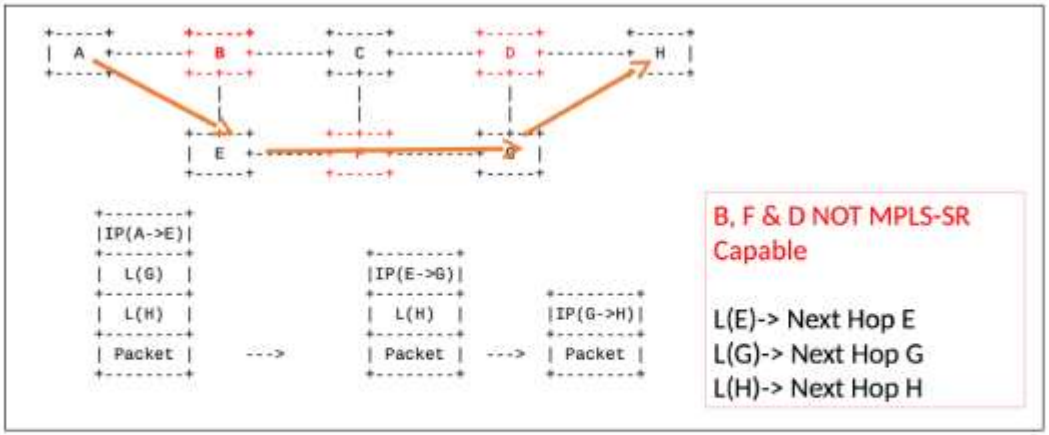
(RTGWG含む)

はじめに(または前回の振り返り)

- ここ(MPLS WG)で話す内容は、前回IETF98報告会での宮坂さんパートの続きとなります。

MPLS-SR over non-MPLS nodes

- https://tools.ietf.org/html/draft-xu-mpls-unified-source-routing-instruction-00
- MPLS capableでないノードがあってもMPLS-SRを動作できるようにする提案
- MPLS over IP / MPLS over UDPはすでにRFC化されているのでそれを利用するだけでよいとのこと



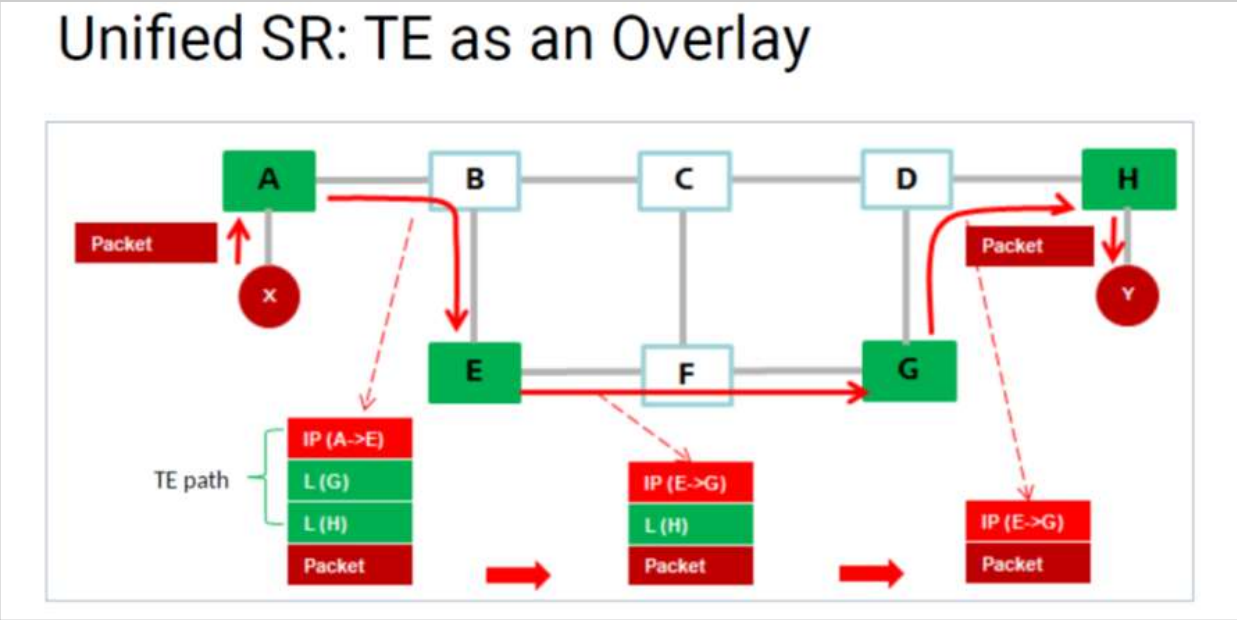
MPLS WG

7

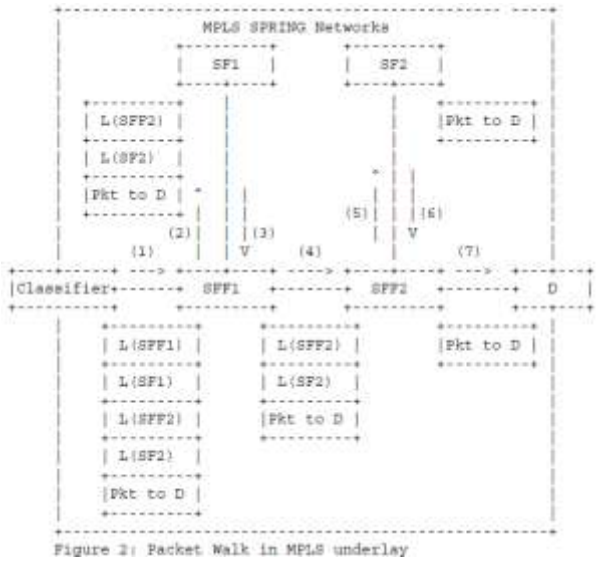
https://www.isoc.jp/wiki.cgi?file=20170512%5Fietf98%2Dupdate%5FTakuyaMiyasaka%2Epdf&page=IETF98Update&action=ATTACH

MPLS WG

- **Unified Source Routing Instruction using MPLS Label Stack** (再掲)
  - draft-xu-mpls-unified-source-routing-instruction
  - MPLS Segment routing(SR)ならびにMPLS over UDP (RFC7510)の組み合わせで、IP SRとの相互接続を実現し、Unified Source Routing 実現するもの
  - adj-SIDによるSRも可能であることを明記すると共に、overlay でも TE ができることをアピール



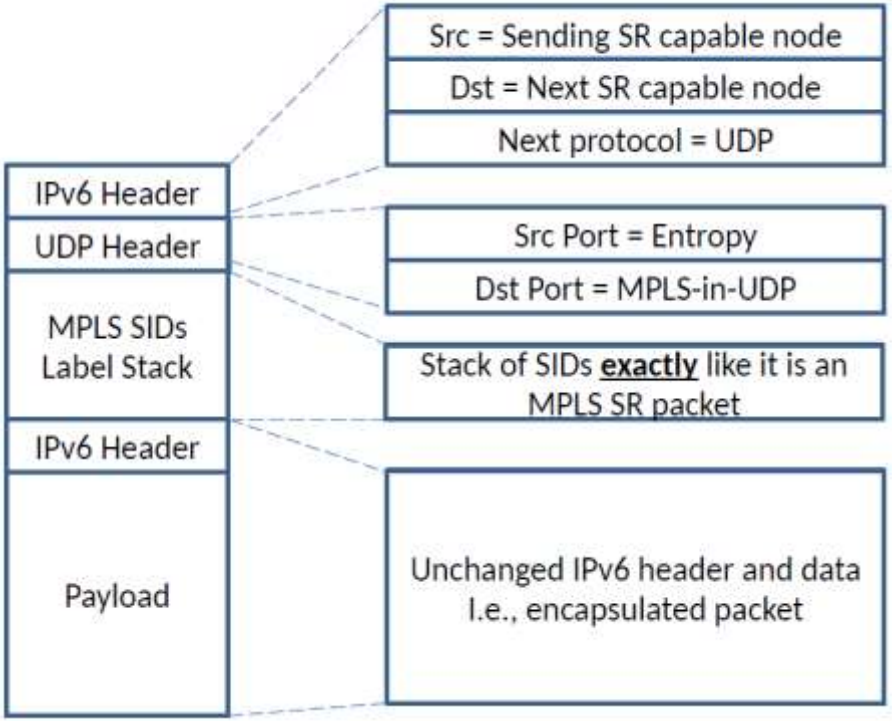
https://datatracker.ietf.org/meeting/99/materials/slides-99-mpls-sessa-02-draft-xu-mpls-unified-source-routing-instruction-ietf99

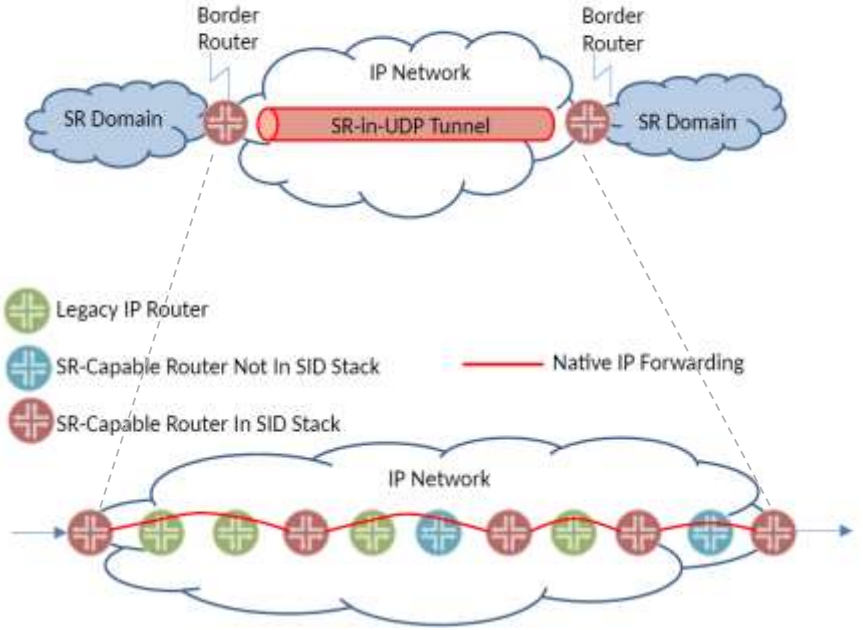


- 応用例としてService Chaining への適用(右)
  - draft-xu-mpls-service-chaining

MPLS WG

- **A Unified Approach to IP Segment Routing**
  - draft-bryant-mpls-unified-ip-sr
- いっそのこと(?)、IPv6 + MPLS によるUnified Segment Routing Protocolを定義してしまおうという提案。このことによりMPLS SR over IPv6を実現
  - IPv6網ではSR capable でもnon capable でも転送可能
  - すでに J 社系では展開中?

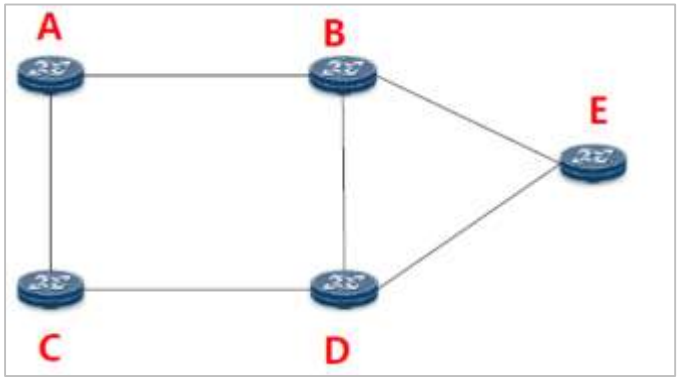


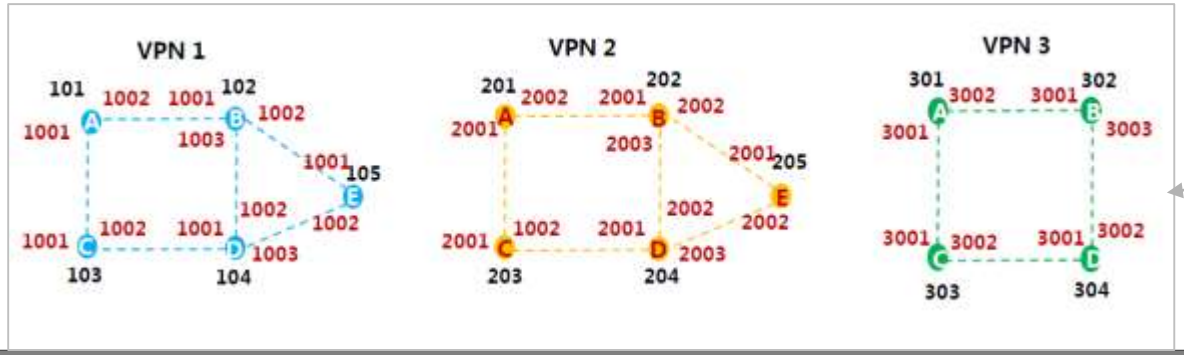


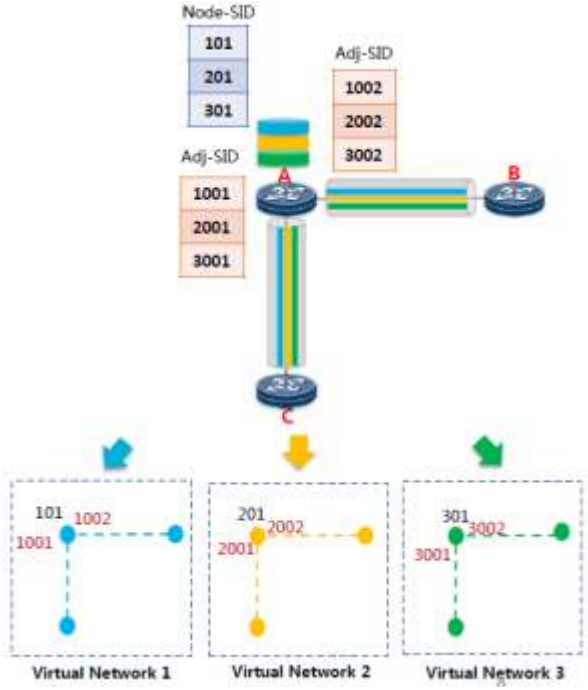
https://datatracker.ietf.org/meeting/99/materials/slides-99-mpls-sessb-07-draft-bryant-mpls-unified-ip-sr

VPN+

- **Enhanced Virtual Private Networks (VPN+)**
  - **draft-bryant-rtgwg-enhanced-vpn**
- Segment routing + IP & MPLS underlay
- SID を多彩に組み合わせることで Isolation を提供し柔軟なVPNを構築可能
- SRの制御/設定(instruction)にて、TEないしはLatency supportも可能







https://datatracker.ietf.org/meeting/99/materials/slides-99-rtgwg-sessb-enhanced-virtual-networks-vpn

Routing in the DC

- VPN+ の話が出たところで RTG WGで進めているData centerにおけるルーティング拡張の今後について
- IETF 100 にて BoF を開催
  - ML: https://www.ietf.org/mailman/listinfo/dcrouting
  - この場で、Problem statement と solution を検討する 1st stepとする予定
  - *以前開催されなかったSCALE BoF(VPN拡張)の二の舞にならないこと祈りつつ..*
- 参考までにこまで議論された主なドラフト
  - draft-keyupate-idr-bgp-spf
  - draft-shen-isis-spine-leaf-ext
  - draft-przygienda-rift
  - draft-sl-rtgwg-far-dcn

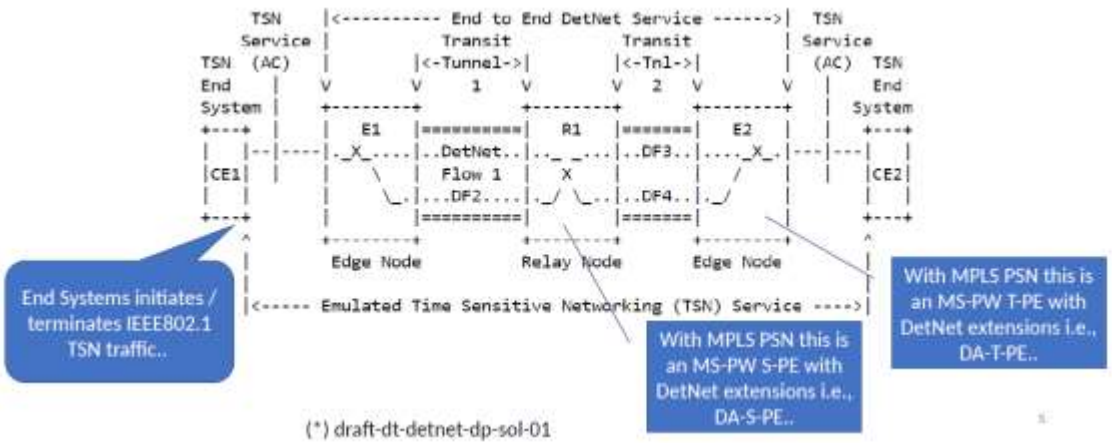
DETNET WG

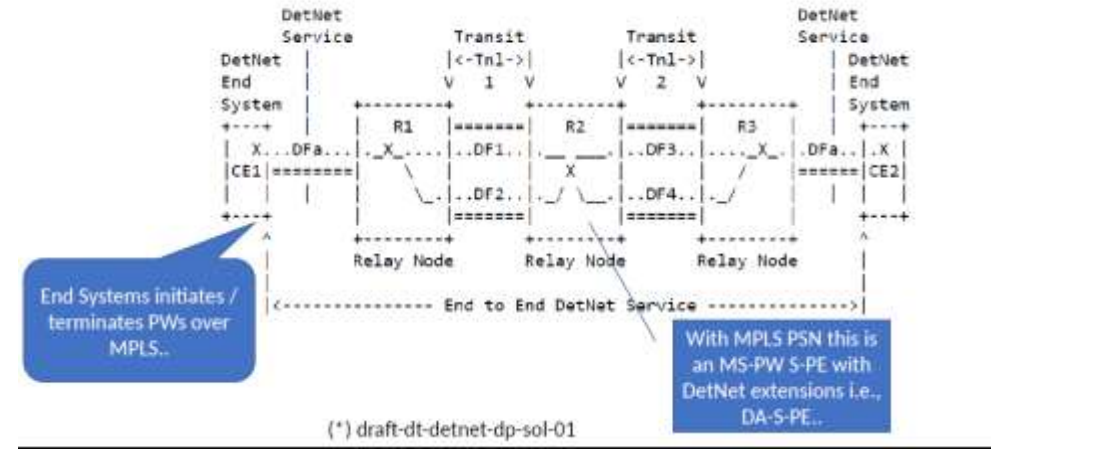
DetNet WG とは

- **Deterministic Networking**
  - L2, L3 networkにおいて、低遅延、低ジッタ(delay variation)を実現するためのネットワーキングを検討
    - 5G networking の要求沿ったネットワーク検討とも
  - IEEE 802.1 TSN (Time sensitive networking) と連携
  - IETFのWGなのでL3観点(IP, MPLS)で検討
- 現在の状況
  - ユースケースならびにアーキテクチャは WG I-Dにて検討
    - draft-ietf-detnet-use-cases
    - draft-ietf-detnet-architecture
  - 目下の話題はEncapsulation(draft-dt-detnet-dp-sol)
    - 2段構えのWG adaptation(問題を修正し合意→WG ID poll)も
  - 今回の会合ではSecurity関連(draft-sdt-detnet-security)も議論
    - WG I-Dになる見込み
- 個人的に思う課題
  - Data plane(Encapsulation)は、おおよその解決はついたと思われるが、DetNet でめざすNetworkのキモである低遅延、低ジッタ、同期について、IETFとしてどれだけcontributeできるのかまだ議論の余地も(つまりIEEE802.1 TSNにかなり依存)

DetNet Encapsulation (draft-dt-detnet-dp-sol)

- これまでの検討では、IEEE802.1TSN over DetNet 、ならびに、PW(Peusdowire)-based DetNetをusecaseとして想定
- いずれにしてもDetNet service にはMPLS/PWを適用する前提





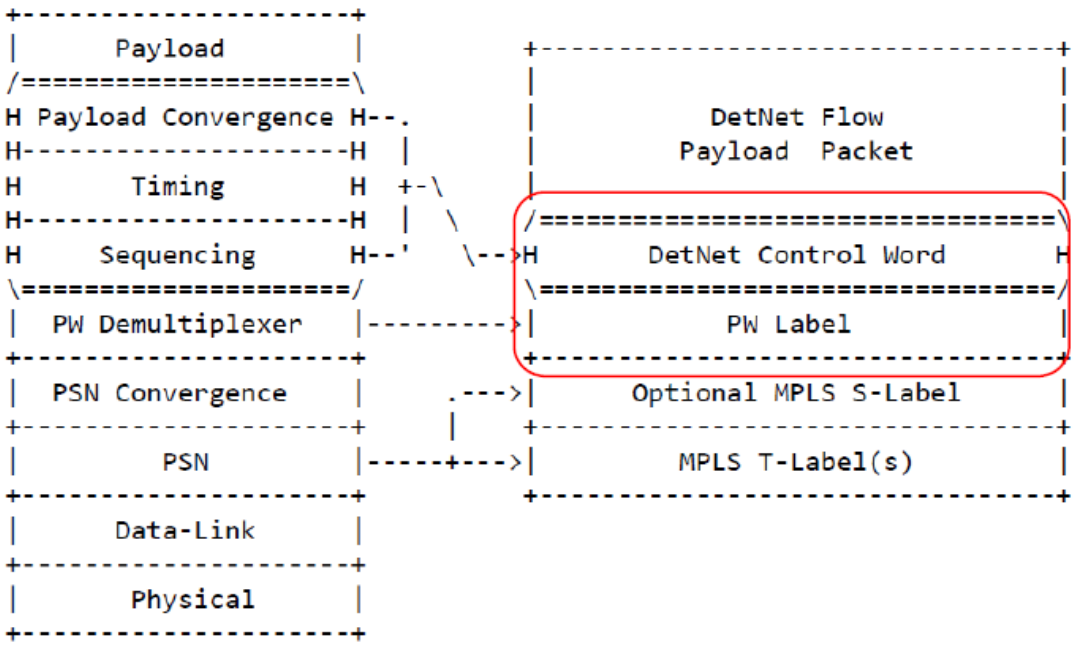
https://datatracker.ietf.org/meeting/99/materials/slides-99-detnet-detnet-data-plane-encapsulation

IEEE802.1TSNとは(参考/個人見解)：
http://www.ieee802.org/1/pages/tsn.html

- IEEE802.1における主に低遅延伝送特性を定義する Task group
- 特に積極的に活動している項目は Bounded low latency 規定
  - Credit Based Shaper (.1Qat)
  - Frame Preemption (.3br & .1Qbu)
  - Scheduled Traffic (.1Qbv)
  - Cyclic Queueing & Forwarding(.1QCh)
  - Asynchronous Traffic Shaping(.1Qcr)
- 並びに、Reliability 実現に以下検討
  - Frame Replication & Elimination (.1CB),
  - Per Stream Filtering and Policing (.1Qci)
- 他 Time & Sync, Resource mgmt を検討
- 参考: IETF99向けTutorial

DetNet Encapsulation

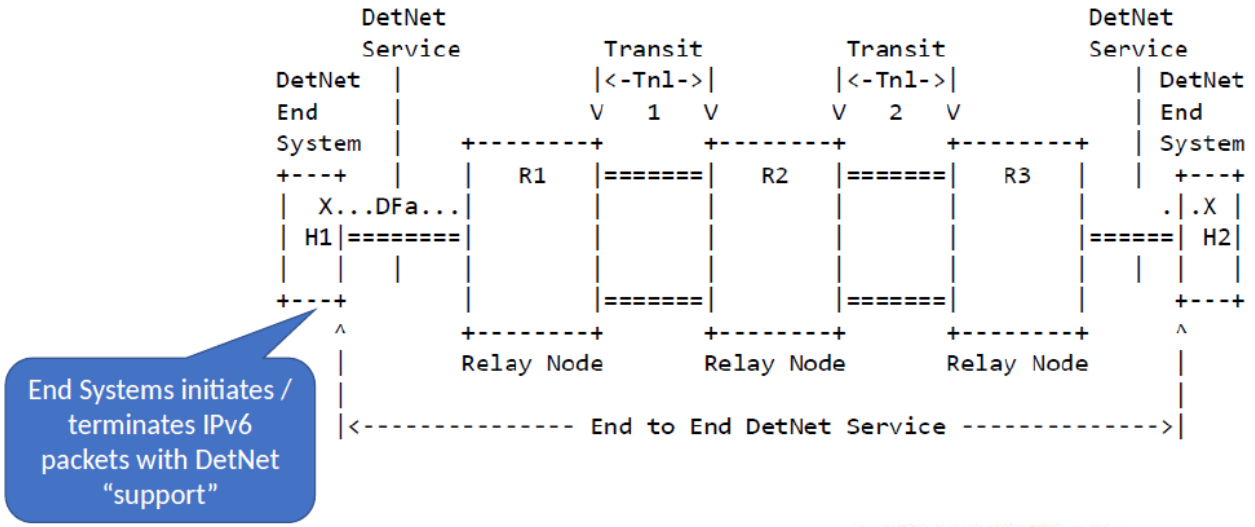
- MPLS/PW での Encapsulation は、RFC 3985 (PWE3 architecture)
- 課題は”DetNet Control Word(CW)”. Ethernet CW (RFC 4448) を想定しているが、Ethernet CW は option. たとえ使用したとしても、内部に定義の16 bit Sequence Number もまたoption なので、実際に使用する場合に問題が発生するとの懸念が…
  - DetNet では冗長提供(packet by packetで提供)のためSequence Number の使用を想定
  - なお、今回の PALS WG では、Option だった Ethernet CW をマンダトリにしようという提案があり RFC 4448 が更新される可能性が大 (当初問題でないと思っていた 0x4, 0x6 で始まる non IP packetへの対応として)

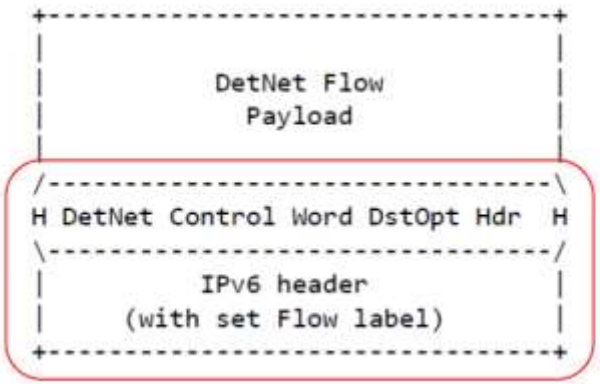


- DetNet flow:
  - Flow-ID -> PW label.
  - SeqNum -> CW.
- S-Label:
  - A DetNet node to DetNet node "service" label that is used between DA-*-PE devices (see slide 5).
- T-Label:
  - Used to identify the LSP used to transport a DetNet flow across an MPLS PSN, e.g., a hop-by-hop label used between LSRs.

DetNet Encapsulation

- 今回の会合(正しくはdraft-dt-detnet-dp-sol-01)にてnative IPv6 の追加
  - よさげに見えるが、IPv6 は PWサポートがないので、これまた懸念も…





- DetNet flow:
  - Flow-ID -> Flow Label.
  - SeqNum -> DetNet DstOpt.
- For explicit routes DstOpt works well for unicast flows e.g., with Segment Routing.

DetNet Security Consideration

- draft-sdt-detnet-security
- Attacker type (RFC7364)に応じて
  要素を分析の上、impact/mitigationを考察

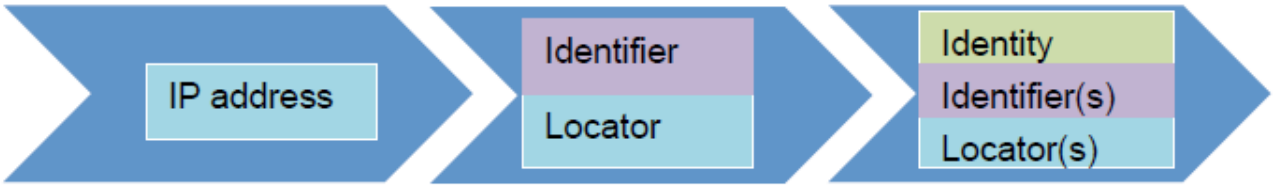
Attack	Attacker Type			
	Internal MITM	Internal Inj.	External MITM	External Inj.
Delay attack	+		+	
DetNet Flow Modification or Spoofing	+	+		
Inter-segment Attack	+	+		
Replication: Increased Attack Surface	+	+	+	+
Replication-related Header Manipulation	+			
Path Manipulation	+	+		
Path Choice: Increased Attack Surface	+	+	+	+
Control or Signaling Packet Modification	+			
Control or Signaling Packet Injection		+		
Reconnaissance	+		+	
Attacks on Time Sync Mechanisms	+	+	+	+

Attack	Impact	Mitigations
Delay Attack	-Non-deterministic delay -Data disruption -Increased resource consumption	-Path redundancy -Performance analytics
DetNet Flow Modification or Spoofing	-Increased resource consumption -Data disruption	-Path redundancy -Integrity protection -DetNet Node authentication
Inter-Segment Attack	-Increased resource consumption -Data disruption	-Path redundancy -Performance analytics
Replication: Increased attack surface	-All impacts of other attacks	-Integrity protection -DetNet Node authentication
Replication-related Header Manipulation	-Non-deterministic delay -Data disruption	-Integrity protection -DetNet Node authentication
Path Manipulation	-Enabler for other attacks	-Control message protection
Path Choice: Increased Attack Surface	-All impacts of other attacks	-Control message protection
Control or Signaling Packet Modification	-Increased resource consumption -Non-deterministic delay -Data disruption	-Control message protection
Control or Signaling Packet Injection	-Increased resource consumption -Non-deterministic delay -Data disruption	-Control message protection
Reconnaissance	-Enabler for other attacks	-Encryption
Attacks on Time Sync Mechanisms	-Non-deterministic delay -Increased resource consumption -Data disruption	-Path redundancy -Control message protection -Performance analytics

IDEAS BOF

IDEAS BoF

- **IDentity EnAbled networkS**
  - 前回はSide meeting。今回はBoFになっての議論。RTG area配下での開催。
  - 前からも紹介された、Generic Identity Service (GRIDS)を導入するための基本的な課題の明確化と既存WGとの課題を明確した内容
  - ポイントとしては、LISPで、Entityに対してIdentifier(とlocator)の定義を導入したが、Identifier (Idf)のライフタイムをどう考えるかを突き止めると、Identity (who)という概念が必要でそのIdentityとIdentifier(where)間でライフタイム管理を行うことで、Idfを意味あるものかつプライバシーを考慮しつつ管理を行い、IDベースのサービス提供を行う枠組みを規定ISP以外にもすでにHIP (Host Identity Protocol) WGでなんとかなるのではという紹介もあり(認証が重くDiscoveryが課題らしい)

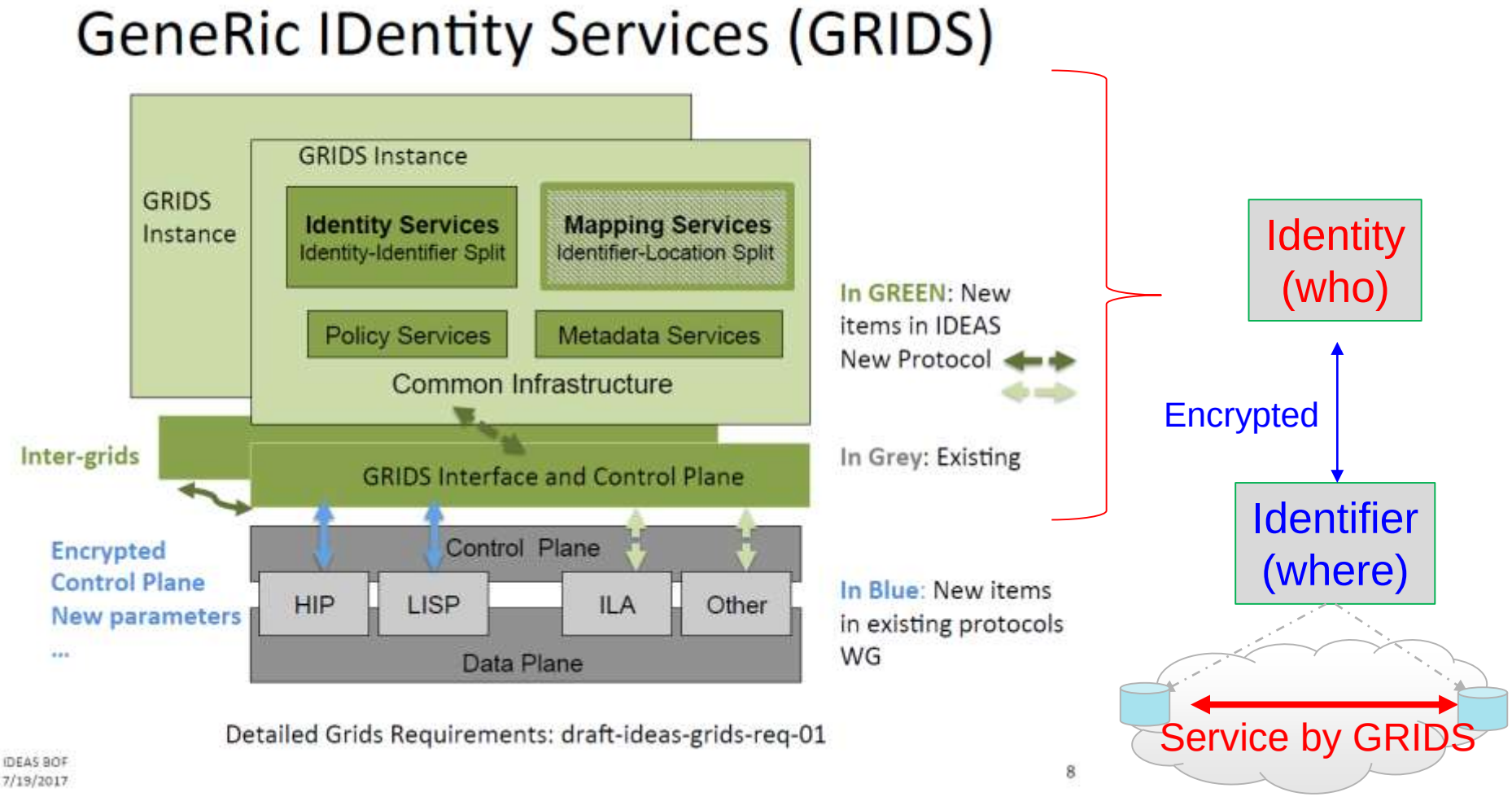


Identity is an enabler:
- Lookup access control without being easily defeated
- Privacy of flows to eavesdroppers
- Immutable but erasable external representation (identifier)
- Simple policies based on Identity
- Features based on Identity

https://datatracker.ietf.org/meeting/99/materials/slides-99-ideas-ideas-problem-statement

IDEAS

- 目指すものまたは実現したいもの – GRIDS



IDEAS (proposed charter)

- Network solutions based on the concept of Identifier-Locator separation are increasingly considered to support mobility and multi-homing across heterogeneous access networks. Identifier-locator separation protocols require infrastructure that allows nodes to discover the network topological location(s) of its peer(s) for packet delivery.
- However,additional infrastructure and new protocol extensions are needed to address new requirements that go well beyond the traditional discovery service and mapping of identifier-to-location for packet delivery.
- In addition,identity-enabled networks introduce the concept of identity-identifier split. <…>

- Examples of the problem space are:
  - Privacy: <…>The endpoint communications should be able to change their identifier while retainingtheir identity and associated policies.<…>
  - Access control :<…>Therefore, it is desirable to have a certain degree of control over who canlook up the identifier-locator binding information for example.
  - Common infrastructure and Primitives: The application of common and consistent basic networking policies that can apply at the level of entity reduces operational complexity associated with managing services for individual endpoints.<…>

IDEAS 所感

※あくまで個人の見解なので今後の展開はMLなどを参照のこと

https://www.ietf.org/mailman/listinfo/ideas

- IDf(Identifier)の定義を明確にしないと発散しかねない？
  - LISP の延長としているが、解釈次第ではどうでも拡大できるかも
  - draft-padma-ideas-req-gridsを読んでも明確に落とせない
- IDy(Identity)とは実は新手のSDN controller定義?
  - draft-padma-ideas-req-grids には以下の記載あり
    Identity-Enabled Networks are enabled by a set of core services that are provided by common control infrastructure
- 他WGとの重複は?
  - Dataplane: NVO3やSFC との違いは?
    - Charter議論で、Identity and Identifier だけでなく identifier 間interactionを考えるべきという声も
  - Netconf/Restconf (NETCONF/NETCONF)との違いは？
    - Identifier と Data model(metadata)に共通点

まとめ

まとめ

RTG中心に最近の話題を紹介

- MPLS WG などにみる最近のMPLSの動向
  - RTG WGも含む
    - さらにDC routing & VPN+ も含む
- DetNet WG
  - PALS WG も含む
  - Encapsulation, Security…
- IDEAS (BoF)
  - ID based network の新たな形の模索？

- 折に触れて紹介したとおり、IP(v6) と MPLS のこれからの付き合い方について変化が生じているようなドラフトがいくつか見られ、今後のNetworking(Data plane構成)にも影響がでるかもしれない、というのが今回の所感

ありがとうございました