IETF112 工作组参会报告

1. DetNet

OAM Framework

Presenter: Greg Mirsky

Draft: https://datatracker.ietf.org/doc/draft-ietf-detnet-oam-framework/

主席 Lou 建议针对每一个参数单独提出对应的 OAM 需求，对 out of band 和 telemetry 的用法进行澄清。对 DetNet OAM 定义的 out of band，与 RFC7799 的定义不完全相同，建议澄清。7799 是表示 passive，DetNet OAM 的对去程 request 定义是 active+inband，回程 reply 报文是 out of band。文稿中有引用 telemetry，Lou 认为 telemetry 不是 OAM 本身，而是对 OAM 的监控。建议对文稿中的 telemetry 进行澄清。

OAM Functions for The Service Sub-Layer

Presenter: Balázs Varga

Draft: https://datatracker.ietf.org/doc/draft-varga-detnet-service-sub-layer-oam/

新定义一个 d-ACH 格式，与原有 RFC5586 G-ACH 的差异如下图。

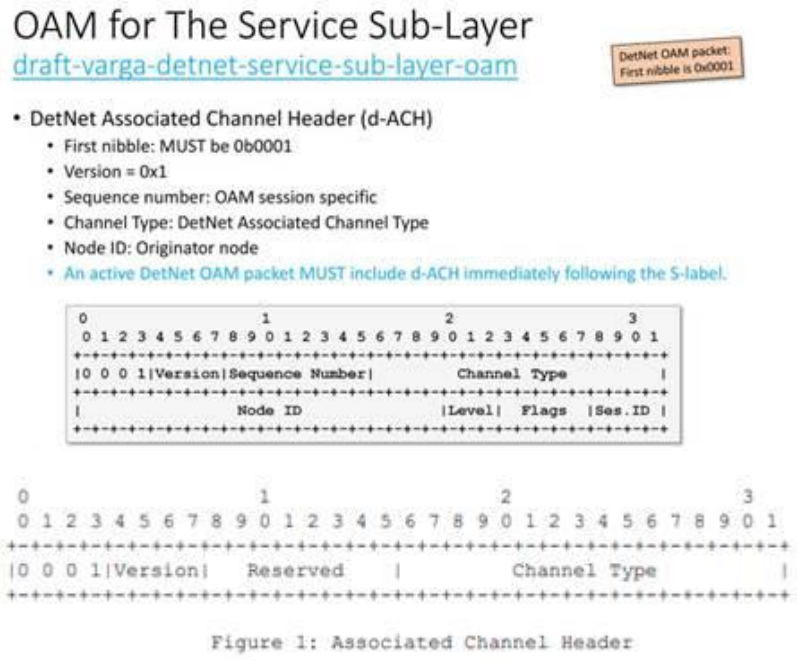


Figure 1: Associated Channel Header

MPLS OAM

Presenter: Greg Mirsky

Draft: https://datatracker.ietf.org/doc/draft-ietf-detnet-mpls-oam/

主席建议下一步将 D-ACH 格式纳入工作组文稿。

Stewart：认为从 PALS 的讨论看，0001 保留比特还要做修改，最终是由 PALS 决定格式，但 channel type 部分没有问题。

Lou ： 先考虑这篇文稿中 detnet 相关内容的处理。如果工作组同意，建议将这篇文稿的技术部分纳入 detnet MPLS OAM 工作组文稿中，同时等待 MPLS 和 PALS 的讨论结果。如果有必要，时间上可以和 PALS 联合进行 WGLC。同时授权 Greg 在 ML 发起对接收这部分技术内容的提议。

PREOF for DetNet IP

Presenter: Balázs Varga

Draft: https://datatracker.ietf.org/doc/draft-varga-detnet-ip-preof/

Toerless 反馈 ML 讨论的问题还没有得到完全解决。问题是指在选收节点时，文稿提出的机制并没有解决对 latency，jitter 和 buffering 的影响。

Lou 认为 Toerless 的问题也是适用于 RFC8964 MPLS PREOF 的问题，不是专门对 IP PREOF 的问题，需要单独讨论，而不需要这篇文稿解决。

思科 Pascal：虽然是 IP 层的 PREOF，但方案只是在传输层内容增加了封装，在 IP 层仍无法对 detnet 流进行识别和 PREOF。会后在邮件列表补充了对方案的意见，主要观点包括：UDP 内封装 PREOF 使用的流 ID 和序列号，对硬件处理不友好； IT、OT 设备可能是轻量级的，不是所有 Detnet 场景的设备都基于 MPLS 和 PW 机制；由于 IPv6 现在要进行诸多扩展，UDP 后的封装更加难以获得；应该结合当前 IPv6、SRv6 的扩展提出与时俱进的方案，并表达不同意工作组接收这部分技术内容。

Steward：大体上认同这种机制。但已有 RFC 都已经有定义了，是否还需要单独发布一篇文稿？对之前的 RFC 增加简单文字描述即可。Balazs 回复这篇文稿的目的就是要澄清下这种机制。

David：支持 stewart 的 comments。

主席建议后续进行邮件列表讨论。

Toerless 邮件列表补充：认为 IP+UDP 提供 PREOF 方案是一种短期 IP over MPLS 的变通方案。希望成立 DT。也同时对 PEF，通过 HbH 携带有界时延所需的序列号和时延参数、流量聚合提了一些讨论意见。

Packet Ordering Function

Presenter: Balázs Varga

Draft: https://datatracker.ietf.org/doc/draft-varga-detnet-pof/

Toreless：认为在设计 POF 时要考虑对 buffer 的时延影响

Lou 认为通过 informational 的文稿来讨论 implementation 的细节的做法很好，对工作组有用，表示支持。

Requirements of large scale deterministic network

Presenter: Peng Liu

Draft: https://datatracker.ietf.org/doc/draft-liu-detnet-large-scale-requirements/

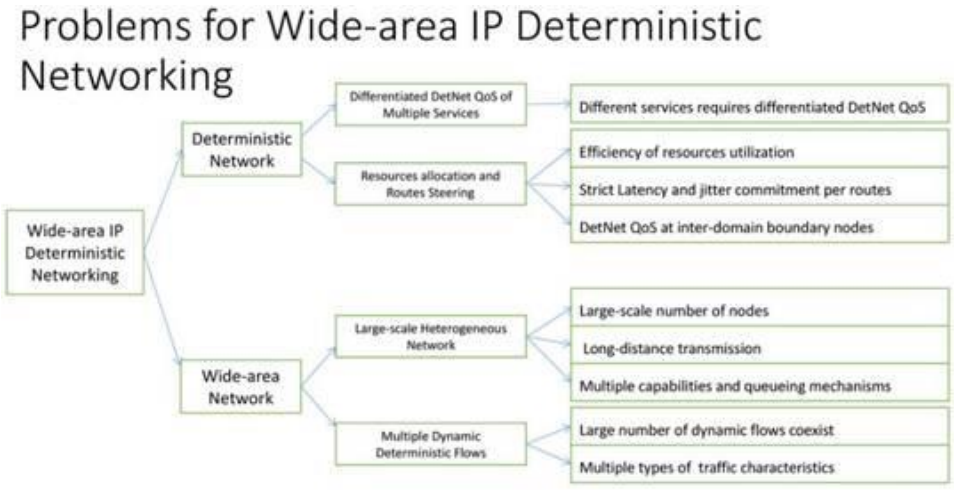
Lou：认为应该去掉后面的方案对比内容，只保留需求。

Janos 询问为什么要有新的 00 稿，与替换的文稿的关系。

The Requirements for Wide-area IP Deterministic Networking

Presenter: Quan Xiong

Draft: https://datatracker.ietf.org/doc/html/draft-xiong-detnet-wide-area-ip-requirements



移动刘鹏建议不在需求文稿中体现具体琐碎的需求，同时询问两篇需求文稿的下一步计划。主席建议可以借机进行讨论，看是否进行文稿合并。

Micro-burst Decreasing in Layer3 Network for Low-Latency Traffic

Presenter: Zongpeng Du

Draft: https://datatracker.ietf.org/doc/draft-du-detnet-layer3-low-latency/

现场没有提问。

DetNet Data Plane - MPLS TC Tagging for Cyclic Queuing and Forwarding

Presenter: Toerless Eckert

Draft: https://datatracker.ietf.org/doc/draft-eckert-detnet-mpls-tc-tcqf/

Janos 认为需要先定义需求，后讨论方案。感觉试图拖延这项工作。

Lou：可以在修改 charter 的同时进行方案文稿的文字准备，在下次会议时有个较成熟的文稿。相对激进的在推动 queuing 的工作。

BGP Flow Specification for DetNet Flow Mapping

Presenter: Quan Xiong

Draft: https://datatracker.ietf.org/doc/html/draft-xiong-idr-detnet-flow-mapping-00

Jeffrey 建议根据 Flowspec 2.0 的要求同步修改本文稿的内容。

Loud 建议文稿从标题到内容，都明确说明是 TSN 到 DetNet 的 mapping，而不是通用的 detnet mapping。建议在 IDR 进行讨论。

2. QUIC

QUIC 工作组总体情况：

基础协议在今年 5 月发布 RFC 后，工作组目前主要讨论的技技术方向仍然围绕基础协议的优化和负载分担以及基于协议的运维和开发等。包括 MultiPath、LB、Qlog、Manageability 和 Applicability 等。

1. RFC 8999/9000/9001/9002 已于 5 月份发布

2. 即将 RFC 发布的有 5 篇，具体如下：

draft-ietf-quic-http-34 Hypertext Transfer Protocol Version 3 (HTTP/3)

draft-ietf-quic-qpack-21 QPACK: Header Compression for HTTP/3

draft-ietf-quic-manageability-13 Manageability of the QUIC Transport Protocol

QUIC 传输协议的可管理性， 重点关注影响 QUIC 的网络运营的注意事项，流的网络可见、特定的网络管理任务（处理 ICMP 消息、性能与故障测量、NAT 相关、DDoS 检测和缓解等）

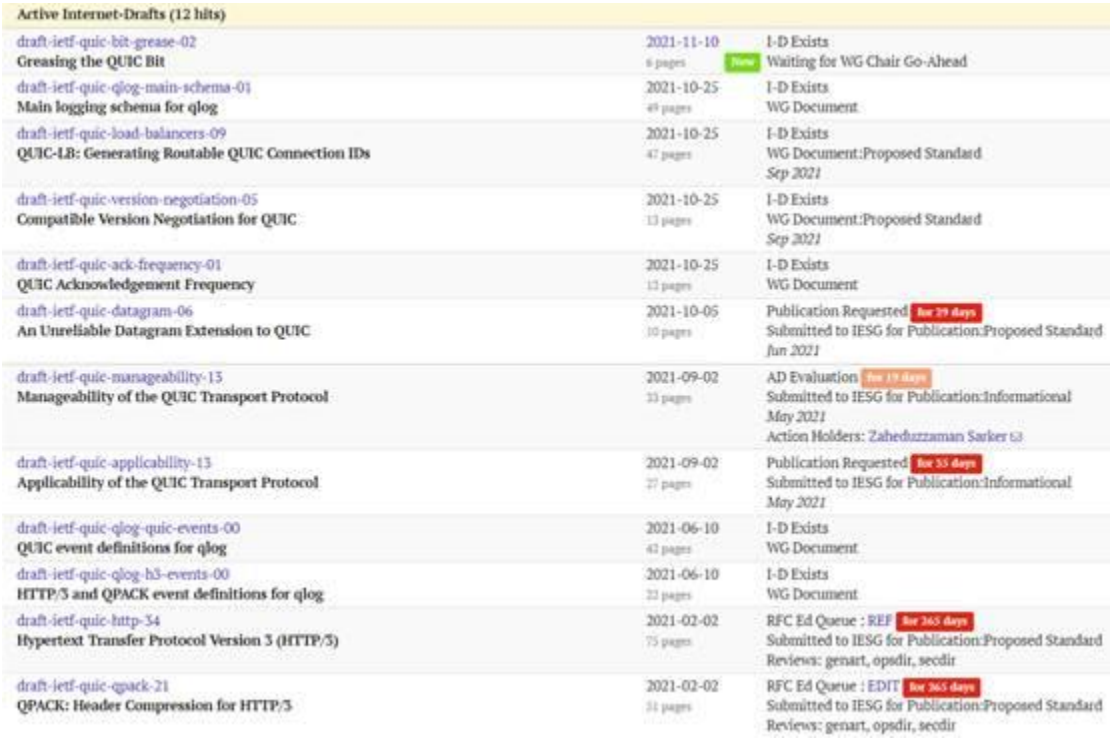
draft-ietf-quic-applicability-13 Applicability of the QUIC Transport Protocol

本文档为有需要的应用程序开发人员提供指导使用 QUIC 协议而无需自行实现，如版本如何回退等

draft-ietf-quic-datagram-06 An Unreliable Datagram Extension to QUIC

提供一种支持不可靠传输的手段，譬如针对实时数据

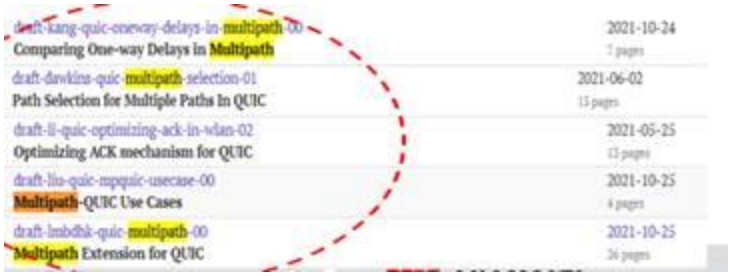
3. 当前工作组文稿如下图所示，本次会议 Topic 有个，ack-frequency，manageabilit、qlog， version-negotiation、multipath、load-balancers、 ACK_RECEIVE_TIMESTAMP extension，其中 Load-balancers 和 Multipath 为主要关注点。



Active Internet-Drafts (12 hits)		
draft-ietf-quic-bit-grease-02 **Greasing the QUIC Bit**	2021-11-10 6 pages New	I-D Exists Waiting for WG Chair Go-Ahead
draft-ietf-quic-qlog-main-schema-01 **Main logging schema for qlog**	2021-10-25 49 pages	I-D Exists WG Document
draft-ietf-quic-load-balancers-09 **QUIC-LB: Generating Routable QUIC Connection IDs**	2021-10-25 47 pages	I-D Exists WG Document:Proposed Standard *Sep 2021*
draft-ietf-quic-version-negotiation-05 **Compatible Version Negotiation for QUIC**	2021-10-25 13 pages	I-D Exists WG Document:Proposed Standard *Sep 2021*
draft-ietf-quic-ack-freqaency-01 **QUIC Acknowledgement Frequency**	2021-10-25 12 pages	I-D Exists WG Document
draft-ietf-quic-datagram-06 **An Unreliable Datagram Extension to QUIC**	2021-10-05 10 pages	Publication Requested for 29 days Submitted to IESG for Publication:Proposed Standard *Jun 2021*
draft-ietf-quic-manageability-13 **Manageability of the QUIC Transport Protocol**	2021-09-02 33 pages	AD Evaluation for 19 days Submitted to IESG for Publication:Informational *May 2021* Action Holders: Zaheduzzaman Sarker (s)
draft-ietf-quic-applicability-13 **Applicability of the QUIC Transport Protocol**	2021-09-02 27 pages	Publication Requested for 55 days Submitted to IESG for Publication:Informational *May 2021*
draft-ietf-quic-qlog-quic-events-00 **QUIC event definitions for qlog**	2021-06-10 42 pages	I-D Exists WG Document
draft-ietf-quic-qlog-h3-events-00 **HTTP/3 and QPACK event definitions for qlog**	2021-06-10 22 pages	I-D Exists WG Document
draft-ietf-quic-http-34 **Hypertext Transfer Protocol Version 3 (HTTP/3)**	2021-02-02 75 pages	RFC Ed Queue : REF for 365 days Submitted to IESG for Publication:Proposed Standard Reviews: genart, opsdir, secdir
draft-ietf-quic-qpack-21 **QPACK: Header Compression for HTTP/3**	2021-02-02 51 pages	RFC Ed Queue : EDIT for 365 days Submitted to IESG for Publication:Proposed Standard Reviews: genart, opsdir, secdir

4. 另外 QUIC 个人草案以及相关的草案也比较活跃 111 会议以来有 20 篇进行了刷新，主要动向为： Multipath 相关草案活跃，以及新增 SRT（The Secure Reliable Transport (SRT) protocol）over quic 的草案。其他 Over quic 草案包括：draft-sharabayko-srt-over-quic-00 、 draft-chen-bgp-over-quic-00 ， draft-dai-netconf-quic-netconf-over-quic-00 、 draft-engelbart-rtp-over-quic-00、draft-hurst-quic-rtp-tunnelling-01、draft-pardue-

quic-http-mcast-08 Hypertext Transfer Protocol (HTTP) over multicast QUIC、draft-kang-quic-apps-multiplexing-a-session-00（CBG 提交）等



议题宣讲：

draft-ietf-quic-ack-frequency-01

内容：QUIC 确认频率，草案定了协议扩展，协商 ack 确认延迟的能力。接收者确认收到的数据包，但它可以延迟发送这些确认。确认的延迟会影响数据发送方的连接吞吐量、丢失检测和拥塞控制器性能，以及数据发送方和数据接收方的 CPU 利用率。

会上讨论：主要争论点，

1) 算法代价：这样需要实现一个新算法，稍微增加了实现成本。

2) 方法讨论：你建议的根据数据包计数添加重新排序阈值。我认为这不是正确的工具。在多路复用场景中，特别是等价多路复用（ECMP），重排序经常发生。使用延迟而不是数据包计数更有意义。

3) ACK 延迟争论：文档中描述主要是针对“如果出了什么事，请迅速开火”，但仅仅靠紧密观察 PN 的变化，在实际中很难使用，因为 PN 的损失大小随 CWND 大小而变化，还取决与发送者的号码是否跳过。因此不仅仅要考虑 ACK 延迟还要考虑 ACK 重新排序的延迟。

4) 需要添加细节描述以及背景描述，尤其是讨论的设计问题

5) 安全问题需要另行讨论

Version Negotiation

主要内容： 版本协商机制，允许客户端和服务器 选择相互支持的版本。Version Negotiation 报文由 server 发送：当 server 接收到 client Initial 报文时，如果发现 client 指定了不支持的 version，可以响应 Version Negotiation 报文，要求 client 执行 version negotiation 过程。

如果互相通告的原始版本可以兼容，则无需再次往返协商产生往返额外开销。

在 21 年 4 月份内部讨论定调后，7 月份 111 会议对 VN 的修改：保持兼容和不兼容的流程设计。

112 会议讨论： 技术上未做讨论，建议能给获得一些实施的性能经验，以证明版本协商机制确实是有效果的。

Load Banlance

草案内容：针对 client Server 的流量定义了一种负载分担的实现方法。

1、QUIC 不希望中间观察者识别出流量（linkability），因此，使用了可变的 CID

2、但是，LB 等中间设备，基于指定的 QUIC 流工作上述二者的要求是矛盾的。

在 client 和 server 上，连接建立后，只需要使用 CID 来唯一识别连接。

在运行过程中，二者都可以通过 NEW_CONNECTION_ID 帧（加密传输）向对方通告未来可以使用的 CID

LB 通过某种某种算法来了解 server 通告给 client 的 CID（称为 routable Connectin ID），从而识别出 client-->server 流量

112 会议讨论：

1) 针对流密码，密钥旋转的东西未来一年内会考虑细化和部署

2) 关于互操作性主席建议：文档是以可实施的方式编写的。在实际部署中，尝试部署此功能并进一步开发配置模型将是非常好的。谷歌为此部署将有所帮助。Nick Banks 也曾为此研究过 Azure，但很难从他们那里获得这方面的反馈。

Unifying the Multipath extensions draft-lmbdhk-quic-multipath.

草案内容： 阿里巴巴牵头，合并了 3 篇草案（draft-deconinck-quic-mulitpath-07, draft-liu-multipath-quic-04,draft-huitema-quic-mpath-option-01），内容包括多路径功能的协商、多路径的启动、关闭、超时管理，报文的重传以及基本的调度等。 其他细节：a，允许在多路径上同时传输非探测帧；b，在某路径（非当前正在传输使用的路径）上收到非探测帧，原路径仍然被使用。C，支持对已废弃路径的管理。

另外草案对传输报文的 Sequence Number 等进行了讨论，如是否所有路径使用同一空间或每条路径单独编号等。双方在开始要协商多路径的能力。如果对端不支持多路径，则需回退到单路径模式。 相对 RFC9000，将“migration”替换成了“simultaneous use”

112 讨论：

1) Ack 在什么路径发送： 路径是由四元组（双向）定义的，接收器是否只需要在接收被确认数据包的路径上发送 ACK？答：不，只是你可以在那条路上收到。如何确认数据包，目前留给实现。不需要在接收数据包的路径上发送 ACK。草案非常清楚地规定了 ACK 可以在任何路径上发送。

a. 继续问：当保留每路径 ACK 队列时，只能在不同路径上 ACK 数据包。单 PN 空间意味着只有一条路径上的 ACK。

b. 目前，ATSS/3GPP 对添加 mpquic 有支持。

2) 单一 PN 和多 PN 是争论焦点，也是未来一个主要的待设计问题，现场也颇多争论。包括：MPDCCP 实现时，发现多 PN 有助于区分接收端丢失的数据包和延迟的数据包。如果数据包需要重新排序，这就变得很重要了。 单一 PN 还是多 PN 对协议可能影响较大，需要后续仔细讨论。

3) 协议效率：草案中是否有关于协议效率的设计原则？例如，mpquic 至少也应该表现得很好？澄清这一点，将有助于推动一些设计选择。 答案是没有。

4) 最后表决通过，quic wg 应该针对 mppath 进行讨论 53/168。草案是否通过 46/167。

其他 Multipath 草案：

draft-liu-quic-mpquic-usecase-00　Multipath-QUIC Use Cases Alibaba

草案内容：讲解了多路径的几个 Usecase， 包括： 冗余传输、带宽聚合、5G 核心网中的应用（带宽）

冗余传输： 多发选收---对于互联网视频直播等应用，用户体验对延迟非常敏感。尤其对于户外网络视频直播，直播设备可以多配备两张手机卡，以实现稳定、健壮的网络连接。

带宽聚合：对于文件下载等应用，如果设备有多个网络接入，例如现在大多数智能手机都有 Wi-Fi 和蜂窝网络接入，多路径 QUIC 可以用于带宽聚合以加快下载速度。

核心网： 需要 5GS 来扩展 应用的带宽，例如高分辨率视频流。为了达到 这个目的，应用程序可以通过不同的 RAN 接入，例如来自 PLMN 的不同无线接入。由于 5GS 只能支持 TCP 的多路径，不能支持多路径的非 TCP 流量功能，因此迫切需要 多路径传输协议对于非 TCP 流量。

draft-dawkins-quic-multipath-selection-01　Path Selection for Multiple Paths In QUIC Tencent America LL

主要内容：1. 针对一个连接多条路径的时候，如何选择路径(主备、延迟与带宽、负载均衡、最小 RTT 差异、往返时间差异、优先级。。。。)。 2. 选择了路径后，如何平滑迁移

draft-kang-quic-oneway-delays-in-multipath-00　Comparing One-way Delays in Multipath　华为 CBG

提案背景：

A. Oliver 教授提出了一种 ” all-uniflow ” （uniflow： unidirectional flow， 单向流） MPQUIC 方案， 在这种设计下，数据包和 ACK 可能走不同的路径；

B. 当前单径 QUIC 中的 RTT 测试方案（要求数据包和 ACK 耦合在同一路径中）在这种 ” all-uniflow” MPQUIC 场景中无法发挥作用。

C. 在 1 和 2 下，提案建议：在 MPQUIC 会话中，通过双端交互 专用的单向时延测试帧，协助数据发送方获取 备选的单向流的单向时延排序，为数据调度提供参考。

3. NMRG

整体情况与会议总结：

本次 NMRG 会议约 50 人参会。会议讨论的热点主要是 IBN use case 和数字孪生网络。目前该研究组两篇文稿（intent 概念和定义文稿与 intent 分类文稿）均处于 IRTF chair review 流程。

个人文稿数字孪生网络概念与架构文稿预计不久后会发起 call for adoption。NMRG 本次有几篇 00 稿新工作，其中包括华为联合中国移动提出的 flexible IP 在数字孪生网络中的应用文稿（draft-li-nmrg-dtn-addressing-protocols-00）、NICT 联合 NTT 与 Telefonica 提出的 AI framework 文稿（draft-pedro-nmrg-ai-framework-00）、Telefonica 的 Luis 提出的基于 RFC8597 的计算和数据感知的 SDN 分层架构演进文稿（draft-contreras-nmrg-clas-evolution-00）与 SANGMYUNG UNIVERSITY 提交的基于 B5G 的自主安全和基于持续安全质量保证框架文稿（draft-kim-nmrg-nnmb5g-00）。

会议相关链接：

Materials: https://datatracker.ietf.org/meeting/112/session/nmrg

Meetecho:
https://meetings.conf.meetecho.com/ietf112/?group=nmrg&short=&item=1

Notes: https://codimd.ietf.org/notes-ietf-112-nmrg

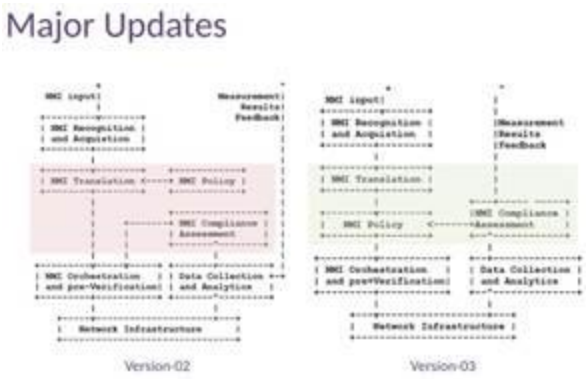
Video recording: https://www.youtube.com/user/ietf/playlists

* IBN draft status (20 min)

Network Measurement Intent, Kehan Yao, 5min + 5min Q&A

https://datatracker.ietf.org/doc/draft-yang-nmrg-network-measurement-intent/

中国移动主推的网络测量意图个人文稿，作为 IBN 的 use case 之一，网络测量的整体目标是让系统能够自动监控网络状态，基于历史数据做自主学习，判断当前网络状态是否繁忙，在繁忙时能够自主做一些网络部署，而不需要人工干预。本次上会主要讨论文稿更新，并请求研究组接纳。主席 Laurent 认为关于 IBN 的 use cases 系列文稿目前已经有 3-4 篇，可以考虑协同合并。



Hackathon 主席 Charles Eckel， OPS 域 AD Rob 以及 Benoit Claise 则分别给出了一些相关文稿认为可能会引起作者的兴趣。

Charles Eckel

This draft in MEF may be of interest to the authors https://www.mef.net/resources/mef-1...rvice-readiness-testing-for-sd-wan/

Robert Wilton

I might be helpful if this document was to reference https://datatracker.ietf.org/doc/draft-ietf-opsawg-ntf/

Benoît Claise

And another related draft: https://datatracker.ietf.org/doc/dr...awg-service-assurance-architecture/ , which will need the measurement aspects.

Interconnection Intents, Luis Contreras, 5min + 5min Q&A

https://datatracker.ietf.org/doc/draft-contreras-nmrg-interconnection-intents/

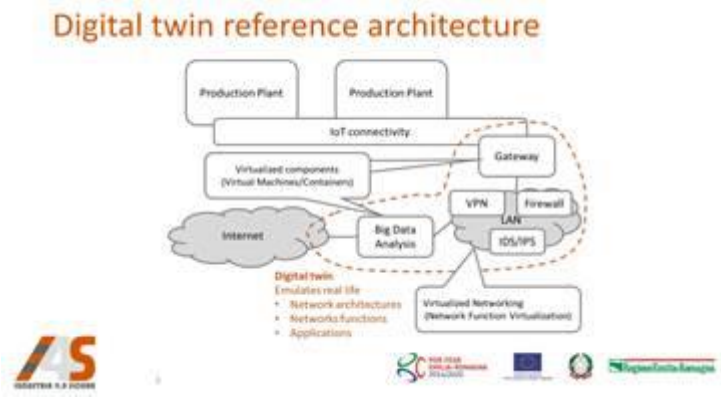
Telefonica 与 NTT 联合推动的网络互联意图个人文稿。传统基于 BGP 的 IP 流量互联存在一定的局限性，难以适应网络可编程性和虚拟化程度提高，多域互联提供服务需求趋势变得明显，网络互联意图的目的主要包括：多域网络服务编程；通过广播多域的计算和存储资源，实现 VNF 的跨域部署；实现跨多域的业务计费。

主席 Laurent 回应后续可能考虑邀请感兴趣的参与者举办一次专门的临时会议讨论 use case 和期望的输出结果，并考虑是否有不同的 use case 之间协同的可能。

* Digital twins (60 min)

Digital Twins for Industrial IoT Networking, Chiara Grasselli, 20min + 5min Q&A

来自意大利博洛尼亚大学的 Franco 的 phd student 宣讲数字孪生在工业 IoT 网络中的应用宣讲并给出 demo 演示。主要的讨论问题在于主席 Laurent 询问工业 IoT 网络怎么跟孪生网络建立连接，如何交互。中国移动 Cheng Zhou 则询问是否有对孪生网络进行性能测试，能够支持大规模部署。



An Efficient Data collection method for Digital Twin Network, Yanhong Zhu, 10min + 5min Q&A

https://datatracker.ietf.org/doc/draft-zhu-nmrg-digitaltwin-data-collection/

中国移动提出的在数字孪生网络中关于数据采集，聚合和关联的架构和方法。介绍了一种高效的数据采集方法：数字世界发送采集数据的指令给物理世界，物理世界解析并执行指令。主席 Laurent 询问孪生世界需要和物理世界保持多大程度上的一致性和同步，数据采集方法不应当是单一的。孪生网络需要什么数据，采集什么，什么时候采集，有没有相关的一些研究。中国移动的 Cheng Zhou 作为这篇文稿的 coauthor 则澄清这不在草案的 scope 范围之内；而 Orange 的 Mohamed Boucadair 则认为孪生世界和物理世界的复制和映射程度需要取决于应用的需求，比如如果应用用于做数据训练或验证场景，不需要和物理网络的实时数据采集和同步。

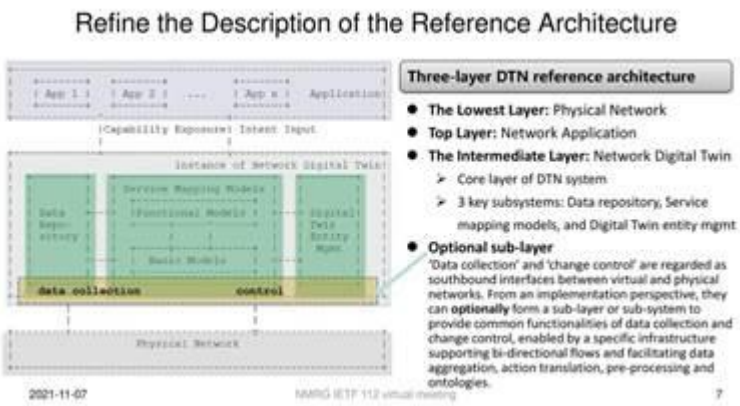
Digital Twin Network: Concepts and Reference Architecture, Cheng Zhou, 10min + 10min Q&A

https://datatracker.ietf.org/doc/draft-zhou-nmrg-digitaltwin-network-concepts/

中国移动联合 Telefonica，华为和 Orange 一起推动的数字孪生网络概念与架构文稿，该文稿是本次会议讨论的热点。本次由中国移动的 Zhou Cheng 宣讲，主要澄清草案更新，并申请研究组的接纳。主席曾在会议之前征求大家意见，希望研究组 review。预计 IETF 会后主席会在邮件列表发起正式的 call for adoption。

本次会上的讨论包括，Rick Taylor 认为 DTN 作为” Digital Twin Network”的缩写不太合适，DTN 已经分配给了"Delay Tolerant Networks"。

美研的 Kiran Makhijani 询问物理世界是否可以映射为多个孪生世界，草案作者们则给出澄清物理世界和孪生世界的映射可以是 1 对 1 或 1 对多。



* Other topic (15 min)

Artificial Intelligence Framework for Network Management, Pedro Martinez-Julia, 10 min + 5min Q&A

https://www.ietf.org/archive/id/draft-pedro-nmrg-ai-framework-00.txt

来自 NICT，同时也是作为 NMRG 组的秘书 Pedro 与 NTT 和 Telefonica 的 Diego 一起提出的 00 稿文稿。提出将 AI 应用于网管的架构 AINEMA，用于设计，部署，实例化，验证 AI 解决方案。

该架构的主要要素有：

1）data framework，负责数据获取，建模，存储，分发。可以是离线采集的历史数据，也可以是在线采集的实时数据。

2）AI modules，具体的 AI functions

3）AI Hub，接收 AI modules 的数据，执行决策并输出需要对网元进行的动作建议，管理 AI modules 的生命周期

该架构执行一系列复杂的管理操作，包括：数据采集，推理，求解，规划。

该次上会主要收集到来自华为的 Olga Havel 的一条意见，认为该架构和 IBN 的架构之间的界限不够清晰。

4. NETCONF

会议总结：

本次 NETCONF 工作组申请了 1 个小时的讨论时间，参会人数达到 50 人左右。主要讨论的议题包括 UDP 上送，变频采集文稿，Tail-f 提出的基于 transaction-ID 的多事务并发管理机制，以及分页管理。

Introduction

Chairs (10 minutes) Session Intro & WG Status

主席介绍工作组草案进展和 Agenda。YANG push notification capability(https://datatracker.ietf.org/doc/draft-ietf-netconf-notification-capabilities/)文稿进入发布流程。client-server 系列文稿完成 WG Last Call，目前还有个别遗留问题没有解决。IEEE802.1 安全组关于 YANG Keystore(https://datatracker.ietf.org/doc/draft-ietf-netconf-keystore/)文稿提出一些 review 意见，Rob 提出会后通过会议交流沟通。HTTP-notif(https://datatracker.ietf.org/doc/html/draft-ietf-netconf-https-notif) 草案已经解决 WGLC 过程中的所有 Open Issues,主席认为可以进入发布流程。

Chartered items:

UDP-based Transport for Configured Subscriptions (10 min)

https://datatracker.ietf.org/doc/html/draft-ietf-netconf-udp-notif-04

Discussion Leader: Alex Huang Feng

INSA 的 Alex 宣讲的 UDP 上送文稿本次上会主要讨论文稿的更新状态，加入 DTLS 支持和安全考虑等其他更新。UDP 上送文稿主要聚焦数据通道采用 UDP 时上送格式的定义，与分布式数据采集订阅文稿配合形成解决方案。本次会议讨论的遗留问题主要在于，AD Rob 表示安全域 AD 对于直接允许未经加密的 UDP 通道上送数据有一定顾虑，并且还需检查文稿是否考虑了拥塞控制等传输问题。另外主席 Mahesh 给出两条 comments，1）文稿中提到要设置 transmission timeout 的值，但 YANG 模型中并没有相关配置定义，需要文稿作者进一步确认；2）YANG 模型中并未设置 UDP 端口号，UDP 上送时端口号如何确定，文稿作者来自 INSA 的 Pierre Francois 澄清采用默认值即可。

Non-Chartered items:

Adaptive Subscription to YANG Notification (10 mins)

https://datatracker.ietf.org/doc/html/draft-wang-netconf-adaptive-subscription-07

Discussion Leader: Qiufang Ma

华为主导的变频采集文稿，本次上会主要解决 IETF111 会议 AD Rob 提出的认为通过任意的 XPath 作为变频采集策略中的条件表达式的设计过于复杂的遗留问题，本次更新中新增一个章节讨论 Xpath 表达式的复杂性，给出一些设计建议降低实现复杂度，如只对某些节点采用 Xpath 过滤，只支持数值型单 leaf 节点比较。AD 指出这种方式是可行的，但仍需要考虑设计一个错误码用于当 server 接收到无法解析的 Xpath 条件表达式时的响应。主席 Kent Watson 提到在分页机制文稿中也用到了任意的 Xpath，server 端如何告知 client 端关于 Xpath 解析复杂度的支持能力可能是一个共同问题。该文稿预计会后会发起 call for adoption.

Transaction ID Mechanism for NETCONF (10 min)

https://datatracker.ietf.org/doc/html/draft-lindblad-netconf-transaction-id-01

Discussion Leader: Jan Lindblad

基于 TransactionID 的多事务并发管理机制，当 NETCONF 客户端和服务器连接时，有时需要知道自从上次连接后哪些配置发生了更改；或者当多客户端并发访问服务器时，如何借鉴 RESTCONF 的 Etag 防冲突碰撞思想，提升配置更新效率。本次上会主要澄清继 00 稿后的一些更新，并梳理 open issues，比如是否支持 client 端分配 Etag，Etag 的粒度是基于数据集还是 container 和 list 等。主席建议将 open issues 放到邮件列表讨论。华为 Benoit 支持由 client 端分配 EtagID，他指出在多个 client 端与同一个 server 交互时，可以通过 EtagID 来标识不同服务请求，便于故障溯源。该文稿作者 Jan Lindblad 后续可能会向工作组申请召开一次专门的中间会议讨论该工作。

List Pagination for YANG-driven Protocols (20 mins)

https://datatracker.ietf.org/doc/html/draft-wwlh-netconf-list-pagination-00

https://datatracker.ietf.org/doc/html/draft-wwlh-netconf-list-pagination-nc-02

https://datatracker.ietf.org/doc/html/draft-wwlh-netconf-list-pagination-rc-02

Discussion Leader: Qin Wu

当使用 NETCONF/RESTCONF 的传统方式对 server 内数据进行提取时，不可避免的会存在需要提取的 list 中的存在大量符合检索条件的条目。当加载的整个 list 中的对象超过 10000 时，加载时间、内存消耗、crashes 等都是很大的问题。分页工作用于实现超长 list 或者 leaf-list,嵌套 list 条目高效数据检索，定义了以下查询参数：

1. where，使用 Xpath 表达式对查询结果进行过滤；

2. sort-by, 按照哪个节点标识的值进行排序；

3. direction，跟 sort-by 配合使用，有 forwards 和 backwards 两个选择；

4. offset，从 list 或 leaf-list 的第几个元素开始返回；

5. limit，返回记录条数

6. sublist-limit 用于限制 list 的子 list 或 leaf-list 的返回记录条数

主要涉及三篇文稿，通用参数定义，RESTCONF 协议扩展支持分页和 NETCONF 协议扩展支持分页。由于时间关系，该工作没有展开讨论，主席建议将 open issues 放到邮件列表讨论。

5. ALTO

本次 ALTO 工作组会议申请了 2 个小时，参会人数达到 45 人，主要参会单位包括中国移动，法国电，腾讯，华为，德电，Telefonica, Benocs, 三星，耶鲁大学，南京大学，阿里巴巴，微软，诺基亚，中国科技大学，同济大学，四川大学，

F5，Facebook, Interdigital，NetAPP，爱立信等，传输域两位 AD，IETF 主席 Lars,TCPM 工作组主席 Michale 也参与了会议的讨论。本次会议主要讨论的焦点是 ALTO OAM, ALTO 新传输，以及收集到的两个部署相关的议题，分别是 G2 和 Benocs 的 Flow Director。AD 对 Benocs Flow Director 的部署和实现表示了感谢；同时本次会议还 review 了 ALTO 新 charter,对两篇 ALTO 工作组草案遗留问题做了闭环讨论，还邀请了微软研究院，中移，Telefonica 讨论部署实现相关的议题，分别是微软的带宽估计，中移的计算感知网络，Telefonia 的 NEF。

Chartered items:

ALTO OAM Support (20 minutes)

https://tools.ietf.org/html/draft-zhang-alto-oam-yang-00

Discussion Leader: Jensen Zhang/Dhruv Dhody

来自同济大学 Jensen Zhang 代表草案作者宣讲了该草案，草案作者包括华为 Dhruv Dhody, 德电 Roland Scott, 四川大学 Gao Kai.

本次会议首次上会，会上 Richard 提出计算业务 map 的复杂性的问题，主要争议是 ALTO OAM 模型是否需要讨论如何计算业务 map,还是由指定 OAM 系统如何提取数据和存储数据；Martin 指出 ALTO Client 配置目前不在 ALTO OAM 建模范围内是一种好事，需要考虑跨域问题是否在范围内；Martin 对于 ALTO 客户端是否支持 NETCONF 客户端表示个人的质疑，会上还讨论了 TLS 不同版本支持问题，达成的主要共识是不定义具体版本；Telefonica Luis 指出 Telefonica 已经实现了 BGP，BGP-LS 与 ALTO 的集成。

ALTO over HTTP2 (15 minutes)

https://tools.ietf.org/html/draft-yang-alto-http2-transport-01

Discussion Leader: Richard YANG/Roland Scott

本次会议来自耶鲁大学 Richard 宣讲了 ALTO over HTTP2 设计思路，该草案也是首次宣讲，该草案作者包括来自腾讯的熊春山，来自德电的 Roland Scott，来自 Benocs 的 Danny. Martin 认为草案初始设计方向是对的，但是建议不要定义 Multi-streaming head-aligned block 新的机制，可以聚焦如何利用在 H2，H3 可以提供哪些 API 上；

Deployment experience Update:

G2 and ALTO integration (20 minutes)

https://tools.ietf.org/html/rfc7971

Discussion Leader: Kai Gao

本次会议由 Gao Kai 牵头讨论了 G2 和 ALTO 融合问题;在 ALTO 会议之前，Richard 邀请了 G2 团队到耶鲁大学，专门讨论 ALTO 和 G2 合作问题，得到 G2 团队的支持，不过本次会议由于 G2 作者企业公司存在 IPR 问题的困惑，他们暂缓上会，会后重启下一步合作讨论。

本次会议主要讨论 G2 部署状态和后续计划，包括 G2 在中国 CERN 网络，Google 网络的部署，Richard 澄清会和 G2 团队确认，并给与回复。来自 TCPM 主席 Michael 提出一个应用场景问

题，即如何应用这些快速变化的拥塞信息，会议达成的共识是在 SDN 控制器网络优化场景可以用到。

ALTO Implementation Update: Flow Director (15minutes)

https://tools.ietf.org/html/rfc7971

Discussion Leader: Danny Alex Lachos Perez

来自 Benocs 的 Danny 宣讲了该议题，主要是分享了 Benocs ALTO 部署实践，Martin 对 Benocs 部署非常赞赏，认为对于后续的 Charter 意义非常重大，Adrian 提了一个关于 out of band BGP 应用细节问题，Danny 指出可以通过 BGP 通告服务器前缀，基于 BGP Community 携带 Cluster ID。

Non-Chartered items:

Considering ALTO as IETF Network Exposure Function (10 7 minutes)

https://datatracker.ietf.org/doc/html/draft-contreras-alto-ietf-nef-00

Discussion Leader: Luis M. Contreras

来自 Telefonica Luis 代表 Telefonica 和腾讯宣讲了 IETF ALTO NEF 议题，会上主要讨论 ALTO NEF 和 3GPP NEF 关系，如何交互问题，以及澄清 ALTO internal applcation,主要达成的共识是 ALTO NEF 和 3GPP NEF 是互补的，ALTO NEF 聚焦 underlay, 3GPP NEF 聚焦 overlay,两者可以协同，协同的接口可以是 ALTO 接口，ALTO internal applciation 主要是指明是否和 ALTO 在相同的管理域。

Compute aware network Use Case (10 7 minutes)

https://datatracker.ietf.org/doc/html/draft-liu-alto-can-usecase-00

Discussion Leader: Peng Liu

来自中国移动刘鹏宣讲了计算感知网络，中国移动在 ITU-T 也布局了计算感知网络的需求，目前正在 IETF 推动计算感知网络的架构，接口，应用场景，本次会议在 ALTO 工作组，刘鹏主要探讨了计算感知网络架构与 Dyncast, CFN 有密切的关系，同时也探讨了与 ALTO 框架的结合点，由于时间问题，建议中国移动在 ALTO 邮件列表发起讨论，征集兴趣和输入。

Bandwidth Estimation on OpenNetLab (10 7 minutes)

Discussion Leader: Zhixiong Niu

来自微软研究院的 Niu Zhixiong 代表南京大学 OpenNetLab 宣讲了一个 Bandwidth Estimation 应用场景，会上主要受到来自阿里和耶鲁大学两个问题，一个是带宽估计如何计算，采样周期和频率大概是什么范围，Niu 分别回答了两个问题，主要是通过日志数据比较，来估算带宽变化，采样频率大概是 100ms~200ms 范围。

6. OPSAWG

工作组进展

codimd: https://codimd.ietf.org/notes-ietf-112-opsawg

工作组状态：

TACACS+ YANG 发布 RFC 9105

Editor queue:

• draft-ietf-opsawg-ipfix-mpls-sr-label-type

• draft-ietf-opsawg-l3sm-l3nm

• draft-ietf-ospawg-vpn-common

IESG：

• draft-ietf-opsawg-ntf

WGLC:

• draft-ietf-opsawg-l2nm

新 WG：

• draft-ietf-opsawg-ol MUD file 版权和 owner

• draft-ietf-opsawg-pcap packet capture 捕获文件格式

会议讨论

SAIN (Service Assurance for Intent-based Networking)

Benoit Claise

Draft: https://datatracker.ietf.org/doc/draft-ietf-opsawg-service-assurance-architecture/

https://datatracker.ietf.org/doc/draft-ietf-opsawg-service-assurance-yang/

通过在设备上建立各种功能的依赖图，建立根因分析 Telemetry 模型。适合较为简单的网络场景，思科 Eliot 认为 IoT 网络的故障管理适用（与 AR 和 IoT 控制器相关？）。但复杂网络的复杂业务的 assurance graph 完备性很难定义。

上次会议意见是，例如依赖关系，“Link -> Interface -> Link”，如何解决根因图循环依赖问题，模型没有修改，本次增加一个空的 Top 层破坏。但 chair Joe 认为 Top 意义,RW 建议采用 Rule 来限制，而不是无端增加的 top 层，因为业务之间的依赖关系是明确的，不能随意调整。

Operational Considerations for use of DNS in IoT devices

Michael Richardson，5 minutes

https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud-iot-dns-considerations

使用 DNS 的运维问题，会建议 MUD controller 更新使用 DNS 下发 ACL 规则，而不是 IP 地址。

PCAP Next Generation (pcapng) Capture File Format and PCAP

Michael Richardson

Draft: https://datatracker.ietf.org/doc/draft-tuexen-opsawg-pcapng/

https://datatracker.ietf.org/doc/draft-ietf-opsawg-pcap/

packet capture 捕获文件格式，Henk 建议 pcap->historic，主要工作是 pcapng 的标准化。

A YANG Model for Network and VPN Service Performance Monitoring

Bo Wu

Draft: https://datatracker.ietf.org/doc/draft-ietf-opsawg-yang-vpn-service-pm/

NCE 北向模型

Med 和 Greg 提了问题，Med 建议补充一些 VPN-network-access 统计，以及基于 class-id 的 link 性能统计 metrics。

控制器获取性能统计的 OAM 方法包括有 BGP-LS，TWAMP 和 Y.1731。

Discovering and Retrieving Software Transparency and Vulnerability Information

Eliot Lear

Draft:https://datatracker.ietf.org/doc/draft-ietf-opsawg-sbom-access/

与 AR 和 IoT 控制器相关？MUD file 扩展描述设备使用的软件，以及软件的安全风险。

新草案讨论：

Data Model for Lifecycle Management and Operations

Marisol Palmero

Draft: https://datatracker.ietf.org/doc/draft-palmero-opsawg-dmlmo/

不仅仅是 NCE 和设备相关，还包括硬件，软件，功能，license 的全生命周期，包括售后管理，例如 EOL 等，工作组讨论的热点，用于管理资产的 license 和设备上的功能。这也与 Telemetry 架构也相关。

IETF 的 YANG 模型类型主要分为控制器模型和 device 模型，这个模型扩大了 YANG 模型的范围，是 Cisco support 网站提供的 API。

Transport Layer Security Verion 1.3 (TLS 1.3) Transport Model for the Simple Network Management Protocol Version 3 (SNMPv3)

Kenneth Vaughn

Draft:https://datatracker.ietf.org/doc/draft-vaughn-tlstm-update/

SNMP 更新，美国 ITS(Intelligent Transport System)智能交通系统，使用 SNMP，但 TLS1.2 有安全风险。

CISA(Cybersecurity and Infrastructure Security Agency)建议 SNMPv3 over DTLS/1.2. So this is an update to RFC 6353 to use DTLS/1.3.

SNMPv3 TLS1.3 扩展功能，AD 计划和 TLSsec 工作组联合讨论。

Soure Address Validation: Gap Analysis

Dan Li

Draft: https://datatracker.ietf.org/doc/draft-li-opsec-sav-gap-analysis/

清华大学李丹老师学生的 SAVA 文稿，但 chair 认为不在 charter 范围内。

Data Manifest for Streaming Telemetry

Benoit Claise

Draft: https://datatracker.ietf.org/doc/draft-claise-opsawg-collected-data-manifest/

设备模型

建议为 Telemetry 数据同时提供硬软件版本描述，提出了 2 YANG models for storing the context: – Platform manifest – Data manifest，建议使用 YANG instance draft 存储信息，从而呈现设备的功能差异。Eliot 和 Frank Brockners 提问如何保证信息的真实性，如果是 instance file。RW 建议引用 YANG package 描述。

Problem Statement and Requirement for Inband Flow Learning

Minxue Wang

Draft: https://datatracker.ietf.org/doc/draft-hwyh-ippm-ps-inband-flow-learning/

移动王敏学宣讲，需要大规模流量识别

A YANG Data Model for Optical Network Inventory

Italo Busi

Draft: https://datatracker.ietf.org/doc/draft-yg3bp-ccamp-optical-inventory-yang/

NCE 北向接口，光网络 inventory 管理，希望定义包括 IP 网络设备在内的 inventory。

Eloit 认为是 WG 今天的第五篇 inventory。也是一种 inventory 信息，工作组多篇草案，名字各异，SBOM, asset，menifest 等，需要 interim meeting 决定，chair 支持，需要解决 terminology 问题和是否重复。

A Network YANG Model for Service Attachment Points

Qin Wu

Draft: https://datatracker.ietf.org/doc/draft-dbwb-opsawg-sap/

NCE 北向模型，华为牵头的文稿，用于向上开放 CE-PE，ASBR-ASBR 的 AC 连接拓扑。

7. RATS

Remote Attestation Procedures Architecture

draft-ietf-rats-architecture

作者：Henk Birkholz (Fraunhofer SIT)，Dave Thaler (Microsoft)，Michael Richardson (Sandelman Softwares)，Ned Smith (Intel)，Wei Pan (Huawei)

RATS 基础架构文稿。

文稿当前状态为等待主席完成 write-up，但是由于 WGLC 后 Intel 在 8 月份声明了一个 FRAND 类型的专利影响了文稿的推进（专利作者 Ned Smith 既是文稿作者也是 RATS 主席之一）。来自 Cisco 的主席认为该类型 IPR 声明会对（开源）使用者造成影响，因此对于文稿的下一步处理需要工作组达成一致。

会上讨论中，来自微软的 Dave Thaler 建议不需要因专利阻碍文稿推进、因为专利范围不会覆盖整个架构文稿，来自 ARM 的 Hannes Tschofenig 建议考虑是否不发布此文稿、因为专利声明的太迟且 FRAND 条款对开发者非常不利。Intel 的 Ned Smith 表示 12 月份专利会公开。目前根据 AD 建议在邮件列表展开为期 3 周对于 IPR 疑虑的讨论。

Attestation Event Stream Subscription

draft-ietf-rats-network-device-subscription

作者：Henk Birkholz (Fraunhofer SIT)，Eric Voit (Cisco)，Wei Pan (Huawei)

该机制可以在设备状态发生变化时实现即时上报触发设备可信状态重新度量，有助于在对远程证明应用的相关方案中提升整体方案的安全性。

文稿在 10 月份刚刚被工作组接纳，本次宣讲回顾了文稿的目标和范围，并介绍了最新的更新情况。

A CBOR Tag for Unprotected CWT Claims Sets

https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/

作者：Henk Birkholz (Fraunhofer SIT)，Jeremy O’ Donoghue (Qualcomm)，Nancy Cam-Winget (Cisco)，Carsten Bormann (Universität Bremen TZI)

背景：RFC8392 定义了 CWT（CBOR Web Token），CWT 是要用 COSE（CBOR Object Signature and Encryption）安全机制封装 CCS（CWT Claims Set）（Claim 是一个“key/value”格式的“键值对”）。

本文稿定义了不需要用 COSE 安全机制进行保护的 CCS（UCCS，即 Unprotected CCS）。原理是通过安全通道的安全机制保护 CCS。当在安全通道（如 TLS）中传输 CCS 时，可以直接利用安全通道提供的身份认证、加密、签名等安全性保护，而不需要再使用 COSE 进行数据层的签名加密保护。

文稿在 IETF110 后被工作组接纳，本次主要讨论在文稿中增加 CDDL 描述适用于 RATS 的 UCCS。

Entity Attestation Token (EAT)

draft-ietf-rats-eat

作者：Laurence Lundblade (Security Theory LLC)，Giridhar Mandyam (Qualcomm)，Jeremy O’ Donoghue (Qualcomm)

高通、ARM 等芯片公司推的基于 CWT 格式的度量值数据模型。该度量值模型主要针对手机、IoT 等终端设备。

本文稿针对终端设备做远程证明的场景定义了描述终端设备状态和属性的 Claims，包括终端的硬件身份、软件身份、安全状态、运行情况、位置信息、密钥信息等，同时可以支持 CWT 与 JWT 封装。

该文稿目前已接近 WGLC 状态。本次主要讨论 Nested CWT 是否应该包括在文稿范围内，以及高通作者希望针对 UCCS 一并支持 UJCS（Unprotected JWT Claims Set）。同时来自微软的 Dave Thaler 提出 EAT 需要支持更多的 Claims 以满足 TEEP 工作组的诉求。为了不影响 EAT 文稿的进度，会上建议将 EAT 文稿作为基础，将这些额外的内容单独抽出一篇文稿。

Attestation Results for Secure Interactions

draft-voit-rats-attestation-results

作者：Eric Voit (Cisco)，Henk Birkholz (Fraunhofer SIT)，Thomas Hardjono (MIT)，Thomas Fossati (ARM)，Vincent Scarlata (Intel)

本文稿是对远程证明结果的标准化，有 Cisco 专利预埋。针对各种不同设备定义出统一的远程证明结果模型，才能实现对不同设备的可信度的互相认可，进而可以实现基于设备可信度的安全交互，相当于将远程证明结果当作设备的另一个“证书”。

本次更新对评估设备远程证明结果是否可信的维度（Trustworthiness Claims）进行了简化，从 Identity、Integrity、Confidentiality 三个维度定义了共 8 中 Claims。这些 Claims 准备采用 EAT Token 的方式进行封装。

Cisco 基于此文稿开发了可信路由路径 Demo，可信计算联盟 CCC 中 ARM、Intel 等联合开发了开源项目 Veraison。

本次会议同意会后发起 Adoption Call。会上高通代表提出由于不同 Verifier 自身可信度不同、其签发的远程证明结果可能会有不同的可信度。远程证明结果相当于设备的另一个“证书”，后续我们可以参考证书机制布局相关专利。

Trusted Path Routing

draft-voit-rats-trustworthy-path-routing

作者是：Eric Voit (Cisco)，Chennakesava Reddy Gaddam (Cisco)，Guy Fedorkow (Juniper)，Henk Birkholz (Fraunhofer SIT)

该文稿是 Cisco 提出的可信路由路径文稿，是对远程证明的应用，基于对路由器的远程证明结果、生成一个均由可信的路由器组成的可信路由路径。

文稿此次只针对 draft-voit-rats-attestation-results 文稿的更新而做了相应更新，计划待其完成后再申请本文稿的工作组接纳。

Attestation Sets

draft-moriarty-attestationsets

作者：Kathleen Moriarty (CIS)，Antonio Fontes (DELL)

本文稿是从安全态势评估角度出发，对设备的远程证明度量值进行分组与标签化，这样使用者可以不用了解每一项度量值细节以选择是否要验证、只需要根据需要选择度量值分组进行验证。本文稿希望针对度量值分组的命名和语义定义一个注册表。

本次会议同意会后发起 Adoption Call。

Direct Anonymous Attestation for RATS Architecture

draft-birkholz-rats-daa

作者：Henk Birkholz (Fraunhofer SIT)，Christopher Newton (University of Surrey)，Liqun Chen (University of Surrey)，Dave Thaler (Microsoft)

DAA 直接匿名验证文稿，从原本的基础交互模型文稿中拆分出的单独一篇文稿，主要介绍可隐藏 Attester 身份的一种远程证明方式。

高通代表质疑 DAA 与 RATS 的关系，以及 DAA 是 TCG 制定的、在 IETF 重新做是否有冲突。作者答复 DAA 是一种通用机制（目前是 ISO 标准），这里想要定义的是 DAA 与 RATS 架构的映射关系，相当于在 RATS 架构中实现 DAA 的解决方案文稿，另外 TCG 中 DAA 的作者也是本文稿的作者，所以可以保证不会发生冲突。另外本次会议上确认了该文稿通过工作组接纳。

Concise Reference Integrity Manifests

draft-birkholz-rats-corim

作者：Henk Birkholz (Fraunhofer SIT)，Thomas Fossati (ARM)，Yogesh Deshpande (ARM)，Ned Smith (Intel)，Wei Pan (Huawei)

该文稿是对远程证明中参考值 Reference Value 和背书 Endorsement 两个消息接口的信息模型/数据模型标准化。CoSWID 是设备软件清单，CoMID 是设备硬件清单，基于 CoSWID 和 CoMID 组合的 CoRIM 是定义设备预期的软硬件信息，包括设备的软硬件层级和关联关系。

本次会议重点介绍了当前文稿已经完善到一个比较稳定的版本，同时 CoRIM 文稿也适用于 TCG DICE、ARM PSA Token、Concise TPM-based Evidence，当前也已经开发了 demo 原型。由于时间原因会在邮件列表继续讨论是否接纳。

8. LAMPS

LAMPS 工作组主要负责证书 PKIX 体系相关的更新，以及 S/MIME 协议相关的更新。

Certificate Management Protocol (CMP) Algorithms

draft-ietf-lamps-cmp-algorithms

作者：Hendrik Brockhaus (Siemens)，Hans Aschauer (Siemens)，Mike Ounsworth (Entrust)，John Gray (Entrust)

该文稿描述了证书管理协议（CMP）中使用具体加密算法的规定。CMP 用于注册 X.509 证书和管理证书的生命周期。

已进入发布流程，AD Review 中。本次更新主要是解决 AD Review 意见。

Certificate Management Protocol (CMP) Updates

draft-ietf-lamps-cmp-updates

作者：Hendrik Brockhaus (Siemens)，David von Oheimb (Siemens)，John Gray (Entrust)

该文稿是对 CMPv2 协议（证书管理协议）的更新 CMPv3，主要是想解决原有协议的限制点，以及对密钥使用的相关扩展。

本次介绍了对 review 意见的解决情况。文稿还在继续完善中。

Lightweight Certificate Management Protocol (CMP) Profile

draft-ietf-lamps-lightweight-cmp-profile

作者：Hendrik Brockhaus (Siemens)，Steffen Fries (Entrust)，David von Oheimb (Siemens)

本文件旨在实现简单、可互操作和自动化的 PKI 管理操作，涵盖工业和物联网场景的典型用例。这是通过对证书管理协议（CMP）、相关的证书请求消息格式（CRMF）以及基于 HTTP 或

CoAP 的传输进行简明但足够详细和自洽的描述来实现的。为了使简单场景和受限设备的安全证书管理尽可能轻量化，只有最关键的操作和选项类型被指定为强制性的。更加特殊和复杂的用例也得到了支持，其特征被指定为推荐或可选。

本次介绍了文稿的更新，文稿持续完善中，接近 WGLC。

General Purpose Extended Key Usage (EKU) for Document Signing X.509 Certificates

draft-ito-documentsigning-eku

作者：Tadahiko Ito (SECOM CO., LTD.)，Tomofumi Okubo (DigiCert)，Sean Turner (Sn3rd)

RFC5280 定义了证书中 KeyUsage 以及 ExtendedKeyUsage 字段规定了证书公钥的使用场景（如数字签名、密钥协商等）。本文稿是针对 Document Signing 功能定义一个通用的 ExtendedKeyUsage OID。Document Signing 指的是对面向人的内容（例如发票）的数字签名。

本次介绍了文稿的更新情况，会后会在邮件列表发起 Adoption Call。

Clarification of RFC7030 CSR Attributes definition

draft-richardson-lamps-rfc7030-csrattrs

作者：Michael Richardson (Sandelman Softwares)，Dan Harkins (Industrial Lounge)，David von Oheimb (Siemens)，Owen Friel (Cisco)

BRSKI 中使用 RFC7030 EST 协议为接入网络的设备申请本地证书，需要在证书中嵌入设备的名称，但是原 EST 协议并没有明确可以在证书签名请求 CSR 的回复消息中包含该内容，需要更新 EST 协议。

该文稿为本次新文稿。会上主要讨论在证书签名请求 CSR 回复中扩展增加 1 个属性还是多个属性。后续将根据讨论意见完善文稿。

Algorithm Identifiers for NIST’s PQC KEM Algorithms for Use in the Internet X.509 PKI

https://github.com/seanturner/draft-turner-lamps-nist-pqc-kem-certificates

作者：Sean Turner (Sn3rd)

美国 NIST PQC Project 经过第 3 轮测试选出了几个备选的 PQC 算法，其中包括 KEM（Key Encapsulation Mechanism）算法。本文档定义了在 X.509 证书中使用这些算法，包括定义 algorithm identifier、ASN.1 编码格式、公钥和私钥的编码。

该文稿为本次新文稿。后续作者会正式提交文稿，并在工作组发起 Adoption Call。

Hybrid Non-composite Multi-certificate

https://datatracker.ietf.org/meeting/112/materials/slides-112-lamps-hybrid-non-composite-multi-certificate-00

作者：Alison Becker (NSA), Rebecca Guthrie (NSA), Daphanie Nisbeth (NSA)

美国 NSA 网络安全标准中心本次宣讲了在向后量子密码演进中的证书演进方案 Hybrid Non-composite Multi-certificate。

Hybrid Design 思想指的是同时使用传统加密算法与后量子密码算法，实现在向最终 PQ-only 方案转变过程中保持互操作性与前后向兼容性。

Composite Design 指的是将传统算法与 PQ 算法结合同时使用，基于此的 Composite Certs 即为一个证书中同时使用传统算法与 PQ 算法。Non-composite Design 指的是将传统算法与 PQ 算法分开使用，基于此的 Non-composite Certs 指的是两个证书分别使用传统算法与 PQ 算法。

使用 Composite Certs 时，优点是协议处理不需要修改，但是缺点是：1）需要定义新的组合算法 OID，2）需要增加 Composite Signature 验证功能，3）需要考虑单个算法被废弃时整个证书的有效性如何处理，4）需要额外的标准实现向 PQ-only 的演进。

使用 Non-composite Certs 方案时，优点是：1）只需要支持传统算法和 PQ 算法两种结构，密码计算过程也保持不变，2）后向兼容，支持与传统设备对接，3）支持无缝演进到 PQ-only，无需新标准。缺点是：1）需要协议逻辑修改，增加一次认证流程，2）可能需要发送重复的信息（重复消息头）。

NSA 更推荐使用 Non-composite Certs 方式实现向后量子密码算法的演进。会上讨论认为 Composite Certs 和 Non-composite Certs 可能都有适用的不同场景，例如对于 TLS 这类存在在线协商的场景 Non-composite Certs 更好，对于 Code Signing、S/MIME 等无协商机制的场景 Composite Certs 更好。LAMPS 工作组可能需要同时支持这两类方式，供具体协议选择使用。

Hybrid Composite Certificate

美国 Entrust 公司宣讲了将传统密码算法和后量子密码算法同时使用的 Composite Cert 机制中的相关文稿，包括 Composite Keys、Composite Encryption、Composite Signature。。

Composite Public and Private Keys For Use In Internet PKI

draft-ounsworth-pq-composite-keys

作者：Mike Ounsworth (Entrust)，Massimiliano Pala (CableLabs)

本文稿定义了将传统密码算法和后量子密码算法结合的公私钥对 Composite Keys，包括公私钥的数据结构格式。

Explicit Pairwise Composite Keys For Use In Internet PKI

draft-ounsworth-pq-explicit-composite-keys

作者：Mike Ounsworth (Entrust)，Serge Mister (Entrust)

本文稿定义了将传统密码算法和后量子密码算法结合并显式成对使用的公私钥对 Explicit Pairwise Composite Keys。Explicit Pairwise 指的是将两个密码算法绑定成一个显式对、用一个 OID 表示，通过该 OID 就可以知道使用的是哪两个密码算法。

Composite Encryption For Use In Internet PKI

draft-ounsworth-pq-composite-encryption

作者：Mike Ounsworth (Entrust)，John Gray (Entrust)，Serge Mister (Entrust)

本文稿定义了使用多个传统密码算法和后量子密码算法进行数据加密的 Composite Encryption 机制，包括 composite encryption data 数据结构格式。

Composite Signatures For Use In Internet PKI

draft-ounsworth-pq-composite-sigs

作者：Mike Ounsworth (Entrust)，Massimiliano Pala (CableLabs)

本文稿定义了使用多个传统密码算法和后量子密码算法进行签名的 Composite Dual Signatures 机制，包括签名值、签名参数的数据结构格式，生成签名与验证签名的处理流程。

9. SAAG

SAAG 是安全域开放会议，主要是 AD 组织安全域各个工作组汇报进展，以及讨论一些开放性问题。本次会议上安全域 AD 邀请了美国 NIST 的 Dustin Moody 来宣讲 NIST PQC Project 项目的背景与进展情况。

Update on NIST PQC Project

https://datatracker.ietf.org/meeting/112/materials/slides-112-secdispatch-saag-session-1-update-on-nist-pqc-project-01

作者：Dustin Moody (NIST)

由于量子计算机的发明，其超高的运算能力可以快速破解公私钥对，对于现有基于公钥的密码算法构成了非常大的威胁。后量子密码（PQC，Post-Quantum Cryptography）指的是能运行在现有传统计算机上、且能够抵御传统计算机与量子计算机攻击的密码算法，也被叫做量子安全密码（QSC，Quantum-Safe Cryptography）或抗量子密码（QRC，Quantum-Resistant Cryptography）。（量子密码 Quantum Cryptography 也叫做量子密钥分发 QKD，是基于量子技术构建的密码系统，由量子的不确定性原理保证了密钥分发的绝对安全（测不准、不可复制）。但是量子密码也有很大限制，例如只能加密不能认证、量子网络扩展性差、部署昂贵且需要专用硬件。）

NIST 在 2016 年成立了 PQC Project，用来征集业界的后量子密码算法提案，并通过对安全性、性能、复杂度、灵活性等维度的比较，确定最终推荐使用的后量子密码算法。当前正在进行第 3 轮比较，确定了 7 个最有希望被标准化的密码算法，以及 8 个候选密码算法。

The 3rd Round Finalists and Alternates

NIST

- NIST selected 7 Finalists and 8 Alternates
  - Finalists: most promising algorithms we expect to be ready for standardization at end of 3rd round
  - Alternates: candidates for potential standardization, most likely after another (4th) round
- KEM finalists: Kyber, NTRU, SABER, Classic McEliece
- Signature finalists: Dilithium, Falcon, Rainbow

- KEM alternates: Bike, FrodoKEM, HQC, NTRUprime, SIKE
- Signature alternates: GeMSS, Picnic, Sphincs+

	Signatures		KEM/Encryption		Overall	
Lattice-based	2		3	2	5	2
Code-based			1	2	1	2
Multi-variate	1	1			1	1
Stateless Hash or Symmetric based		2				2
Isogeny				1		1
Total	3	3	4	5	7	8

10. SecDispatch

SecDispatch 工作组的作用是讨论归属不明确的新文稿该分发到哪个工作组。本次会议上共有两个议题。

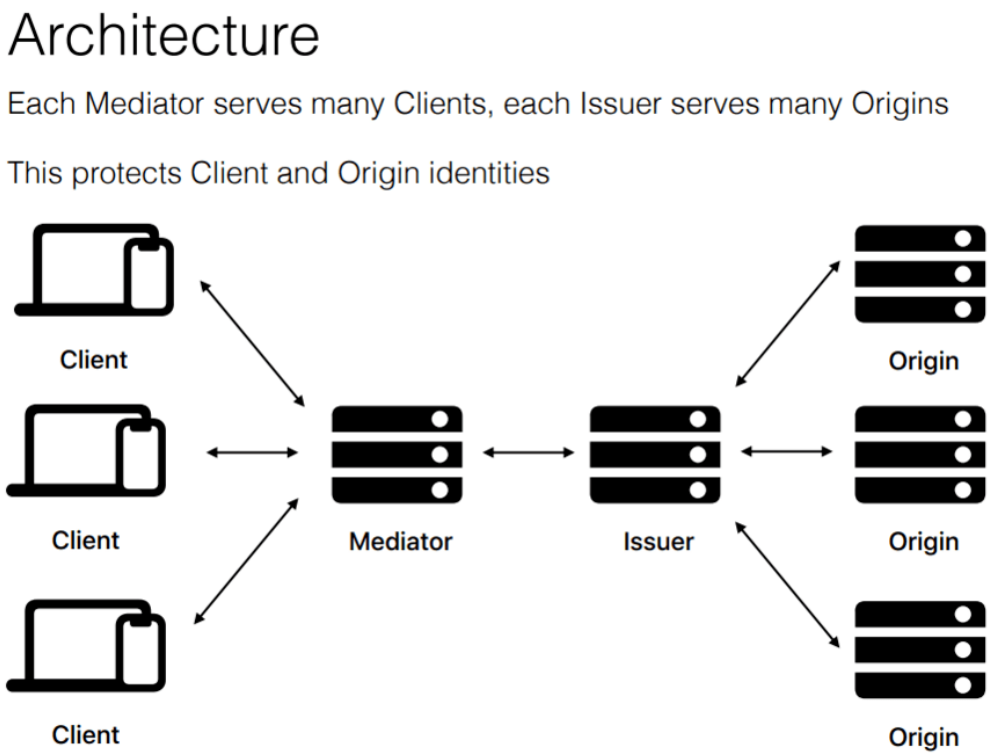
Private Access Tokens

draft-private-access-tokens

作者：Scott Hendrickson (Google)，Jana Iyengar (Fastly)，Tommy Pauly (Apple)，Steven Valdez (Google)，Christopher A. Wood (Cloudflare)

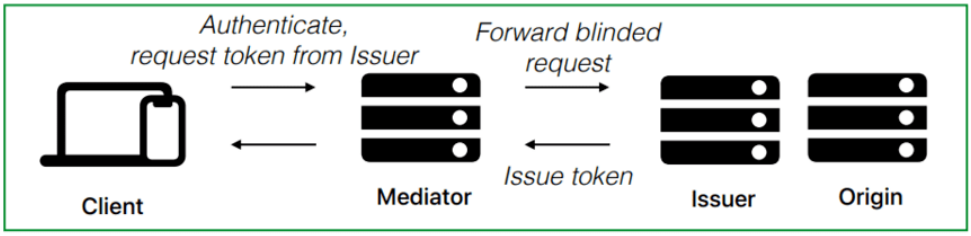
传统的应用服务器针对接入客户端实施接入策略与使用策略时，通常使用如 IP 地址在内的被动、不变的标识符来标识客户端（例如一个服务器可能会限制某个 IP 地址的接入速率、或者一段时间内可以访问的内容）。IP 地址通常也和地理位置相关联，因此这样会导致用户的网络访问行为、位置信息等被跟踪，泄露个人隐私。

作者提出一个保护用户隐私的 Private Access Token 架构，如下图所示。Client 为用户，Origin 为应用服务器，在 Client 和 Origin 之间部署两个代理 Mediator 和 Issuer，其中：1）Mediator 负责认证 Client、替 Client 向 Issuer 申请 Token，由于访问具体 Origin 的信息被加密，因此 Mediator 不会感知 Client 的网络范围行为；2）Issuer 根据要访问的 Origin 颁发 Token，但是由于其看到的申请者只是 Mediator，因此 Issuer 也不会感知 Client 的行为。



Token Issuance

Who can issue per-origin tokens?



Combination of client-trusted Mediator and origin-trusted Issuer

Mediator checks, then hides, client identity. Mediator only sees Issuer name, not Origin

Issuer enforces policy on behalf of the Origin

会上认为该工作与现在 PrivacyPass 工作组的工作范围比较接近，后续会到 PrivacyPass 工作组先进行讨论。

Security and Privacy Considerations for Multicast Transports

draft-krose-multicast-security

作者：Kyle Rose (Akamai)，Jake Holland (Akamai)

该作者是 MBONED 工作组中多篇组播相关文稿的作者，本次宣讲先介绍了组播的好处和价值，随之介绍了其认为组播可能面临的安全和隐私风险。

Multicast Security

- Integrity & Authenticity:
  - Separated from Confidentiality
  - Existing (TESLA/signed packets) and new (AMBI/ALTA) solutions
  - Anchored with secure unicast
- Confidentiality
  - many receivers must decode same packets
    - Decryption keys cannot be 1-to-1, regardless of symmetry
  - Privacy considerations key differences(?) with unicast:
    - Bad: exposes new info to local network/next-hop router
    - Bad: contents very discoverable
      - But: multicast mainly applicable to highly discoverable traffic via traffic analysis
    - Good: removes destination IP address, much increasing anonymity North of access
  - Threat model
    - gap in literature? Or only pervasive monitoring and personal information are concerns?
    - Private browsing mode block is sufficient?

会上讨论有人提出有组播 IPSec RFC5374，同时当前 IPSec 工作组中有 G-IKEv2 文稿在做基于 IKEv2 协议的组密钥管理。对于组播场景下具体是否有安全问题、具体是什么问题目前仍不清晰，因此建议现在 msec 邮件列表讨论。

11. TLS

IANA Registry Updates for TLS and DTLS

draft-salowey-tls-rfc8447bis

作者：Joseph Salowey (Salesforce)，Sean Turner (Sn3rd)

本文稿是 TLS 工作组主席提出的指导 IANA 对 TLS/DTLS 相关注册表进行修改，包括增加备注字段、修改注册规则等，对于“是否推荐”字段除原本的“Y/N”选型外增加“空”选型。

该文稿是本次新文稿，工作组同意会后发起 Adoption Call。

The Pseudorandom Extension for cTLS

draft-cpbs-pseudorandom-ctls

作者：Benjamin Schwartz (Google)，Christopher Patton (Cloudflare)

cTLS 是 TLS 1.3 的紧凑版本，通过在 Client 和 Server 双方预先定义一个 TLS 参数的 template，使得在 TLS 连接建立时可以不用发送冗余或无用的信息。本文稿定义了 CTLS 的一个扩展机制，使用 Strong Tweakable Pseudorandom Permutation 实现对发送的 TLS 报文进行重新排序，使得 TLS 连接双方使用的 template 完全无法被感知，增强安全性。

该文稿是本次新文稿，是 Experimental 类型文稿，目前主要在征求工作组的输入和意见，后续再根据情况申请工作组接纳。

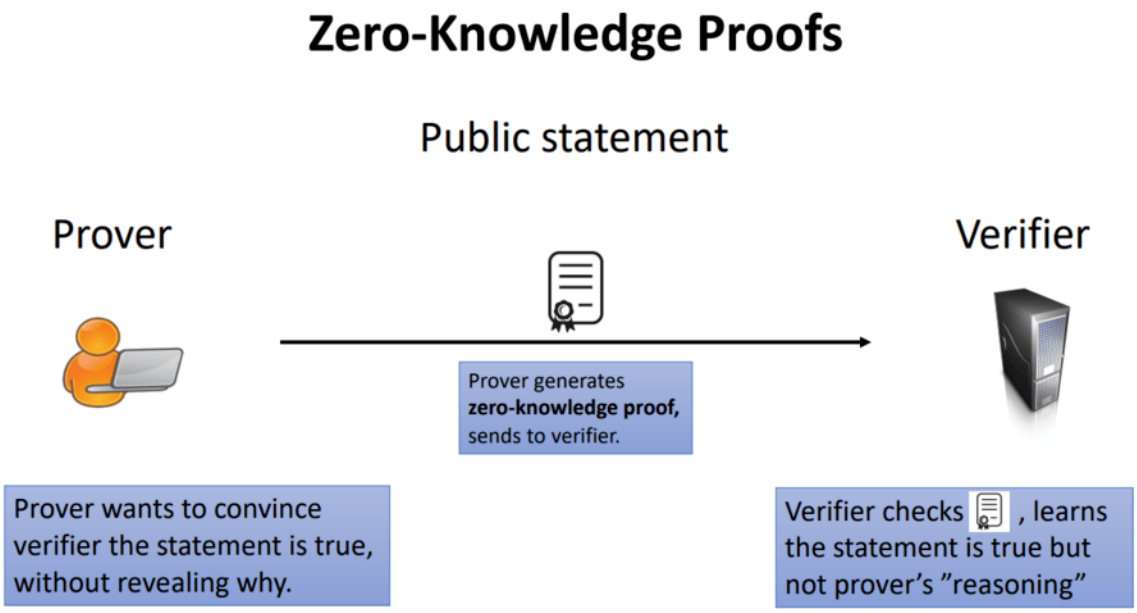
Zero-Knowledge Proofs meet TLS

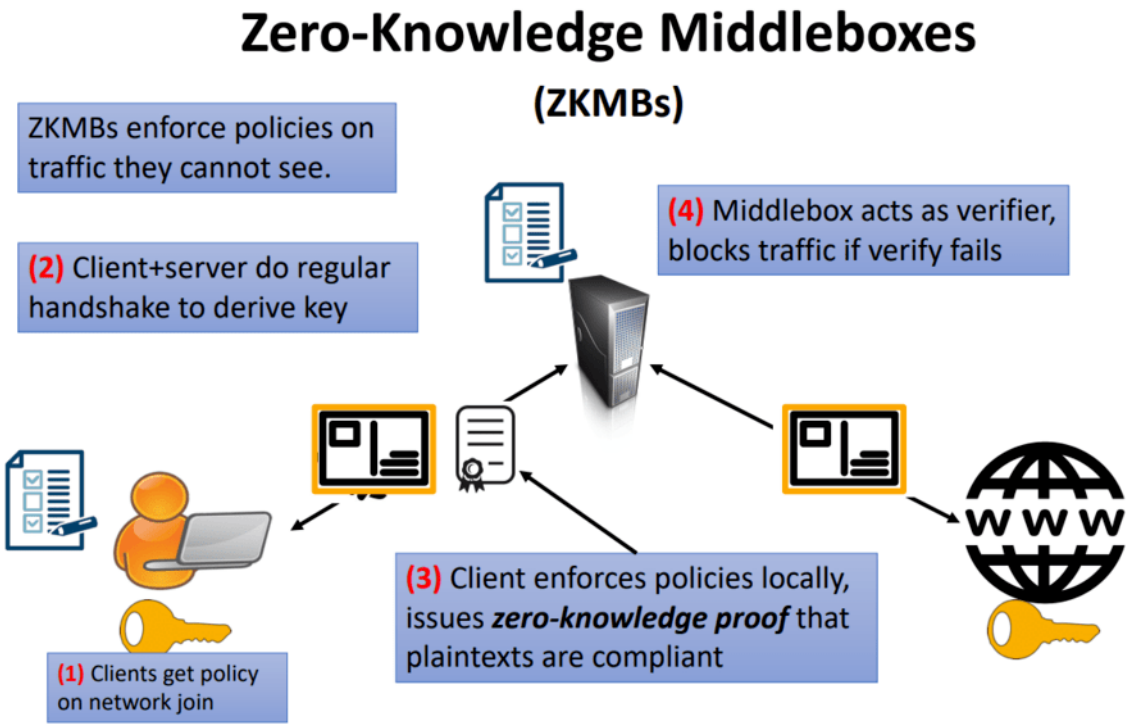
https://eprint.iacr.org/2021/1022.pdf

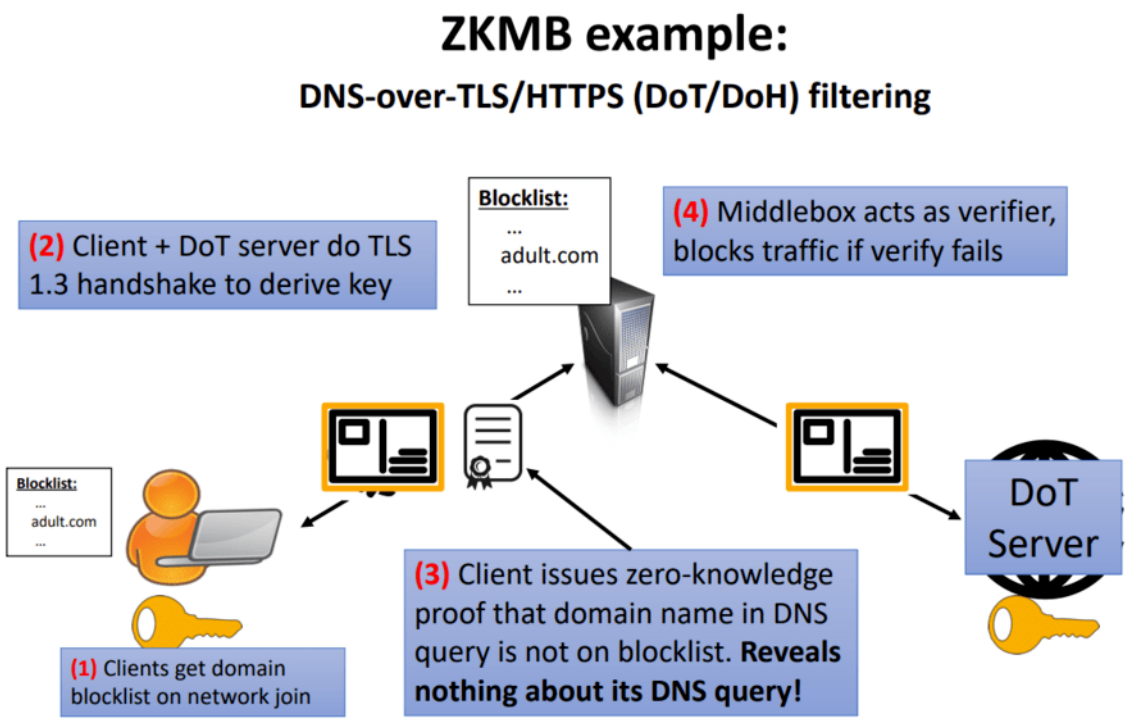
作者：Paul Grubbs (NYU)，Arasu Arun (NYU)，Ye Zhang (NYU)，Joseph Bonneau (NYU)，Michael Walfish (NYU)

该议题是来自纽约大学学生写的一篇论文，主要是讲 Zero Knowledge Proof 与 TLS 的结合。TLS 1.3 端到端加密虽然可以增强用户隐私，但是流量全加密使得网络运营商无法扫描流量来实施安全策略，DNS 过滤、入侵检测、恶意软件检测等安全功能丧失作用。传统的解决方案是在 TLS Client 和 TLS Server 之间部署 TLS Middlebox，但是这会带来安全性的降低、隐私暴露的风险。

该论文提出了利用 Zero Knowledge Proof 来解决该问题，实现在用户不暴露具体流量行为的情况下证明其流量满足安全策略。不过目前方案还不够成熟，某些场景下处理性能较差，例如密钥一致性检查需要耗时 15 秒、DoT 过滤检测需要耗时 3 秒。







12. PRIV BoF

PRIV 是 Mozilla、Google 等 OTT 厂商推动的一次 WG-forming BOF，本次会议也同意工作组成立，后续工作组可能会叫 PPM（Privacy Preserving Measurement）。

Privacy Preserving Measurement

draft-gpew-priv-ppm

作者：Tim Geoghegan (ISRG)，Christopher Patton (Cloudflare)，Eric Rescorla (Mozilla)，Christopher A. Wood (Cloudflare)

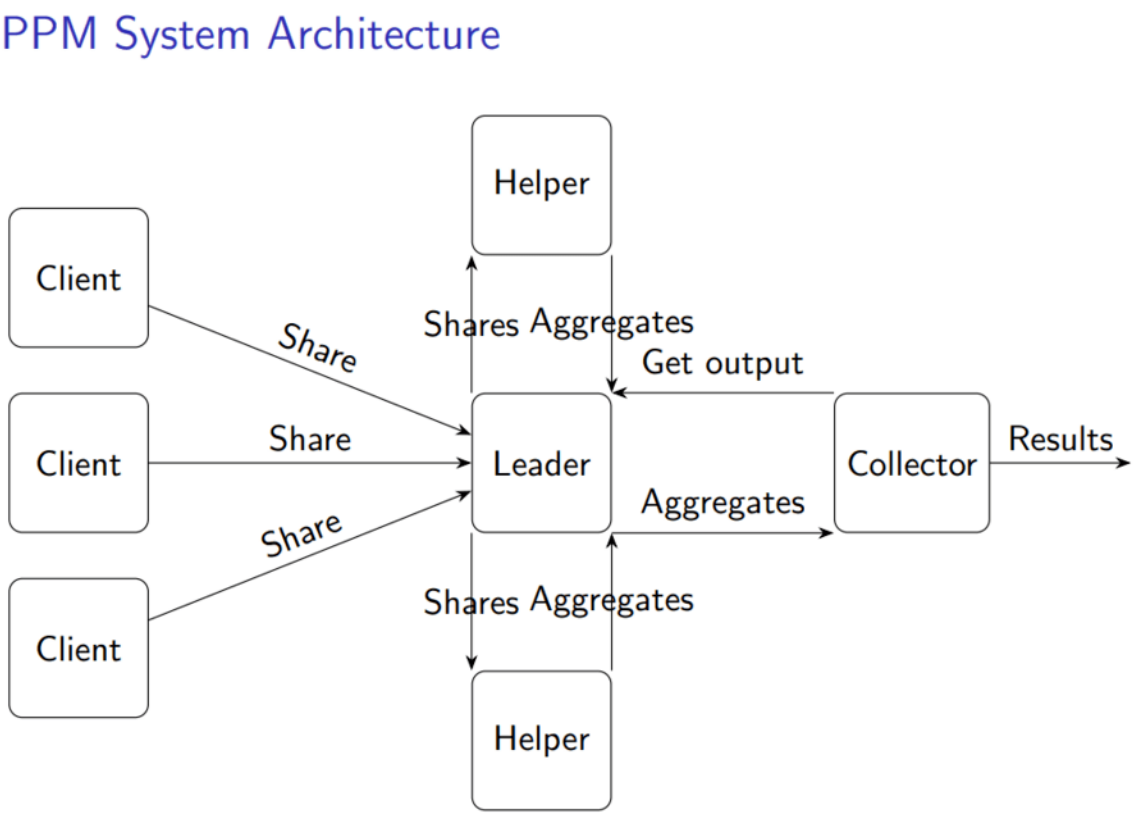
企业/政府/机构等经常希望收集与人相关的数据用于分析，例如不同年龄人群在网站访问习惯的分布情况、网站在不同浏览器上渲染问题的分布情况、新冠病毒暴露风险通知等。这些数据与人相关，但是收集这些数据的组织并不关心某个人的数据，而是只对汇总数据感兴趣。传统方法需要先收集每个用户的反馈然后再将数据聚合，这样就将每个数据和具体人关联起来，从而对用户隐私构成威胁。

业界目前有一些匿名化数据收集的方案，基本思想是收集数据时去除能标识用户的信息，常见做法包括两种：在 Client 侧直接剥离用户标识信息，以及通过 Proxy 剥离元数据（例如 OHAI

（Oblivious HTTP Application Intermediation））。这种做法依赖于信任 Proxy 不作恶，同时由于所有数据都经过 Proxy，当数据量足够时也可以反向推测出用户信息。

业界目前最新的技术是利用多方计算密码学机制来解决此问题。多方计算的基本原理是 Client 将数据分成多份发给不同的 Server，每个 Server 只看到部分数据进行计算，Collector 汇总多个 Server 的计算结果后得到最终完整的计算结果。

针对上述多方计算的原理，Mozilla、Cloudflare、ISRG 等公司提出了隐私保护度量（PPM）协议，旨在基于 HTTPS 构建一个通用的、模块化的协议，可以适用于多种多方技术密码学算法。



13. DANCE

DANCE 是原本 DANISH BOF 后成立的工作组，本次会议是工作组第一次会议。

DANCE 推动者：Ash Wilson (Valimail)，Shumon Huque (Salesforce)，Viktor Dukhovni (Two Sigma)。

DANCE 主旨：使用 DNS Name 作为 Client 的身份标识（Client 可以是 SMTP Client、IoT 设备等），将 Client 的 DNS Name 和公钥证书发布在 DNS 记录中，通过利用 DNS（及 DNSSEC）机制省去部署 PKI 系统的开销与复杂性，实现轻量化等效果。

DANCE 方案：将 DANE 机制由原 Server Authentication 扩展到 Client Authentication，通过在 DNS Record 中存储 Client 的公钥证书与 Client 的 DNS Name 的绑定关系，让 Server 在认证 Client 时通过查询 Client 的 DNS Name 即可获得 Client 公钥证书的验证信息。

DANE 背景：传统的非对称密码学认证机制都是建立在 PKI 机制上，由 CA 为设备的公钥签发证书，实现以 CA 作为可信锚点（trust anchor）为设备的公钥提供信任背书，认证时通过信任 CA 根证书来信任其签发的设备证书。DANE 方案去除了对 PKI 的依赖（使用 DNSSEC 代替 PKI），将设备的公钥和 DNS Name 绑定，这样只需要通过 DNS 查询获取 DNS Record 来建立对设备公钥/证书的信任，实现轻量化的效果。

An Architecture for DNS-Bound Client and Sender Identities

draft-wilson-dance-architecture

作者：Ash Wilson (Valimail)，Shumon Huque (Salesforce)，Olle Johansson (Edvina.net)

该文稿主要分析现有 PKI 系统给企业带来的开销大、复杂性高、命名空间重叠等问题，并介绍应用 DANCE 机制来解决这些问题的用例和架构。DANCE 在 Client/Server、Peer2Peer、Decoupled 这几种通信模式中都适用，适用的场景包括网络接入认证（如 EAP-TLS）、应用会话建立（如 TLS、HTTPS）、对象安全（如 JOSE、COSE）。

本次会议对于在 Client 侧利用 DANE 机制的整体流程/全生命周期讨论较多，例如对于证书如何发布到 DNS 服务器、如何修改/更新/吊销等都是需要考虑的点，目前对 DANCE 整体应用方案仍存有疑虑。

TLS Extension for DANE Client Identity

draft-huque-tls-dane-clientid

作者：Shumon Huque (Salesforce)，Viktor Dukhovni (Two Sigma)，Ash Wilson (Valimail)

TLS Client Authentication via DANE TLSA records

draft-huque-dane-client-cert

作者：Shumon Huque (Salesforce)，Viktor Dukhovni (Two Sigma)，Ash Wilson (Valimail)

这两篇文稿是 DANCE 的解决方案文稿，主要是对 DANE TLSA 类型的 DNS 记录如何扩展支持到 Client 侧、以及 TLS 协议如何扩展支持传输 Client 侧 DANE ID。

本次会议对于 TLS 协议如何扩展有相关讨论。有意见认为不需要扩展 TLS 协议，而是应该在 Client 的证书里扩展字段表明该证书是用在 DANCE 场景。会上同意在会后发起对这两篇解决方案文稿的 Adoption Call。

14. MADINAS

MADINAS 在 IETF109 和 IETF111 举行了第一次和第二次 BOF，本次会议是工作组成立后的第一次正式会议。

MADINAS 推动者： Juan-Carlos Zuniga (Sigfox)、Carlos Bernardos (Universidad Carlos III de Madrid)、Amelia Andersdotter (CENTR)、Jerome Henry (Cisco)、Yiu Lee (Comcast)、Tim Twell (WBA)

MAC 地址随机化的讨论大概在 2015 年左右兴起，并且业界如 iOS、Windows、Linux 等主流操作系统都做了 Wi-Fi 接入时 MAC 地址随机化的实现。MADINAS 工作组的目标不是为了讨论 MAC 地址随机化该如何实现，只分析 MAC 地址随机化可能的影响以及相关技术现状。

针对上述目标，工作组目前有两篇文稿分别是分析 MAC 地址随机化对网络/用户产生影响的 Use Cases（draft-henry-madinas-framework）、和分析总结当前业界标准组织中（主要是 IEEE 802.11 和 WBA 无线宽带联盟）涉及 MAC 地址随机化相关的技术现状（draft-zuniga-madinas-mac-address-randomization）。本次会议同意会后在邮件列表发起这两篇文稿的 Adoption Call。

目前看 MAC 地址随机化主要是对个人设备（如笔记本、手机、平板灯）在 Wi-Fi 场景下可能造成影响。对于企业园区场景，一方面企业网络内接入的移动终端应当受到强管控/有用户认证机制、不会仅凭 MAC 地址识别设备，另一方面企业网络内 IoT 设备一般不会/不需使用 MAC 地址随机化，因此 MAC 地址随机化对园区网络影响有限。

15. PIM

IETF 112 PIM 工作组基本情况：

参会人员：33 人左右

会议内容：

PART 1: 工作组基本情况

1．工作组文稿

重点关注 SR P2MP 相关文稿的进展；SR P2MP Ping 结束 WG Adoption Pull，工作组问题：本文稿是针对 MPLS 数据面还是同时适用于 MPLS/IPv6；Hooman 回应说会以 MPLS 作为开始，两种数据面都包括；

2．Re-charter

1）现状是 SPRING, BESS, IDR 都有组播的内容；其中 SR/SRv6 P2MP 作为 Re-charter 的内容加入 PIM 范畴；BESS/IDR 保持现状；

2）电信王爱俊表示和 SRv6 组播相关内容可以在 MSR6 Side Meeting 进行讨论，可以成立新的工作组；AD Alvaro 表示 Side Meeting 是非正式工作组，是否成立工作组还需要由正式 IETF 流程来进行判断，需要看是否有足够的新工作进行支持；

PART 2: 内容宣讲

1）draft-ietf-pim-jp-extensions-lisp

Cisco Stig 宣讲，主要解决当组播源和接收方处于不同 LISP sites 的情况下，边缘节点的行为；扩展 TLV 用于组播地址探寻。

Mike 评论：是否需要把 LISP 作为 Re-charter 内容？Stig 认为暂时可以维持现状。

2）draft-ietf-pim-sr-p2mp-policy

Nokia Hooman 宣讲，由于网络问题，未能完整宣讲。

3）igmp-mld-extension-source-management

China Telecom Lihuanan 宣讲，主要扩展 IGMP 和 MLD 进行源发现；会上问题较多，来自 Cisco Acee, Juniper Lenny Giuliano，认为在组播历史上源发现协议很多，但是都没有被广泛应用；Host 直接支持类似的信令，应用较为困难。

4）draft-hb-pim-light

Nokia Hooman 宣讲，在两个 PIM domain 中间跨越 BIER domain 过程中，PIM Join/Prunes/Assert 信令都需要 PIM Hello；本文的方案讨论非 PIM 邻居发送该消息的方法。

Alvaro 提问：是否可以更名为 PIM Lite Interface，这样可以缩小问题域。

5）Advancing IGMPv3&MLDv2 Internet Standard

对 RFC3376 和 RFC3810 进行更新（IGMPv3/MLDv2）。

16. SIDROPS

议题宣讲：

SIDROPS 宣讲议题如下：无草案宣讲

```
1) Agenda bashing and Chair's slides - [5 minutes]

2) Ben Maddison - [20 minutes] rpkimancer
https://github.com/benmaddison/rpkimancer

3) Oliver Borchert - [10 minutes] BGP-ASPA Hackathon Report
```

Topic 1： 主席介绍：both ASPA drafts still need work before last call

Topic 2： RPKIMancer

Ben 介绍了 RPKIMancer 工具，该工具的功能是“用于快速创建和读取任意 RPKI 签名对象的库和关联命令行实用程序。” 主要动机是能够直接从 ASN.1 Content-Type 实例定义新的 RPKI 签名对象类型，且具有最小的样板和零自定义编码逻辑。

会上大家的评论：

1. 表示该工具是有用的。

2. 除了生产对象之外，以后还可能要考虑跟踪对象 “in the middle” 的事情，需要 CT。

Topic 3：Hackathon 进展：

- NIST 支持 RFC8210,BGPSec,ASPA，但主流设备厂商还不支持这几个
- SRx Server 作为 RP 支持 ASPA
- Quagga SRx (integrates SRx API into Quagga router)支持 ASPA
- 支持 draft-ietf-sidrops-8210bis-03
- 根据 CAIDA 路由数据集构建本地 ASPA 数据库
- 根据 RouteViews3 收集的 BGP 路由模拟接收全量 BGP 路由做测试

集成上述工作，完成 ASPA 基本功能验证工作。

17. MPLS 工作组

MPLS 工作组会议时长 1 小时，有 105 人参会，会议的主要内容包括 MPLS Open DT 的进展简要介绍，Stamp for PW，MPLS MSD YANG，以及基于 MPLS 的 Detnet CQF。

工作组现有文稿的推动

在工作组进展介绍环节中，Kireeti Kompella 表示 LARP（基于 ARP 扩展分发标签）文稿可以发起 adoption poll。Shraddha 表示 EPE OAM 文稿可以发起 WG LC，主席表示后续将发起流程。

中国移动主推的 MPLS inband PM 文稿考虑使用 MPLS Open DT 的方案来减少需要携带的特殊标签层数，因此文稿作者会等 Open DT 的方案出来。

MPLS Open DT 进展介绍

Loa 简要介绍了 Open DT 的整体进展情况。Open DT 给这个工作的命名是 MPLS Indicators and Ancillary Data (MIAD)。其中 Indicator 携带在 MPLS 标签栈中，Ancillary Data 可以携带在标签栈中（ISD）或标签栈之后（PSD）。Open DT 前期整理了相关的 use case，对 MIAD 在功能和兼容性方面的基本要求进行了讨论，并在会前输出一篇需求文稿。此外 Juniper 的 Kompella 有两篇涉及 MPLS 数据面新扩展方案的文稿，John Drake 也提出了一种 Indicator 和 Ancillary Data 的封装方案，这些将在 PALS 的 Open DT joint session 进行宣讲和讨论。DT 的下一步工作将是在考虑后向兼容和未来扩展性的前提下，确定 Indicator 与 Ancillary Data 的格式和处理机制。

- Encapsulation of Simple TWAMP (STAMP) for Pseudowires in MPLS Networks

Cisco 的 Rakesh 宣讲，针对 STAMP 报文在 PW 中的封装给出两种封装方式：带 IP/UDP 头和不带 IP/UDP 头，针对不带 IP/UDP 头的情况需要定义新的 GACH type。爱立信的 Greg 质疑是否需要不带 IP/UDP 头的封装，Rakesh 的回答是针对 non-IP 业务确保 Stamp 报文和业务报文的 ECMP 相同。Stewart 建议本周内做一次小范围的讨论，Kompella 也表示有兴趣参加。

- A YANG Model for MPLS MSD

Futurewei 的 Yingzhen Qu 宣讲，模型比较简单，申请发起 adoption poll。会上有一些关于模型中名词用 segment 还是 label 的讨论，另外 Cisco 提到 SRv6 也有类似的需求，不过 Yingzhen 表示这个模型只是针对 MPLS 的，SRv6 需要的话可以单独定义。

- Deterministic QoS for MPLS data plane considerations

draft-eckert-detnet-mpls-tc-tcqf-01 and beyond

Futurewei 的 Toerless 宣讲，内容既包括基于现有 MPLS 数据面的 TCQF 实现方案，也包括对新扩展数据面的一些考虑。

1. 基于现有的 MPLS 数据面，Toerless 建议的方案是用 TC 字段的 3-5 个取值来做 TCQF，需要定义新的 QoS PHB。

2．基于新的数据面扩展，Toerless 认为有很多选项，还需要同时考虑 bounded latency 之外的其他 QoS 需求，且不限于对 MPLS 数据面的扩展。

18. PALS

PALS 工作组与 MPLS, Detnet 工作组针对 MPLS Open DT 的联合会议，时长 2 小时，有 77 人参加会议。

https://datatracker.ietf.org/meeting/112/materials/minutes-112-pals-00

Requirements for MPLS Label Stack Indicators for Ancillary Datas

Kireeti: 对 use special purpose label as last resort 有不同意见，认为可以用一个 special purpose label 来指示多种 action（ADI）

Kireeti 认为应该放宽这个要求，但认为 slice identifier 应该要求端到端的支持

DetNet ACH Update

Kompella 认为 ACH 的 first nibble 数量很少，需要结合 sub-type 字段来扩展其支持多种功能。

MPLS First Nibble

Kireeti 介绍 MPLS First Nibble 的 registry 和建议的扩展格式

Stewart 认为由于以太报文的前 4bit 可能是任何取值，使用 first nibble 来区分报文的封装类型存在风险。

Haoyu 认为如果标签栈中有了 indicator，不需要 first nibble 来区分不同类型的封装。

Multi-purpose Special Purpose Label for Forwarding Actions

Kompella 倾向于 ISD 携带的信息全部做 HBH 处理，PSD 则可以是 HBH 或 E2E 的处理方式

Network function Indicator

John 的方案中，ISD 可以是 HBH 或 E2E 的，HBH 在前，PSD 也可以是 HBH 或 E2E，通过 NFF 中的每个 Flag 指示一种 function 类型，每种 function 的定义需要明确是 LSD 还是 PSD。

19. NETMOD

周四会议时间只有一个小时，约 40 人参加，运营商 Equinix，Telefonica，Orange，BT，TI，Swisscom，移动，联通；厂家主要包括思科，Juniper，Nokia，Ciena，Ericsson，烽火参加，

WG Chairs:

Lou Berger (lberger at labs dot net)

Kent Watsen (kent plus ietf at watsen dot net)

Joel Jaeggli (joelja at bogus dot com)

工作组进展更新

In RFC Editor Queue：

– draft-ietf-netmod-nmda-diff-07 Shepherd: Joel

NMDA Diff 华为主导工作组草案，主要解决不同数据集差异比较的方法，目前该草案已经提交 IETF 发布;

– draft-ietf-netmod-geo-location-07Shepherd:

Kent 地理位置定位模型，目前是来自 LabN Chris 主导撰写，该草案也已经进入 IETF 发布阶段;

- draft-ietf-netmod-yang-instance-file-format-21

YANG Instance 文件格式是华为和爱立信主导;

Post LC：

– draft-ietf-netmod-intf-ext-yang-09 (expired, waiting on authors) Shepherd: Lou

– draft-ietf-netmod-sub-intf-vlan-model-07 (expired, waiting on authors) Shepherd:

YANG 模型接口两篇草案由思科主导，是 IETF 和 IEEE 协作的成果，目前也已经过期，RW 工作 overload，无暇兼顾。

WG:

– draft-ietf-netmod-syslog-model-26 – Missref Shepherd: Kent

– draft-ietf-netmod-rfc6991-bis-07 RW 希望尽快发布

– draft-ietf-netmod-yang-versioning-reqs-05 已经 WGLC，需要其他版本管理一同 IESG

– draft-ietf-netmod-node-tags-03

MDT 自解释标签定义草案，定义自解释标签，对采集的 YANG Data 进行分类，标识运维数据的各类性能指标单指标、多指标、多维数据的 AI 分析，实现网络负载、流量、容量、质量的秒级可视

– https://tools.ietf.org/html/draft-ietf-netmod-eca-policy-01

ECA（(Event Condition Action)）模型主要解决设备运维管理自动化问题

议题讨论

YANG 版本管理更新，YANG Versioning Update (15 min)

https://datatracker.ietf.org/doc/draft-ietf-netmod-yang-module-versioning/

https://datatracker.ietf.org/doc/draft-ietf-netmod-yang-semver/

https://datatracker.ietf.org/doc/draft-ietf-netmod-yang-packages/

https://datatracker.ietf.org/doc/draft-ietf-netmod-yang-ver-selection/

https://datatracker.ietf.org/doc/draft-ietf-netmod-yang-schema-comparison/

Jason&Reshad Rahman

版本管理系列草案，包括整体 solution 说明，RFC7950 更新，Semver，Package，Package selection，versioning comparison tooling7 篇草案。

本次会议 Model versioning，Semver 两篇草案已稳定。YANG package 做了编辑性更新，计划增加 schema mount 的 mount point 加载 package 功能。但因为又定义了 module list，和 Hello，YANG library 功能重复，会给控制器带来多份数据源的困扰。

System-defined Configuration 设备系统配置，client 不感知问题

https://datatracker.ietf.org/doc/html/draft-ma-netmod-with-system-00

Discussion Leader: Qiufang Ma

系统配置是由厂商或设备提供的配置数据，目前各厂商系统配置的行为定义不一致。

该工作在 2021.10 月召开中间会议，对关于系统配置的行为定义的目标，范围和基本的解决方案达成基本一致。

对于系统配置，设备应当做到对 client 可见、可配置，当用户配置引用系统配置时应尽量保证避免重复定义。

本次上会主要梳理遗留问题，包括是否需要保证数据集满足离线验证需求，对于 client 端拷贝到中的系统配置是否需要在数据集中数据源标记为“system”，是否需要定义“immutable”声明只读的系统配置等。目前草案对于系统配置的处理行为可以类比为 with-defaults 处理行为中的 explicit mode,Watsen，诺基亚和思科建议和 default 的处理行为保持一致。

Extensions to the Access Control Lists (ACLs) YANG Model

https://datatracker.ietf.org/doc/html/draft-dbb-netmod-acl-00

Discussion Leader: Oscar González de Dios

Telefonica 认为现有 IETF 发布的 ACL 模型（Mahesh 牵头定义的）无法满足控制器集中管理的需要，希望通过定义模板，掩码等集中创建，从而方便下发给设备。当前设备的 ACL 模型定义主要是精确匹配。

Chair Lou 希望能进一步确认，相比现有的 ACL，是否增加新的功能，以及模型架构有所影响。需要草案提供更多的分析和说明，方便工作组决策。

Juniper Jeffery 认为有必要区分精确匹配和掩码匹配，并且不希望依赖枚举类型来获取

思科此前在邮件支持该工作，认为当前 ACL 会有 m prefix x n port, rule 条目过多。如果定义通过 object-groups/defined-sets for prefix and port，m prefix + n port 条目，减少配置条目。

CCAMP 光网络存量的 YANG 数据模型

https://datatracker.ietf.org/doc/html/draft-yg3bp-ccamp-optical-inventory-yang-00

Chair 认为没有时间宣讲，并且已知悉相关工作在 CCAMP 开展。

20. 6MAN

Chairs: Bob Hinden, Ole Trøan

Introduction and Document Status

Bob Hinden presented. Slides: Introduction, Agenda Bashing

Ole asked if anyone wanted to bash the agenda. No-one asked for any changes to the agenda.

Bob mentioned the Friday joint session with v6ops WG. Agenda link: IPv6 Operations

Ole presented the slide on document status. There was some discussion on document status of various documents, involving Erik Kline (AD) and Jen Linkova.

SID & IPv6 addressing

Erik Kline presented. Slides: SRv6 SIDs

Suresh Krishnan presented Next Steps.

Erik Kline: Thank you to Suresh for bringing clarity to what the issues are.

Ron Bonica: Would you like to comment on the 6man and Spring mailing lists?

Suresh: Prefer 6man. But following Spring, too.

Ole: Thank you.

IPv6 Application of the Alternate Marking Method

Giuseppe Fioccola presented. Slides: IPv6 Application of the Alternate Marking Method

Ole: it seems that we are making progress. Any comments? No. Hopefully it won't take too much longer.

Carrying VTN Identifier in IPv6 Extension Header

Presented by Jie Dong. Slides: Carrying VTN-ID in IPv6 Extension Header

Ole: Thank you. Comments?

Jie has asked if we could put this draft out for adoption call.

Will run a quick poll to determine interest from WG. Poll results are Raise Hand: 11; Do Not Raise Hand: 33.

Bob: The "11" raised hands appeared to be a stable number (was not increasing). The "Do Not Raise Hand" had still been increasing when the poll ended.

ICMPv6 Extensions for IOAM Capabilities Discovery

Xiao Min presented. Slides: ICMPv6 Extensions for IOAM Capabilities Discovery

Presentation deferred to end due to poor audio from presenter.

ND Prefix Robustness Improvements

Presented by Eduard Vasilenko. Slides: ND Prefix Robustness Improvements

Ole: A lot of comments on chat. Comments?

Jen Linkova: I'm confused. Host switch supports rule 5.5? (abrupt router change)? We believe this is not needed. We already have mechanisms to solve this, but host implementations do not care (yet).

Eduard Vasilenko: We believe no. It is not the case. It has good recommendation. But not details. Just good guidance. No explanation on what to do.

Jen: It's about cost and not about changes in new products. There are not many implementations of host side. We do not see this problem in real life.

Eduard Vasilenko: this host selection is related with ND. Two stages. RFC8028 gave recommendations. We follow it not contradict it. More details are still needed.

Ole: Continue to discuss on list.

Bob: We need agreement on the problems that need to be solved first, before identifying solutions.

IPv6 Fragment Retransmission

Fred Templin presented. Slides: IPv6 Fragment Retransmission

Bob: Comments? Nobody?

There were no comments.

Ole: We can do a poll to see if there is interest.

Fred: The most important part is chart 2.

Ole: Is that in inherent aspect of fragmentation?

Fred: Bursty nature of sending 1 large packet is what allows greater utilization for same time period by leveraging fragmentation bursts.

Ole: OK it solves some problems.

Bob: A lot of discussion in chat. There will be interactions with transport protocols if IP protocol is doing retransmissions and transport protocol is doing retransmissions.

Fred: It is not correct. Transport retransmission is imperfect.

Bob: In IPv6 it is the endpoint that performs fragmentation.

Erik Kline: As individual, are some of these things separable? Is there something valuable in just the soft error?

Fred: Definitely more there in soft error. More in the draft.

Erik Kline: Maybe that is more useful than other components of the draft.

Poll results are Raise Hand: 12; Do Not Raise Hand: 24.

ICMPv6 Extensions for IOAM Capabilities Discovery

Xiao Min presented. Slides: ICMPv6 Extensions for IOAM Capabilities Discovery

This presentation had been deferred from earlier in the agenda. Audio was much improved.

Cheng Li: Can hosts outside of a domain send an ICMP packet to trigger the IOAM capability?

Xiao Min: Do you mean the host? Yes.

Cheng: What if I am a hacker and send a lot of DDOS packets to get IOAM info from your network? You're saying we can use IPsec for security. But if you want to provide this kind of prtection you need full IPsec mesh in your network. Is this possible?

Xiao Min: This draft provides security mitigate methods. You can also ask network operator to establish policies.

Cheng: But in real network, IPsec is very heavy. It's hard for implementation/usage/deployment. To protect IOAM, we must build up any-to-any IPsec mesh. That's not realistic. You could do some rate limiting for preventing DDOS. I agree with that.

Xiao Min: IPSec is not a MUST.

Eduard V: it is HBH or end-to-end? IOAM is more useful when HBH. How much will it be useful if not HBH?

Xiao: In this draft ICMPv6 echo request is not just E2E. It can be sent to intermediary nodes in path. Intermediate nodes can send replies to host.

Eduard V: Seperate probe for seperate host. Understood.

Eric Vyncke: This draft relies on IPPM draft. Can you say some words about that draft? Is it in WGLC?

Xiao: It is adopted this year in July. 01 working group draft.

Erik Kline: How large do you think these messages are going to be?

Xiao: For the echo request, the message will not be too big. The reply may exceed the MTU limit. We have the big reply message.

Erik: You have a truncation plane?

Xiao: Scoll to slide 3. If the message is too big and exceed the MTU limit, the value can be set to indicate the message it is too big.

Bob: Thank you. I think this needs more discussion. And we would like to hear from IPPM WG and how this fits into what they're doing. This needs to fit into a larger use case.

21. SPRING

WG Status

Joel Halpern presented.

The issue tracker for the adopted compression document will be on the Github.

Srihari Sangli (from the Chat Panel): Should 6man bless the document? c-sid and its relationship to RFC4291.

Joel Halpern: The 6man will decide the relationship.

Enhanced Performance Measurement Using Simple TWAMP in Segment Routing Networks

draft-gandhi-spring-enhanced-srpm

Rakesh Gandhi

Greg Mirsky: It enables one way measurement. The reflector doesnot have a state, and the packet does not leave the data plane. The format of the reflected packet is different from the format of the packet received from the sender. How you can simply swap the source and destination address of the two packets? Also if you dont have state in the reflector you cannot measure one way but only round trip. It is not accurate. I think some serious problem with this.

Rakesh Gandhi: Thanks. The loopback measurement mode has been defined in a working group document. Please have a look at the draft and let us know. That is for the round trip delay. This is an optimization where the session reflector using the network programming function as the receiver timestamp. This is explained in the enhanced loopback mode draft. Please have a look and let us know about your comments.

Greg Mirsky: I sent comments before the meeting. I see contradiction between the statements. SR programming does not introduce any special mode in the stamp. The reflector has to be stateful for the one way measurement. The underlay for the packet encapsulation is not really relevant. We can continue in the mailing list.

Rakesh Gandhi: I will look at your recent email and reply.

Stewart Bryant: How do you avoid the ECMP issue with this? The ECMP will give you a different answer when you run this. Is ECMP safe? Is it for MPLS?

Rakesh Gandhi: For ECMP there are standard techniques for example using the Entropy label.

Stewart Bryant: You require the Entropy label for the ECMP safe measurement that is absolutely fine, but you must show it. Currently it is not.

Rakesh Gandhi: We will add it.

Stewart Bryant: It has to be high level required because people will get the wrong answer. You cannot publish a document where people get the wrong answer.

Rakesh Gandhi: Good comment. We will add it.

Andrew Alston: What is the impact on the BCP38? The incorrect sender and receiver. That reversal of addresses does kind of worry me. Would like to hear your thoughts on the impacts on things like BCP38 and anti-spoofing protection.

Rakesh Gandhi: If that is not suitable for the network, so the second method for the reverse path can be SR-MPLS. The full label stack could be used to bring the packet back to the sender. Both methods have been defined depending on the deployment. One of them can be selected. There are already many RFCs around about using the swapping of the source address. It is no difference here.

Joel Halpern: Please continue email discussions.

Segment Routing for End-to-End IETF Network Slicing

draft-li-spring-sr-e2e-ietf-network-slicing

Yongqing Zhu

Vishnu Beeram: Slide 3 that showed all the relevant drafts. We have a WG draft on framework which stated ietf network slices, and we don't limit the scope of that draft. It would be good to limit the scope of this draft on how to stitch multiple vtns together.

Jie Dong: The related framework draft of this draft will be presented tomorrow in teas. This draft is more about SR based extension to solve the multi-domain mapping and concatenation.

Adrian Farrel: Speaking as the editor of the network slicing framework draft in teas which is intended to be sort of all embracing for ietf network slices. I want to caution the authors here to be very careful about the term end-to-end. It has been used by 3GPP. The IETF network slice is only a part. The concept of end has a strange meaning in IETF. Maybe step back from the headline title of end-to-end and talk more about what you want to achieve, rather than get hooked on the terminology.

SRv6 inter-domain mapping SIDs

draft-salih-spring-srv6-inter-domain-sids

Salih K A

Zhenbin Li: End.replace is similar to swap of MPLS. In SRv6 we don't need SWAP. Why to introduce this SID.

Salih: It is for multi-domain. On the boarder node, it is for option C and uses BGP.

Ketan Talaulikar: End.DB6, service SID is per prefix or per VRF.

Salih: Per prefix. It is option B.

Ketan Talaulikar: Please clarify in the draft. Also, suggest to consider per VRF instead.

Salih: Sure.

Cheng Li: Don't understand why to replace the destination address. 2. When the SID list contains one SID like BSID, what is difference between the BSID and End.replace. The procedure is the same.

Salih: If it is multiple SIDs to reach the other domain. It will be based on the situation. We will update the draft with more details.

Zhenbin Li: The purpose of this type of SID. It is different from MPLS and SRv6. IPv6 can reduce using aggregation. It is reducing the benefits of SRv6.

Salih: Different scenarios. It is for multiple domains and it is option C. It could be multiple intent-based path. Different mechanisms for different scenarios.

Shraddha Hegde (from the chat box): This mechanism is for loosely coupled domains where aggregation is not possible.

Darren Dukes: Additional discussion of how an SR Source uses SIDs of these behaviors and will be interesting to see in subsequent versions.

Salih: Will update the draft.

Shaofu Peng: END.Replace seems enough why we need END.ReplaceB6?

Salih: In the diagram you can see that cross areas you need multiple SIDs in the SRH and that is why you need to push an additional SRH at the corresponding ingress boarder nodes. It will be clear with an example when we mention it in the draft.

Cheng Li (from the chat box): Better to clarify why we need these new behavious why not the existing ones.

SRH encapsulation for Alternate Marking Method

draft-fz-spring-srv6-alt-mark

Giuseppe Fioccola

Ron Bonica: Why would you not to make it more general, and make it work for any other routing header?

Giuseppe: Just to leverage this capability of SRH to be extended to TLV. The solution for all the routing header is already in the 6man draft. There we define the DOH that can be applicable to all the routing header. It can be an optimized solution only for SRH.

Ron Bonica: It seems a second solution for the problem you have already solved.

Tianran Zhou (from the chat box): The generic way is defined in 6man. This is only an optimization for SRH.

Joel: Please continue in the mailing list.

A Simplified Scalable ELAN Service Model with Segment Routing Underlay

draft-boutros-spring-elan-services-over-sr

Sami Boutros

Éric Vyncke: Your draft and your slides got a section about IPv4 arp but nothing about v6 NDP. Will add support for IPv6 support later?

Sami: Yes, will add later.

Matthew Bocci: Relationship with the draft in BESS? Clarify your intention of the BESS draft. This relates to BGP signalings and it should really live in BESS.

Sami: The concept is more segment routing so we present the concept here in SPRING. The signaling details will be in BESS. Here is more about the concept and the architecture. Will clarify in the later version.

Joel Halpern: The Chairs will coordinate to make sure that the right materials are discussed in the right WG.

Patrice Brissette: The same comment to Matthew. Is it any difference between there two drafts?

Sami: No, not right now. Will change the other draft to more signaling aspects in the later version.

Intent-based Routing

draft-li-teas-intent-based-routing

Zhenbin Li

Linda Dunbar: Is that intent perform the similar function to QoS / Policy in a way that you can steer traffic and give another layer of policy matching criteria?

Zhenbin Li: To some extent, it is similar. To be more exact, it is like color, such as low latency or high bandwidth, not only just like DSCP which is just a codepoint. It is a abstract of the requirements. Not a detailed service requirement.

Eric Vyncke (from the chat box): please specify whether the IPv6 Dest Options should be BEFORE or AFTER the routing header.

Source Segment for Multicast Source Routing over IPv6

draft-xl-msr6-source-segment

Xuesong Geng

Ron Bonica: What happens if a packet has a SID as its source address but for some reasons the packet can not be forwarded, and the node cannot forward it sends an ICMP message to that source address. What does the ICMP message go?

Xuesong: The source address is still routable. The locator part is still routable. Just the MVPN information can be carried in the Argument part.

Ron Bonica: So lower bits are totally ignored at the source.

Joel: This is a detailed discussion. Please go to the mailing list.

Zhaohui Zhang: This concept was first brought up in BIER. There were a lot of discussions in the mailing list.

Xuesong: It is not for BIER. This can be used for any IPv6 based multicast scenarios to carry mvpn. We also discussed this in the section 6 in the document. Please review the draft.

Functional Addressing (FA) for internets with Independent Network Address Spaces (IINAS)

draft-eckert-intarea-functional-addr-internets

Toerless Eckert

Joel: It is very questionable whether it is within the charter of SPRING.

22. LSR

Flooding Speed

Les Ginsberg / Bruno Decraene (5 mins)

https://datatracker.ietf.org/doc/draft-decraeneginsberg-lsr-isis-fast-flooding/

Cisco/Orange 主导。文稿主要结合拥塞控制机制，调整 Flooding 发送速率，以降低丢包，加快 IGP 同步；Isis flooding control 的两篇文稿合并，Flooding Parameters TLV 被保留（三个来自 Bruno，三个新定义），不直接限制 congestion control 的机制；Cisco 表示希望尽快 WG Adoption，这样可以产品实现。

主席 Acee：会发起 adoption call，不过需要确定文稿类型是 informational/experimental；

IS-IS Flood Reflection

Tony Przygienda (10 mins)

https://datatracker.ietf.org/doc/draft-ietf-lsr-isis-flood-reflection/

Juniper 主导。文稿定义了一种 L2 的泛洪反射机制，用于提升 L2 的扩展性；

Juniper 表示已有实现，希望能够加快标准进程；本次更新群分了两种实现模式，一种有 tunnel 一种没有 tunnel；同时定义了 sub-sub-TLV 用于隧道类型发现；

主席 Chris 询问为什么需要信令来建立 tunnel，为什么不能直接通过配置来实现；Tony 回应说每个节点需要知道自己的角色以及隧道类型；Chris 询问和 TTZ 的机制差异，Huaimo 和 Tony 澄清，TTZ 需要在 L1 内泛洪，本文稿的机制仅需要在 L2 进行扩展；

The Application Specific Link Attribute (ASLA) Any Application Bit

Shraddha Hegde (10 mins)

https://datatracker.ietf.org/doc/draft-hegde-lsr-asla-any-app/

Juniper 主导。该文稿为 Standard Application Identifier Bit Mask 引入一个新的比特位，称为 A 位，如果 A 位被置位，该链接属性可以被被任何应用程序使用。

主席和 Les 认为对当前机制进行扩展即可，没有必要定义新的 bit 位。该方法的必要性需要在邮件列表的继续讨论。

Updates for PUA and Passive Interface Attributes

Gyan Mishra/Aijun Wang (15 mins)

https://datatracker.ietf.org/doc/draft-wang-lsr-prefix-unreachable-annoucement/

https://datatracker.ietf.org/doc/draft-wang-lsr-passive-interface-attribute/

电信主导。该文稿定义了 Prefix Unreachable Announcement(PUAM)，用于检测并通告网络失效，以避免因为多区域/层次网络中，发生故障时 导致 LPM 组件前缀从 FIB 中被遗漏导致路由黑洞的问题。

是否使用 IGP 解决该问题，以及怎样对 IGP 进行扩展以解决该问题都需要继续讨论；不足以进行 WG Adoption;

Flex Algo Extension for 5G Edge Computing Service

Linda Dunbar (10 mins)

https://datatracker.ietf.org/doc/draft-dunbar-lsr-5g-edge-compute/

本文定义了应用于 5G 本地数据网络（LDN）中的新的 metric，用于描述应用相关的信息，如 site-costs, preference 等，用于在 LDN 中实现 CSPF，提高路由能力；

Shraddha 表示该扩展的主要目标是实现负载均衡，但是扩展 metric 可能不是最好的方法，如会带来路由的不稳定；Chris 认为使用 metric 进行负载均衡是合理的。

IGP Extensions for Path MTU

Xing Xi (10 mins)

https://datatracker.ietf.org/doc/draft-hu-lsr-igp-path-mtu/

在 SR 场景中，由于没有类似传统 MPLS 的路径建立信令，无法支持 Path MTU；因此需要进行 IGP 扩展以支持 Path MTU；

Jeff 认为信令的通告不一定可信；Les 认为 ISIS 当前有两个字段可以用作这一功能；Acee 认为扩展的粒度（node 粒度或者 link 粒度）需要进一步讨论。

Signaling Flow-ID Label Capability and Flow-ID Readable Label Depth Using IGP and BGP-LS

Xiao Min (10 mins)

https://datatracker.ietf.org/doc/draft-xzc-lsr-mpls-flc-flrd/

扩展 IGP 以泛洪 Flow-ID Label 和可读深度，用于测量。

工作组认为该信息不用于路由，不应该使用 IGP 扩展，且扩展的粒度（node 粒度/link 粒度/Prefix 粒度）选择不合理；

IS-IS Extensions for Link Bit Error Ratio

Chenxi Li (10 mins)

https://datatracker.ietf.org/doc/draft-li-lsr-isis-link-ber/

使用 IGP 扩展携带误码率信息。

工作组认为该 metric 的定义需要进一步明确，且说明相对于已有的丢包率，优势在哪里。

23. COINRG

参会人员：90 人左右

会议内容：

主要包括论文分享，刷新草案和新草案的讲解，其中第一篇论文 EI（Extensible Internet）的讨论比较多，其他论文和草案都只是讲解，移动提的新草案因时间原因未分享。

Extensible Internet

这是 SIGCOMM CCR 期刊论文《Revitalizing the Public Internet By Making it Extensible》，未来 Internet 网络架构相关，且是业界大拿 UC Berkeley 教授 Scott Shenker 宣讲，关注比较多。

- 参照 OTT 的 Global Private Network 的 POP，为 Public Internet 增加了 SN（Service Node）节点，部在边缘（分别于源和目的相连），提供平台，通用业务，比如部署在网业务：比如流终结，缓存，负载均衡器等，允许公共互联网包含更广泛的功能。
- 协议不改动，因此论文的 L3.5 层或业务层（Service Layer）并不是数据平面的 3.5 层报文扩展。SN（Service Node）之间是管道，Tunnel over IP。

对于大家的疑问的答复：

- 对于 Addrian Farrel 提到的疑问：（1）确认源和目的之间的传输层是否是端到端，还是说会在 SN 做终止在重建连的操作：答复是传输层还是端到端，SN 之间是管道。（2）对于传输层做了加密，SN 会怎么做的问题：答复是如果希望 SN 提供服务，那么传输层就不能加密或者提供其他信息供 SN 处理。
- 对于 SN 之间的互连是否会需要类似于 SDN 的控制面来确定 SN 之间如何可达，答复当前未考虑控制面，但是应该会采用类似于 SDN 的控制面。

Scott Shenker 提到 EI 的一个 Case：目前，云为面向用户的大型网络花费，云可以要一个在边缘部署这些通用服务的通用基础架构，从而更加专注后端服务。此外，一旦 EI 成为整体架构，主机就可以选择服务，从而实现更广泛的网络内服务。已经与所有主要云公司的人进行了交谈，认为这样的故事是有道理的。

云公司并不“紧急”需要 EI，但是 (i) 使用了 EI，云会省钱，并且 (ii) EI 为更广泛的网络内服务（In-Network Service）打开了大门，这些服务将提高安全性、隐私性和应用程序性能。

ATP: in-network aggregation for multi-tenant learning

(Wenfei Wu, Peking University)

ATP: 面向多租户的深度学习训练聚合传输协议，第 18 届 USENIX NSDI(网络系统设计与实现)年会最佳论文奖。论文出自清华大学吴文斐研究组，这是中国高校（含港澳台地区）首次在 NSDI 会议取得最佳论文奖。

随着机器学习数据量和模型规模的扩大以及其应用场景的扩展（例如联邦学习），机器学习系统逐步以分布式的方式来部署和实现，尤其是在数据中心或多租户多训练工作同步进行的私有集群场景。在最近的一些工作指出，部分训练工作的网络传输时长占着训练时间愈来愈高的比例，甚至已经成为瓶颈，制约着分布式学习系统的整体效率。与此同时，通过对分布式学习训练的研究，文章作者注意到分布式训练的网络传输部分有着可以优化的流量模式，再利用与可编程网络的共同设计，提出了 ATP 系统。

ATP 是一套面向于多租户多机架场景的机器学习训练加速协议，利用可编程交换机技术对分布式训练的网络传输部分进行聚合优化，建立了一套由终端主机网络协议栈和可编程交换机共同交互组成的高速分布式训练协议，在网络中提供尽力服务(best-effort)及资源动态分配(dynamic)的聚合语义，并考虑了多租户场景下的竞争策略，重新设计了丢包恢复和拥塞控制算法。实验表明 ATP 协议在各个不同的模型中效能超越了现时主流通用的分布式框架，并在竞争严重的多租户场景下维持了十分良好的效能。

Information-centric dataflow: re-imagining reactive distributed computing

(Dirk Kutscher, Emden University)

属于 piccolo 项目，在网计算的项目的成果。2021 SIGCOMM ICN workshop 的一篇论文。

对于 Apache Flink、Google Dataflow 这样的大数据分布式计算平台，既支持流式处理，也支持批处理。计算实例包括生产者和消费者之间是通过基于连接的，基于 Overlay 的通道互连，这样的方式有些效率问题。

配置和管理问题

1）应用逻辑关心的是分解出的计算实例，但是当前这些实例之间互连是通过地址建立的通道，目前采用映射系统或者协同层维护这种名址映射关系。

2）计算任务并行化，数据流图中，多个连接的端点需要进行配置或重配置，配置困难。

数据流动效率问题：

1）一（生产者）对多（消费者）的并行化的计算采用的是多个通道复制的方式，不是组播的方式。

2）Overlay 的通道，IP 网络对其是黑盒，连接通道所走路径不一定是优化的路径。

为了本论文提到的基于信息为中心的系统 IceFlow，除了通过 ICN 进行计算功能之间的通信外，提供额外的流处理系统需要的功能，例如流量控制、数据流分区以及用于同步流管道中计算的窗口概念，可以替代当前流处理系统的底层框架。能解决上面的现有大数据流处理系统的问题，做到：

- 减少数据流系统的复杂性，去除基于连接的 overlay 和协同层系统需求
- 减少数据复制，通信更有效
- 通过直接通信和在网缓存对系统性能进一步改进。

Use Cases for In-Network Computing

(Ike Kunze, RWTH Aachen University)

https://datatracker.ietf.org/doc/html/draft-irtf-coinrg-use-cases-01

在网计算的 Use Case 进行了刷新，增加了一个新的 Use Case-Virtual Networks Programming，将 Case 进行了新的分类，分成了四类：Providing New COIN Experiences, Supporting new COIN Systems, Improving existing COIN capabilities, Enabling new COIN capabilities。

Transport Protocol Issues of In-Network Computing Systems

(Dirk Trossen, Huawei)

https://www.ietf.org/archive/id/draft-kunze-coinrg-transport-issues-05.txt

草案地址技术章节中增加了灵活寻址 Flexible Addressing 和基于语义的路由 Semantic Routing 的描述。

Enhancing Security and Privacy with In-Network Computing

(Ina Fink, RWTH Aachen University)

https://datatracker.ietf.org/doc/draft-fink-coin-sec-priv/03/

该草案的内容主要就是在网络设备上实现安全和隐私机制，和 middle box 相比，性能和安全性增强。本次会议草案根据最新的一些和在网计算安全相关的论文总结后对草案进行了刷新，相关论文内容包括：可编程交换机的设计支持安全加密功能; 网络中的身份验证没有延迟开销; 可扩展、透明且轻量级的匿名化; 对异常情况的在线检测和反应、减少入侵检测系统 (IDS) 的负载; 高效的网络监控，例如用于网络取证。

A Compute Resources Oriented Scheduling Mechanism based on Dataplane Programmability

(Kehan Li, ChinaMobile)

https://datatracker.ietf.org/doc/draft-li-coinrg-compute-resource-scheduling/

移动提的算力网络相关草案，试图用数据面去做资源申请（向算力资源管理节点），及生命周期管理的事情。不涉及算力资源管理节点如何收集资源。

电信则是协议控制面如何发布和收集资源。资源申请及生命周期管理用的也是控制面。

24. TEAS

本次 TEAS 会议的参会人数为 137 人，主要议题为网络切片和 TE YANG 模型相关。

上次 IETF 会后原工作组秘书 Matt 不再继续担任该职位，由来自 Telefonica 的 Luis 担任工作组的秘书职位。

TEAS 目前有 22 篇工作组文稿，有 14 篇是和 TE 和 ACTN 架构的 YANG 模型相关。TE 相关的 RSVP-TE YANG，SR-TE 相关的 YANG 已经稳定，计划 WGLC。

TE/VN 相关 YANG 模型更新

Dhruv 宣讲了三篇 TE VN 相关 YANG 模型的进展。

https://datatracker.ietf.org/doc/html/draft-ietf-teas-actn-vn-yang-13

ACTN VN 模型，KDDI 实现，根据部署扩展了预计算路径 RPC 的需求，本次增加了基于 COS 进行 VN-member 的路径计算。VN 和 TE-topo 紧绑定，TE 路径只支持 TE 隧道，无法支持 SR TE，VN 需要扩展，但并无运营商有需求，目前只增加了一个 underlay container 作为后续扩展建议。

https://datatracker.ietf.org/doc/html/draft-ietf-teas-actn-pm-telemetry-autonomics-07

ACTN TE 及 VN 性能监控模型以及根据性能 metric threatthold 自动扩缩容模型，添加 VPN PM 的关系说明，及相关编辑性修改。

https://datatracker.ietf.org/doc/html/draft-ietf-teas-te-service-mapping-yang-09

TE service mapping 解决 LxSM/LxNM 隧道映射策略配置，给出了 VPN 模型与 TE-topo，TE-Tunnel，SR-policy 的映射；工作组主席建议 TE service mapping 模型只解决 LxSM/NM，VN，TE 映射，并尽快 WGLC，不建议该文稿解决切片的 mapping。

网络切片定义与通用架构文稿更新

https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slices-05

IETF 网络切片文稿由 Adrian 作为 editor 在会前进行了更新，主要包括对术语的更新，对切片内业务需求描述方式的修改，以及网络切片的实现架构与流程。文稿中对切片的 endpoint 描述进行了更新，增加一种 ancillary CE 的类型，具体内容请见文稿。

文稿中定义了基于 connectivity matrix 描述切片内的连接和 SLO 需求的方式，以及 connectivity matrix 的类型在会上引起较多的讨论，未能达成一致，将在会后继续讨论。

IETF 网络切片北向业务模型文稿更新

https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slice-nbi-yang-00

对应 IETF 切片架构文稿对业务需求的描述，切片的业务模型建模需要考虑几个问题：

1）NS framework 中 1 个切片业务多个 Connectivity Matrix 如何建模；

2）Juniper 希望增加 connection-group 描述，单 NSE point 关联的 connection 的带宽约束；

3）Juniper 切片 Tag 用于关联 5G S-NSSAI, 切片 traffic class 定义；

现场的问题集中在对 Connectivity Matrix 的建模。Kireeti Kompella 认为组播 connection 描述复杂，不同 path 可能 delay 不同。xufeng liu 反对一个切片业务支持多个 connectivity matrix，建议 client 通过多个切片业务来支持多个 connectivity matrix。

网络切片实现相关文稿更新

1）Realizing Network Slices in IP/MPLS Networks

https://datatracker.ietf.org/doc/html/draft-bestbar-teas-ns-packet-05

Juniper 的 Tarek 在 TEAS 工作组宣讲对 bestbar-ns-packet 文稿的更新，其中主要的修改是将原来描述切片 underlay 的术语 slice aggregate 替换为 network resource partition，同时将 slice aggregate 重新定位为切片业务流的聚合。Juniper 再次向工作组申请发起 adoption。

2）VPN+/VTN 扩展性分析与优化

https://datatracker.ietf.org/doc/html/draft-dong-teas-enhanced-vpn-vtn-scalability-04

华为董杰在会上对 VPN+和 VTN 术语体系进行了回顾，并介绍了 VTN 在控制面和数据面的扩展性优化方案，并表示文稿内容已经成熟稳定，向工作组申请发起 adoption。表示文稿除了术语之外，其他内容已经 stable，可以在确定新术语之后 adoption。主席表示将在邮件列表发起流程，Juniper 表示希望文稿使用通用术语 Network Resource Partition 替换目前的术语 VTN。

3）Slice Policy YANG

https://datatracker.ietf.org/doc/html/draft-bestbar-teas-yang-slice-policy-02

Juniper 的 Tarek 宣讲了 Slice Policy YANG 模型文稿，并申请工作组 adoption。会上对这文稿提出术语和内容等方面的多项意见，说明文稿当前还不够成熟。

Dhruv 对术语提出疑问，认为 Slice Policy 不够准确；Robin 认为目前数据面切片 ID 的封装格式定义还不确定，无法定义 YANG 模型；吴波指出该模型无法描述 per link 的带宽（Tarek 认为 topology filter 关联的 PHB 适用），并建议补充例子说明 NRP 对应三种模式的的 CP, DP 配置。

Juniper 在 bestbar-ns-packet 文稿中定义了大量新的术语，使得 slice aggregate，slice selector，slice policy 与切片业务以及切片 framework 中描述的 NRP(Network resource partiontion)之间的关系描述很不清晰，也影响这篇 YANG 模型文稿的描述。此外，Juniper 的切片方案定义了三种模式，DP，CP，CP+DP，而 CP 的切片采用 RSVP-TE 或 PCE 进行资源预留；Juniper 声称该模型主要是 device 模型，但也适用于 controller。。

4）YANG Data Model for Topology Filter

https://datatracker.ietf.org/doc/html/draft-bestbar-teas-yang-topology-filter-02

来自 Juniper 的工作组主席 Pavan 宣讲了 topology filter 的 YANG 模型，在物理拓扑，L3 逻辑拓扑(MT、Flex-Algo)或 TE 拓扑的基础上叠加亲和属性约束，得到过滤后的定制拓扑。Juniper 意图将 topology filter 作为一种通用的定义拓扑约束的机制，并在 Slice Policy YANG 模型中引用了这一模型来定义 Network Resource Partition（资源切片）的拓扑。

会上 Susan Hares 对 topology filter 与 routing filter 的关系提出疑问，Juniper 文稿作者做了澄清。华为指出 topology filter YANG 模型和 PCEP 扩展的内容存在不一致，对于 topology filter 的用法和流程也需要进一步说明。

端到端网络切片相关文稿

1. 5G 端到端网络切片映射

https://datatracker.ietf.org/doc/html/draft-geng-teas-network-slice-mapping-04

文稿新加入 Nokia 合作者 Reza，本次由 Reza 进行宣讲。文稿主要是简化了对 3GPP 切片相关内容的描述，更加便于理解。另外文稿也澄清了 IETF 切片对接标识和 IETF 网络切片标识的术语含义，也可以使用现有的标识实现。文稿收到来自多方的积极反馈意见，多个运营商表示认同切片映射的重要性。会上申请发起 WG adoption，主席建议在邮件列表继续讨论，后续有望接受为工作组文稿。

2. 端到端 IETF 网络切片架构

https://datatracker.ietf.org/doc/html/draft-li-teas-e2e-ietf-network-slicing-01

李振斌宣讲了端到端 IETF 网络切片的架构文稿，文稿的主要内容是如何在数据面，控制面和管理面实现端到端切片的打通，以及跨多域的网络切片拼接。会上的主要意见是需要说明与 IETF 网络切片文稿的关系，另外“端到端切片”特指 5G 网络切片，需要避免产生混淆。

意图路由

https://datatracker.ietf.org/doc/html/draft-li-teas-intent-based-routing-00

李振斌宣讲了意图路由文稿，主要内容是通过数据面的 intent ID 实现灵活的转发策略，将数据包映射到 SR Policy，切片或其他的转发流程。会上对于 intent 的含义有较多讨论，另外 TEAS 工作组主席希望邮件讨论和确定文稿属于哪个工作组。

25. PCE

工作组整体介绍

1. draft-ietf-pce-binding-label-sid 已经到 ADreview 阶段，等待 ADreview，即可推动后续 RFC 发布。AD John Scudder 表示会尽快处理。

2. Nokia Andrew 表示 draft-ietf-local-protection-enforcement 已经稳定，请求继续推动。

宣讲内容

1．draft-ietf-pce-multipath-03

思科 Mike 介绍 PCEP 支持 SR policy 中 Candidate path 支持多 SID List 的方案。文稿扩展了基于 Path ID 来绑定正反向 SID List。该方法与基于 Path Segment 表示正反路径的方法有一定的类似。华为李呈建议和基于 Path Segment 的 SR 正反路径文稿作者展开讨论，梳理正反路径实现方案的细节。Loa 表示 SR 双向隧道和这篇多路径的双向隧道内容可以合并。近期将与思科讨论如何支持 SID List 级别正反路径的问题，争取将 Path Segment 加入到 SID List 级别的属性中，从而满足 SID list 级别 path Segment 携带的问题。

2． draft-ietf-pce-segment-routing-policy-cp-06

思科 Mike 介绍 PCEP 支持 SR policy 文稿并表示思科和 juniper 已经基于 vendor TLV 来做了验证。Nokia 表示近期也做了原型进行了验证，目前看还没有到版本落地阶段。

3． draft-li-pce-pcep-pmtu-05

MTN 客户 Fabrice 宣讲了 PMTU 的 PCEP 文稿，现场没有问题，将加入到接收队列中等待接收。

4． draft-chen-pce-sr-ingress-protection-06

陈怀莫宣讲了 SR 头节点保护方案，文稿描述了为 SR 和 BIER-TE 路径提供保护的方案。主席 Dhruv 询问是否可以支持其他类型的数据保护。主席质疑为什么不做成通用的方法，通过 Path Setup Type 来为不同的路径类型提供帮助。中兴张征建议先到 SPRING 和 BIER 工作组讲 use case 再到 PCE 来讲扩展。思科 Mike 询问是否需要在 CE 设备上建立连接状态，回复无需建立连接。主席 Dhruv 建议解决当前的 comments 再继续推动。

PCEP 更新文稿

1． draft-dhody-pce-pcep-object-order-00

主席 Dhruv 宣讲了关于放宽 PCEP Object 必须按照 RFC5440 里面定义的顺序处理的草案。现场 Nokia andrew 表示对后向兼容上有风险。可能为了长期的可互通性而带来了短期无法互通的风险。主席 Julien 回复这只是第一稿，还需要收集工作组的建议，看看最终如何决策。

电信王爱俊表示这样可能失去了定义顺序的意义。主席 Dhruv 回复这主要是希望遵循协议涉及里面的发送端严格编码，接收端宽容处理的哲学。举例 RSVP-TE 也支持无需的 object 处理，PCEP 理应也可以支持。Nokia，Cisco 等工程师展开讨论，觉得需要将这个能力发布出去，从而支持后向兼容。

2．draft-xpbs-pce-topology-filter-01

中兴熊泉宣讲了 Topology filter 文稿，华为董杰表示华为已经提交了 VTN 的扩展文稿，并表示原来的文稿一拆二，是否会影响 topology filter 的定义完整性，需要澄清这个文稿定义的内容和 YANG model 文稿的内容。熊泉表示文稿在两年前就提出来了，但由于 TEAS WG 对于切片 ID 的术语还未统一，所以还没有写在这个版本里面，会考虑后续增加。主席表示请作者关注 TEAS 的进展，并会基于 TEAS 的进展决定 PCE 如何推动。

3．draft-dong-pce-pcep-vtn-00

董杰宣讲 PCEP 携带 VTN ID 的扩展。Juniper Tarek 表示 TEAS 已经明确切片 ID 为 NRP-ID，担心这个文稿会带来一个功能两个 ID 的问题。建议和中兴文稿合作，解决问题。主席对是否达成一致表示怀疑，建议后续明确结论后推动。关于 VTN-ID，表示来自 VPN+，其概念比网络切片大。网络切片框架 editor Adrian 表示还没有对术语达成一致。但是可能不会强迫大家修改各自方案的术语。只会达成一个基本的技术定义，然后各自厂商的方案可以解释自己的方案如何映射到这个基础技术框架上。

4．draft-dhodylee-pce-pcep-ls-22

Verizon Gyan 宣讲 PCEP-LS 文稿，华为李呈，李振斌表示支持这个工作，希望继续标准化。

组播相关文稿

1． draft-li-pce-based-bier-02

电信李华南宣讲了基于 PCEP 支持 BIER 的文稿。主席表示需要和 BIER 工作组联合讨论后续的工作进展。并表示文稿中包含了非 BIER 的内容，会带来误解。Gyan 表示文稿需要只关注 BIER 上。非 BIER 的已经在 RFC6006 里面定义了。

其他文稿

1． draft-rajagopalan-pce-pcep-color-00

Juniper 宣讲了通过 PCEP 携带 Color TLV 的文稿。主席表示需要明确 TLV 携带的位置。回复携带位置取决于应用，可能在 LSPA OBJECT, 可能在 Path-attribute object。

2．draft-wang-pce-vlan-based-traffic-forwarding-01

电信宣讲基于 VLAN 的数据包转发。王爱俊解释了这是一种类似于 MPLS 转发的机制，但可以部署在 Native IP 场景。他们将会努力与 PCEPCC 机制对齐，从而支持 PCE 作为控制器配置 VLAN 等信息。

26. MSR6

会上议题

1. 主席介绍 MSR6 Side Meeting 的背景，运营商为了应对逐步增长的实时网络业务，IPv6 的趋势，介绍 MSR6 的需求，设计理念和思路；

2. 中国移动介绍 MSR6 BE 的基本应用场景，包括单 AS 域，跨 AS 域，以及面对直播场景的组播源路由需求，同时给出了基于 IPv6 DoH 的 MSR6 BE 方案；

3. 中国电信介绍 MSR6 BE 的潜在技术方案，包括基于控制器的 MVPN 方案，以及基于 IPv6 RH 的 MSR6 BE 方案；

4. Verizon 介绍运营商在组播 TE 方面的现有技术方案，以及面对 IPv6/SRv6 的发展趋势，对于基于 IPv6 的组播源路由方案的需求；

5. 介绍 MSR6 TE 的两种潜在方案，定义新类型的 Routing Header，并在 segment list 中进行组播树的编码，用于显式指定组播路径；

6. 中国联通介绍了现网在 IPv6/SRv6/切片的部署进展，以及联通在组播切片，组播故障定位，以及组播测量方面的需求；

7. 中国移动介绍 SD-WAN 的组播应用需求，以及基于此，在组播流量加密方面的需求；

参会情况和会上讨论

1. MSR6 Side Meeting 参会人数 70 人左右，除了国内三大运营商，KPN，Verizon，Telefonica，Nokia，Juniper，H3C，ZTE 等参加了 Side Meeting；

2. Juniper 在会上提问，询问与 BIER，PIM 工作组现有工作的关系，以及除了 IPv6 封装之外的新的组播需求； 中移动回应说，MSR6 的工作组独立于其他工作组，提供不同的技术选项，同时可以充分借鉴 IETF 现有的技术思路，如 SRv6, BIER 等；

3. BIER 工作组主席 Greg 提问，MSR6 是否是在推动某一厂商的已实现方案；华为回应说 MSR6 是开放话题，希望更多的厂商参与贡献；

4. 中国联通和电信表示希望有新的工作组来讨论基于新需求的组播方案。