

IETF115 工作组会议总结

工作组

LAKE

主席：Stephen Farrell (Trinity College Dublin), Mališa Vučinić (Inria)

工作组旨在针对 OSCORE 协议设计一个轻量级的认证密钥交换协议（OSCORE 协议是 CoAP 协议的应用层安全机制，CoAP 协议可看作是适用于物联网的 HTTP 协议），即 Ephemeral Diffie-Hellman Over COSE (EDHOC)。面向物联网场景，该协议的一揽子标准化文稿可以为轻量化安全协议的研究提供参考。

主要玩家：以 Ericsson、RISE、Inria 等一系列欧洲的公司和研究院为主。

工作组文稿：

Ephemeral Diffie-Hellman Over COSE EDHOC (draft--ietf-lake-edhoc-17)

作者：John Preuß Mattsson & Göran Selander (Ericsson)

背景：Ericsson 主推的密钥交换协议，使用 CBOR 编码、COSE 加密、CoAP 传输，能实现双向认证、前向安全性、以及身份保护。Ericsson 已与法国 Inria、瑞典 RISE 研究院等研究机构在此方向有合作，完成了协议的开源实现 (<https://github.com/lake-wg/edhoc>)。

进展：本次主要介绍了针对 WGLC 中的意见的更新情况，计划于 11 月提交更新版，准备发布。

Traces of EDHOC

作者：John Preuß Mattsson & Göran Selander (Ericsson), Marek Serafin (ASSA ABLOY), Marco Tiloca (RISE)

背景：文稿包含 EDHOC 协议端 (Initiator) 到端 (Responder) 认证测试运行中逐消息的注解，输入、输出和中间处理结果，以及部分简化实现的测试，测试主要分为两类：

X.509 证书 hash 值标识签名密钥。身份认证采用 ECDSA，临时密钥交换采用 X25519；

身份认证采用 CWT 声明集合标识的静态 DH 密钥，临时与静态密钥交换均采用 NIST P-256。

进展：准备 WGLC，广泛吸纳 comments，发布时间不设限。

个人文稿：

Lightweight Authorization for EDHOC (draft-selander-lake-authz-00)

作者：John Preuß Mattsson & Göran Selander (Ericsson), Michael Richardson (Sandelman Software Works), Mališa Vučinić (Inria), Aurelio Schellenbaum (ZHAW)

背景：LAKE WG 新文稿，文稿前期在 ACE (Authentication and Authorization for Constrained Environments) WG 推了近三年，未能成为工作组文稿；目前已经存在开源代码 (<https://github.com/EricssonResearch/ace-ake-authz>) ；

文稿主要将入网权限验证流程嵌入到 EDHOC 中，即注册设备入网前，服务器将向第三方权威服务器查证注册设备入网的权限情况；

进展：由于时间有限，未组织现场讨论。Marco Tiloca (RISA)通过 mailing list 给了意见，作者准备根据意见修改下次再上会。

OCSP Stapling for EDHOC (Certificate Revocation in Resource Constrained Environments)

演讲者：Yousef AbdElKhalek (RISE)

背景：演讲者 2022 年在 TU Berlin 的硕士毕业论文。核心思想是通过利用 OCSP 与 EDHOC 来实现证书撤销：受限设备选择可信 OSCP 响应节点，并通过 EDHOC 请求消息要求 EDHOC 响应方去该 OSCP 节点处请求可信消息附带在 EDHOC 响应消息上，从而将证书撤销查验的操作从资源受限链路迁移到 EDHOC 响应节点与 OSCP 响应节点之间的链路上。部分实现链接 (<https://github.com/eriptic/uoscore-uedhoc>) 。

进展：作者当前还未写文稿，只是针对此想法来征求意见，表示会后根据 mailing list 意见决定是否提交 draft。

Guidelines for EDHOC Implementations (Certificate Revocation in Resource Constrained Environments)

演讲者：Marco Tiloca (RISE)

背景：EDHOC 协议在实际实现过程中部分细节的考量并未纳入 EDHOC 协议范围，存在三方面：1) 身份认证凭据/应用密钥的失效/清除；2) 新的身份认证凭据在不同信任模型下的处理逻辑；3) 额外的处理（例如认证凭据的验证工作的加速等都会影响 EDHOC 协议的性能）。

进展：演讲者想提一个关于 guideline 的文稿，针对此想法来征求意见。主席表示在 EDHOC 发布之后，计划进行一次内部讨论，决定接下来工作的方向。

MPLS&PALS

会议时间：

MPLS: 11.8 周二下午, Session III

PALS: 11.9 周三上午, Session I

综述：约 60 人参加了本次 MPLS 工作组会议和 PALS 与 MPLS、Detnet 工作组的联合会。主要参与厂商为华为, Cisco, Juniper, Ericsson, Nokia, Ciena, Infinera, ZTE, 等, 主要参与运营商为 DT, BT, AT&T, Verizon, Orange, Telefonica, Liquid, 中移动, Tencent 等。

MPLS 工作组近期的主要工作仍是 MPLS Open DT, 近期主要在进行 MNA 封装方案的讨论。下一步的议题还包括如何基于 MNA 来支持 non-IP (PW) 业务。

MPLS 相关的 YANG 模型和 OAM 机制的更新和扩展也是一个持续推进的方向。工作组近期新接纳的工作组文稿为 Futurewei 牵头的 draft-ietf-mpls-msd-yang。

MPLS session 会上议题情况：

A YANG Model for MPLS MSD

draft-ietf-mpls-msd-yang-00

Yingzhen Qu

Futurewei 的 Yingzhen 宣讲了文稿的更新。Cisco 的 Ketan 表示 MSD type 中包括 MPLS 和 SRv6 两类, 建议文稿对此进行明确和限定。

Simple Two-way Active Measurement Protocol (STAMP) for MPLS Label Switched Paths (LSPs)

draft-mirsky-mpls-stamp-01

Greg Mirsky

Ericsson 的 Greg 宣讲了 MPLS 的 STAMP 扩展文稿。Tarek 询问方案与现有 MPLS 性能测量机制相比有什么优势，Greg 表示 STAMP 除了检测丢包和时延之外，还可以用于检测乱序和重复报文。Matthew 和 Rakesh 认为文稿需要对一些技术细节进行澄清。

LSP Ping/Traceroute for Enabled In-situ OAM Capabilities

draft-xiao-mpls-lsp-ping-ioam-conf-state-00

Xiao Min

ZTE 的肖敏宣讲了这篇 00 版文稿。Tarek 表示在多数情况下更希望在 LSP 建立之前收集设备的 IOAM 能力信息，而文稿的方案需要先有 LSP，再进行能力发现。Tarek 认为 IGP 可能是更合适的选择。

PALS & MPLS & Detnet Joint session 会上议题情况：

Open DT Report

Tarek Saad

Cisco 的 Tarek 介绍了 Open DT 的整体进展情况：

- MNA use case 文稿近期增加了一些新的 use case，后续将继续完善现有的 use case，并可能增加新的 use case。
- MNA requirements 文稿进行了一次更新，以解决 Adrian 的部分 comments。作者认为文稿后续可以发起 WG LC。
- MNA 架构文稿根据例会的讨论补充了一些内容，作者认为后续可以发起 WG LC。
- MNA 方案文稿从多篇文稿逐渐开始收敛为 1 篇 ISD 封装文稿和 1 篇 PSD 封装文稿。
- 关于 MNA action 的执行顺序和作用范围的讨论在 framework 文稿中有相关描述，对方案文稿也提出了一些要求。

- 工作组对现有设备的 MPLS 标签栈处理进行了问卷调查，结果发布在 draft-farrel-mpls-forwarder-poll-response 中。

Requirements for MPLS Network Actions

draft-ietf-mpls-mna-requirements-04

Matthew Bocci

Nokia 的 Matthew 宣讲了 MNA 需求文稿的更新进展。他指出需求是针对协议设计，而不是产品实现。认为文稿附录中的 adoption call 问题已经被解决，因此在这一版本更新中删除了附录。华为董杰表示之前反馈过一些 comments，需要确认是否在新版本中得到解决。

MPLS Network Action (MNA) Header Encodings

draft-jags-mpls-mna-hdr-03

Jaganbabu RAJAMANICKAM

Cisco 的 Jags 宣讲了 MNA In-Stack Data 封装文稿的更新版。经过前段时间的 Open DT 会上会下讨论，目前这一版本有包括 Cisco, Futurewei, Juniper 的多家设备商合署，Broadcom 也是文稿合作者之一。文稿经过几次的更新之后，内容更加完善，不过也显得方案比较复杂，这在会上引起了一些人的担心。Joel Halpern 认为方案中有冗余的部分，而对于 action order 的指示机制，建议考虑更利于实现的方式。Joel 和 Matthew 认为当标签栈中的所有 ISD 弹出时，PSD 是否需要弹出以及如何弹出是一个要考虑的问题。

MPLS IOAM

draft-gandhi-mpls-ioam

Rakesh GANDHI

Cisco 的 Rakesh 宣讲了 MPLS IOAM 文稿的更新。文稿基于 MNA 的 ISD 和 PSD 封装方案携带 IOAM 信息。Ericsson 的 Greg 认为当 IOAM 携带逐跳增加的信息时，报文头的封装开销会很大，而且通过 PSD 携带时的写入性能也会较差，认为不是所有的 IOAM mode 都适用于 MPLS。

BFD Extension for DetNet Remote Defect Indication (RDI)

draft-huang-detnet-rdi

Hongyi Huang

华为黄弘毅宣讲文稿，提出基于 BFD diagnose code 传递性能下降信息。Juniper 的 Jeff Haas 指出 BFD 不适合用于这类功能，Greg 此前有篇文章定义类似的功能，可以考虑进行合作。

Echo Request/Reply for DetNet Capability Discovery

draft-tan-detnet-cap-discovery-00

Ren Tan

文稿介绍一种扩展 echo request/reply 机制发现设备的 Detnet 能力的方案。会上没有收到反馈意见。

Open Discussion on MNA

Stewart 认为会上的反馈意见体现出还需要继续通过 Open DT 进行方案的讨论，Loa 认为需要重新审视方案的复杂性。

包括 Adrian, Matthew, Haoyu 和董杰等多人在会上公开讨论中都表示可能需要重新审视 use case，简化需求文稿，比如对灵活指定 action order 的需求可能并不是必要的。Matthew 还建议对架构文稿的描述进行加强，参考 MPLS-TP 和 PW 的架构。

Juniper 的 Tony Li 和 Kompella 前期是部分新需求的提出者，本次也认为前期讨论的一些需求可能缺少真实的 use case，导致方案过于复杂。

路由域 AD Andrew 作为运营商给出的观点是如果方案过于复杂，会导致实现的周期很长，而且容易出现 bug，最终会导致运营商并不想使用该方案。

IDR

会议时间：11.7 周一下午，Session II

综述：约 110 人参加了本次 IDR 工作组会议。主要参与厂商为华为，Cisco，Juniper，Arccus，Ciena，Nokia，ZTE，锐捷等，主要参与运营商为中国移动，中国电信，中国联通，Orange，DT，Bell Canada，Verizon，AT&T，Google，Amazon，KDDI 等。

工作组近期的主要工作聚焦在 BGP 跨域意图路由方案（包括 BGP CAR/CT/CPR）以及 CAR/CT 互通方案，BGP Next-hop 相关扩展方面。此外 BGP Flowspec 相关文稿的更新和扩展也是一个持续推进的重要方向。

工作组近期接纳的工作组文稿包括：华为与移动合作的 Flowspec SR Policy 引流 (draft-ietf-idr-ts-flowspec-srv6-policy)；更新的 BGP entropy label 扩展。华为的另一篇文稿 draft-dong-idr-node-target-ext-comm 完成了 WG adoption call，目前正在由工作组主席进行 call 的结果评估。

会上议题情况：

Distribution of Traffic Engineering (TE) Policies and State using BGP-LS

draft-ietf-idr-te-lsp-distribution

Ketan Talaulikar

文稿定义了通过 BGP-LS 上报 TE 隧道和 SR Policy 状态信息的协议扩展。目前多家厂商只实现了 SR Policy 信息的上报，为了便于加快文稿的推进，作者建议将 SR Policy 部分和 TE 隧道部分拆成两篇文稿，主席认同对文稿拆分的提议，目前正在工作组中征求意见。

BGP YANG Model for Service Provider Networks

draft-ietf-idr-bgp-model

Mahesh Jethanandani

文稿近期的更新主要是和 TCP 模型配合进行安全相关内容 TCP-AO/MD5 的更新。目前模型还有一些正则表达式方面的遗留问题，例如对 AS Path 的表达方式统一，在 IETF 期间进行了 side meeting 讨论。此外扩展团体属性的表达也是一个待解决的问题。

Deprecation of AS_SET in BGP

draft-ietf-idr-deprecate-as-set-confed-set

Jeff Haas

文稿指出 BGP 的 AS_SET 属性带来的一些问题，包括对 ROV 的影响，此外也会影响其他的 BGP 相关的 Policy。文稿建议对带有 AS_SET 的路由执行 treat-as-withdraw 操作，

并对进行路由聚合的设备行为进行修改。会上讨论认为这一修改是可行的，不过文稿还需要进一步澄清。华为谭镇提出在部分部署了 AS_SET 的网络中可能引起业务中断问题，Jeff 建议把相关问题场景进行说明，并在邮件列表讨论。

BGP Extension for 5G Edge Service Metadata

draft-dunbar-idr-5g-edge-service-metadata

Linda Dunbar

Linda 介绍了 5G edge service 文稿对 BGP next-hop 的修改，next-hop 体现的是所连接的 site 的能力，建议定义新的路由属性来代表 service 信息。会上 Acee 表示不太理解这一用法，还需要会后进一步讨论澄清。

BGP SR Policy Extensions for metric

draft-zhang-idr-sr-policy-metric

Ka Zhang/Jie Dong

华为张卡/董杰宣讲了 BGP 下发 SR Policy 时携带 metric 信息的扩展。会上 Ketan 提问 metric 应该是 candidate path 粒度还是 segment list 粒度。工作组主席则建议在 SPRING 工作组也发起相关讨论，收集一下意见。

Connecting IPv4 Islands over IPv6 Core using IPv4 Provider Edge Routers (4PE)

draft-mishra-idr-v4-islands-v6-core-4pe

Gyan Mishra

Gyan 介绍了通过 IPv6 core 连接 IPv4 island 的方案，称为 4PE。作者希望对文稿发起 WG adoption。

BGP Flowspec for IETF Network Slice Traffic Steering

draft-dong-idr-flowspec-network-slice-ts

Jie Dong

华为董杰宣讲了 BGP Flowspec 扩展实现网络切片引流文稿，包括对切片 ID 的流匹配规则定义，以及定义实现封装数据面切片 ID 的流转发动作，支持引流到切片内的 BE 路径或 SR Policy。会上没有收到意见。

Problem statement of Inter-domain Traffic Redirection Risks

draft-cheng-idr-redirection-risks-ps

Weiqiang Cheng

中移动程伟强宣讲了对流量重定向导致的一系列问题的分析文稿。工作组主席 Jeff 建议这篇文稿更适合放在 GROW 工作组。Cisco Acee 认为 Flowspec 用于重定向并不是最初设计的目的，这也是导致问题的原因。与 Savnet 相关。

BGP for Mirror Binding

draft-chen-idr-mbinding

Huaimo Chen

Futurewei 的 Huaimo 宣讲了基于 BGP 下发 Mirror Binding SID 的机制，用于提供本地保护。会上 Nokia 的 Andrew 认为文稿的方案有一些缺陷，需要在会后进一步讨论。

Extended Communities Derived from Route Targets

draft-zzhang-idr-rt-derived-community

Jeffrey Zhang

Juniper 的 Jeffrey 介绍了一种新的 BGP 扩展团体属性，用于表达和特定 VPN 的关联关系。文文稿中列出了一些可能的应用场景，但作者表示并不会描述新属性的具体用法。Acee 提问是否需要专门的文稿来描述在特定场景下的用法，Jeffrey 表示对于其他 use case 可以单独写文稿描述。

BGP MultiNextHop Attribute

draft-kaliraj-idr-multinexthop-attribute

Kaliraj Vairavakkalai

Juniper 的 Kaliraj 介绍了 BGP multi-nexthop 属性的产生背景和可以实现的一系列功能。文稿在之前的 IDR 中期会议做过宣讲，当时没有展开讨论。会上 Keyur 对属性的发布范围和错误处理提出疑问，另外认为新属性功能很多，并不适合叫 multi-nexthop。Jeff Haas 则建议工作组对文稿进行 review，认为属于 next-hop 相关扩展的一部分。

TEAS

会议时间：11.8(周二)下午，Session II 和 Session III

综述：约 120 人参加本次 TEAS 工作组会议，主要参加厂商为思科，华为，Nokia，Ericsson, Ciena, Juniper 等，欧美运营商以及 Oracle, Microsoft, amazon 等。

本次的会议主题仍旧是网络切片，目前切片有多个不同层面的实现架构，包括控制面/转发面/管理面架构，VPN+, ACTN, RFC8309, NRP scalability, NS IP/MPLS 从不同的角度说明，网络切片对应的模型已经基本完整。

会上议题情况：

工作组整体进展：

流量工程 (TE) 架构文稿提交到 IESG review; IETF 网络切片架构文稿发起 WG LC，华为主推的 VPN+ 架构文稿已完成 IPR poll，后续将发起 WG LC;

WG Draft updates: 工作组主席说明当前 25 篇工作组草案进展，不在本次讨论中的文稿下一步计划，包括 ACTN VN, TE tunnel 等模型。

Updated Common YANG Data Types for Traffic Engineering

Draft: <https://datatracker.ietf.org/doc/html/draft-ietf-teas-rfc8776-update-01>

Presenter: Italo Busi

发布 RFC8776bis 草案。此前讨论 Option 2 采用 NETMOD 定义的 semver 方案，但 semver 未发布 RFC。

IETF Network Slice Use Cases and Attributes for the Slice Service Interface of IETF Network Slice Controllers

Draft: <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slice-use-cases-01>

Presenter: Luis M. Contreras

目的：切片用例以及业务属性，Telefonica 和 NTT 牵头，建议将切片定义为通用连接服务，用于描述业务的 SLA 特征

更新：本次增加了 DC 互联场景，为了解决 DC 互联(RoCE 场景，需要提供无丢包特性。草案中已描述 5G,SD-WAN 互联场景。

下一步：预计会后接纳为工作组草案,TEAS 工作组不想将切片只限定在 5G 场景,原本 CCAMP OTN slicing 希望切片只用于 5G 场景。

IETF Network Slice Service YANG Model

Draft: <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slice-nbi-yang-02>

Presenter: Reza Rokui

更新：本次宣讲了当前草案的关键 open issue,包括 peer-sap-id, custom topology 和 IP 相关的 opaque 属性。

意见：

- 传接在 CCAMP 工作组的 OTN Slicing 模型基于这篇草案扩展，不希望保留 SDP 及 AC 有关 IP 相关 opaque 属性；
- 另外希望业务模型中扩展拓扑模型，但经过 side meeting 沟通，同意引用 TE topology，用于进行 feasibility check 或 custom IP+光路径定制。
- 此外，本次会议 Telus 还建议补充一些切片的运维信息。

下一步：计划在解决这些 issue 后，发起 WGLC。有关技术相关属性的争议，会在模型中提供 placeholder，可以进行 technology specific 的扩展。

Instantiation of IETF Network Slices in Service Providers Networks

Draft: <https://datatracker.ietf.org/doc/html/draft-barguil-teas-network-slices-instantation-05>

Presenter: Luis M. Contreras

IETF Network Slice Controller and its associated data models

Draft: <https://datatracker.ietf.org/doc/html/draft-contreras-teas-slice-controller-models-04>

Presenter: Luis Contreras

目的: NSC 的 RFC8309 参考实现架构,较 VPN+的管理面, 列举了 NSC 实现的各种选择, 其他 Option 是 ACTN 架构中的 MDSC/PNC 如何支持实现切片功能。

更新: Luis 宣讲了两篇草案, Chair 发起了投票, 有 1/3 支持, 后续可能合并为一篇草案, 并进行工作组接纳。是一篇 informational 草案, 用于描述切片模型如何与现有的 LxSM/LxNM, TE tunnel 进行 mapping, 从而实现切片业务。

下一步: Chair Lou 认为有足够的兴趣, 会后可以进行 adoption。将建议作者增加 NRP YANG 及 slice service mapping 草案。

A YANG Data Model for Network Resource Partition (NRP)

Draft: <https://datatracker.ietf.org/doc/html/draft-wd-teas-nrp-yang-02>

Presenter: Bo Wu

更新:

- 介绍与 NRP policy 模型的差异, 主要区别是 A2A connectivity 的实现。
- 和 NRP policy 的 merge 状态, 说明后续会一个模型, 同时兼容分布式控制面和集中式 TE 控制面。

改进意见:

- 数据面 ID 会修改为 NRP selector,考虑到与 DSCP 的 class selector 的相似概念;
- NRP topology 定义将支持两种方式, Option1, 在 NRP 实例化显示指定 link, 或者 Option2 已创建的 filter topology。
- control plane 定义 NRP aware routing

下一步计划: 会后输出一个 merged model,争取下次 IETF 会前 WG adoption。

IETF Network Slice Application in 3GPP 5G End-to-End Network Slice

Draft: <https://datatracker.ietf.org/doc/html/draft-gcdrb-teas-5g-network-slice-application-01>

Presenter: Xuesong Geng

文稿是对 3 篇和 5G 网络切片应用、映射相关文稿的合并。文稿合作者对文稿结构和内容进行了持续讨论和更新，目前的遗留问题包括：是否需要体现 5G 网络内部的技术差异，此外还有一些术语需要确定。会上工作组进行了投票，一部分人认为文稿还需要进一步完善。

A Realization of IETF Network Slices for 5G Networks Using Current IP/MPLS Technologies

Draft: <https://datatracker.ietf.org/doc/html/draft-srld-teas-5g-slicing-02>

Presenter: Julian Lucek

Juniper 的文稿作者介绍了如何使用现有的 IP/MPLS VPN 和 TE 技术满足 5G 网络切片的需求。华为耿雪松表示文稿与上一篇 5G 网络切片应用文稿有一部分重叠，希望能够共同协调。华为董杰表示文稿只是提供了一种实现 5G 网络切片的选项，希望说明文稿的适用范围和限制。

IETF Network Slice Service Mapping YANG Model

Draft: <https://datatracker.ietf.org/doc/html/draft-dhody-teas-ietf-network-slice-mapping-02>

Presenter: Dhruv Dhody

目的: 切片业务模型 mapping 草案, 可以是 NSC 的内部实现, 也可以用协同器与域控制器间接口。此前 TE service mapping technology 不包含切片业务。

下一步: 争取在 NRP YANG 接纳后, 进行 WG adoption。

Traffic Mapping YANG model for Traffic Engineering (TE)

Draft: <https://datatracker.ietf.org/doc/html/draft-dhody-teas-te-traffic-yang-03>

Presenter: Dhruv Dhody

目的: TE 流 mapping 模型。

意见: Charles eckel 认为 SD-WAN 有类似定义, 还包含了 application id。Lou 认为和 ACL 模型重复, 或者是 route policy 重复。

YANG Data Model for Topology Filter

Draft: <https://datatracker.ietf.org/doc/html/draft-bestbar-teas-yang-topology-filter-04>

Presenter: Vishnu Pavan Beeram

目的: 用于 pre built topology filter。

意见: 华为董杰认为模型定位过于局限, 只适用于集中式算路的场景, 对于分布式算路的 MT 或 Flex-Algo 并不适用。

下一步: Chair Lou 投票认为支持者不足。

Precision Availability Metrics for SLO-Governed End-to-End Services

Draft: <https://datatracker.ietf.org/doc/html/draft-mhmcsfh-ippm-pam-02>

Presenter: Greg Mirsky

定义了更精确的 SLO 指标, 例如统计信息。TE, BGP-LS 等大多数标准当前只是平均时延, 或最长时延。需要 OAM 功能确认对 SLO 指标定义的影响, 例如 E2E 时延 99%报文不能超过 20ms, 99.999%不能超过 25ms, 任何报文不能超过 30ms。

Applicability of ACTN to Packet Optical Integration (POI) extensions to support Router Optical interfaces

Draft: <https://datatracker.ietf.org/doc/html/draft-mix-teas-actn-poi-extension-00>

Presenter: Gabriele Galimberti/Jeff Bouquier

Cisco 牵头用于补充 draft-ietf-teas-actn-poi-applicability(Applicability of ACTN to Packet Optical Integration (POI)),IP+光自动部署, 需要一组 YANG 模型, 这篇草案分析了 Gap, 建议定义 interface YANG 扩展 ietf-ext-xponder-wdm-if 支持 IP 路由器的 DWDM optical 接口配置。Juniper Chair Pavan 建议和现有 POI 文稿合并, 作者提到已经在 POI DT 讨论, 目前是 00 稿, 还需要进一步讨论。

6Lo

会议时间：2022/11/9

主要议题：

Draft/topic	Link	Presenter	Role/Company
Introduction and draft status		Bhandari/Gomez	Chair
Update of Transmission of IPv6 Packets over NFC	https://datatracker.ietf.org/doc/html/draft-ietf-6lo-nfc-18	Younghwan Choi	韩国大田大学
Status update of 6lo Applicability & Use Cases	https://datatracker.ietf.org/doc/html/draft-ietf-6lo-use-cases-14	Yong-Geun Hong	韩国大田大学
IPv6 ND Multicast Address Listener Registration	https://datatracker.ietf.org/doc/html/draft-ietf-6lo-multicast-registration-11	Pascal Thubert	Cisco
IPv6 ND Prefix Registration	https://datatracker.ietf.org/doc/html/draft-thubert-6lo-prefix-registration-01	Pascal Thubert	Cisco
Path-Aware Semantic Addressing for LLNs	https://datatracker.ietf.org/doc/html/draft-li-6lo-path-aware-semantic-addressing-00	Luigi Iannone	Huawei (巴黎数据通信网络算法实验室)
Reliability Considerations of Path-Aware Semantic Addressing	https://datatracker.ietf.org/doc/html/draft-li-6lo-pasa-reliability-00	Luigi Iannone	Huawei
Transmission of SCHC-compressed Packets over IEEE 802.15.4	https://datatracker.ietf.org/doc/html/draft-gomez-6lo-schc-15dot4-04	Carles Gomez	西班牙加泰罗尼亚理工大学
IP Payload Compression excluding transport layer	https://datatracker.ietf.org/doc/html/draft-ls-6man-ipcomp-exclude-transport-layer-00	Hang Shi	Huawei

Introduction and draft status

主要介绍了一下目前的工作组文稿状态，6lo-nfc 和 6lo-use-case 都在等待 IESG 评估。

WG Drafts Status

IPv6 over PLC (RFC Editor Queue)

<https://tools.ietf.org/html/draft-ietf-6lo-plc-11>

IPv6 over NFC (IESG Evaluation)

<https://tools.ietf.org/html/draft-ietf-6lo-nfc-18>

6lo Use Cases (IESG Evaluation)

<https://tools.ietf.org/html/draft-ietf-6lo-use-cases-14>

IPv6 ND Multicast Address Listener Registration

<https://tools.ietf.org/html/draft-ietf-6lo-multicast-registration-11>

Update of Transmission of IPv6 Packets over NFC

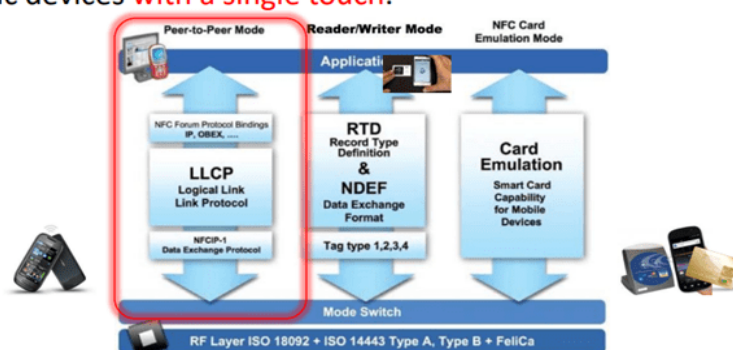
NFC 有三种模式点到点模式、读写模式、NFC 卡仿真模式，文稿是针对点对点模式的扩展。

What is Near Field Communication (NFC) ?

- **NFC technology enables** (Source: NFC Forum)
 - simple and **safe two-way interactions** between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices **with a single touch**.

- **NFC Functions**

(Source: NFC forum)



IETF114 的时候 Erik 给了一些 comments。

- 修改安全考虑，增加了增加了通过 LLCP(Logic Link Control Protocol)协议安全传输数据的考虑和 NFC 短地址的安全考虑；
- 增加对 RFC3756 的引用；

后续准备完成第 19 版修订；

Status update of 6lo Applicability & Use Cases

本次主要更新：

- 更新了附录部分，解决了 Robert Sparks 的 comment，附录 A 既不是介绍也没有在文章主体部分引用，为什么会在这里出现？
- 附录 A 是部署相关信息，是有必要保留的，在 introduction 部分增加了对附录 A 的引用
- 更新了安全考虑部分，Robert Sparks 的 comment，认为目前的内容还不够，本节应该说明为什么需要 L2 安全，以及解释如果不提供安全，会带来什么威胁。

IPv6 ND Multicast Address Listener Registration

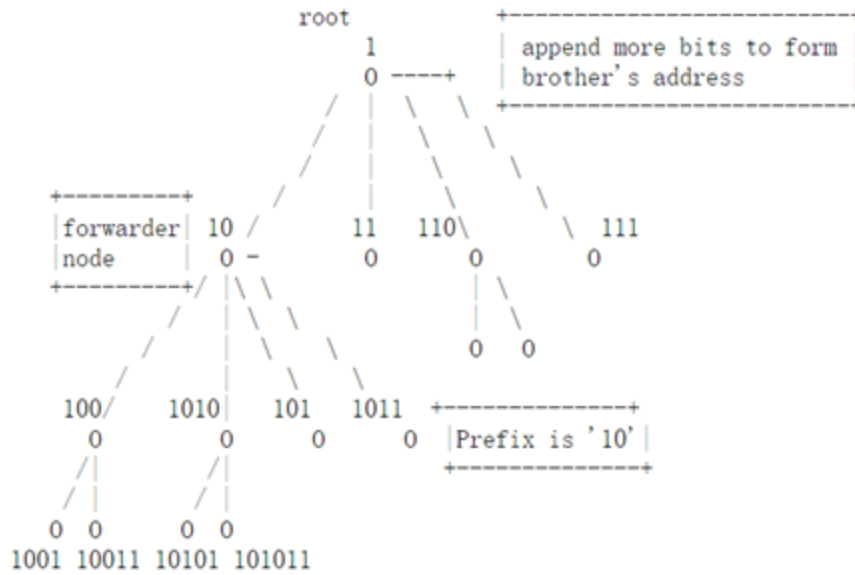
介绍了针对低功耗网络的组播地址侦听方案，IPv6 的多播不适用于 6Lo 的原因是低功耗设备多数时间处于休眠状态，不会响应查询，而且广播会浪费大量能耗与 6lo 的初衷不符。本篇文稿在 roll 工作组也进行了宣讲。AD 说可申请工作组 last call，会和 6man 一起看。

IPv6 ND Prefix Registration

在多播地址注册的基础上再进行扩展，当低功耗节点连接到一个前缀网络（该网络不一定运行了 RLP 协议）时，通过在服务路由器上前缀注册，可以使低功耗节点接收到指定前缀的所有流量，然后再在子网内进行转发。现场没有评论和问题，主席建议大家读一下文稿，提一些意见。

Path-Aware Semantic Addressing for LLNs

本次主要更新：补充了 use case 章节，增加了报文头部格式章节。方案主要是针对稳定拓扑，允许不携带全长地址的链路上传输 IP 数据包的情况，根据网络拓扑来生成设备地址。数据包转发是无状态的，路由器不需要构建路由表，转发决策仅基于目的地址结构。



Tommaso 问为什么不用 GHC 或者 SCHC 压缩方案（目前用的是 6lowpan 的 IPHC）？作者说不排除使用这两种方式，但是目前没有使用，IPHC 是够用的。Dsko 认为在智能家居和 PLC 场景下没有分层寻址的必要，作者认为即使是智能家居也有可能分层的，可以看 use case 章节。

Reliability Considerations of Path-Aware Semantic Addressing

主要一些考虑包括多地址情况（每个节点多个地址，每个地址对应一个父节点）、单地址情况（每个节点一个地址）、链路/节点错误检测和恢复（多地址情况下，链路故障后节点将其当前地址，称为次父节点的子节点；单地址情况下，链路故障后根节点重新计算路径，分配新地址）、可靠性几个部分。

Transmission of SCHC-compressed Packets over IEEE 802.15.4

SCHC 的压缩方案相比于 6LoWPAN 有更大的压缩效率，能延长设备的电池使用时间；

- IPv6/UDP/CoAP header size

b) Table 6, RFC 8824

	IPv6/UDP (bytes)	CoAP (bytes)		TOTAL (bytes)	
		a)	b)	a)	b)
No compression	48	4	16	52	64
6Lo(WPAN) - RFC 6282	7	4	16	11	23
SCHC - RFC 8724, 8824	1	1	1	2	2

- SCHC: static context, a priori knowledge of header field values
- Theoretical battery lifetime improvement over IEEE 802.15.4 by a factor up to >2
 - **Actual improvement will be lower**, depending on device HW, MAC/adaptation/application layer settings, payload size, network topology, etc.

该文稿主要介绍了如何在 6LoWPAN 环境下使用 SCHC 的压缩报文头，如何在 IEEE 802.15.4 上携带 SCHC 压缩报文头。

工作组 adoption 现场投票 16 支持，0 反对。

IP Payload Compression excluding transport layer

现有的 IPComp 将载荷部分全部压缩了，但是传输层的信息如源端口、目的端口在传输中是有用的，因此提出一种排除传输层信息的载荷压缩方案。此外针对部分未压缩报文导致的乱序问题，可以针对每个报文都增加压缩头或者为没有压缩的报文使用新的 CPI 来解决。没有问题讨论，主席建议把文件的链接放出来，让大家有时间去读一下。

RATS

主席: Kathleen Moriarty (CIS), Nancy Cam-Winget (Cisco), Ned Smith (Intel)

Remote Attestation Procedures Architecture

<https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/>

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

进展: 当前文稿已完成 IESG Review 进入 RFC Ed Queue, 目前正在解决 RFC Editor 的评审意见。

Attestation Results for Secure Interactions

<https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/>

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

背景:

本文稿是对远程证明结果的 (信息模型) 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做设备的另一个 “证书”。

文稿中定义了:

可信层级 (Trustworthiness Tiers), 包括 affirming、warning、contraindicated、none 4 个层次, 每个层次都给出了一个 standard 和 private 的取值范围, 针对不同的评估类别具体值的含义不同, 总共是 256 个取值空间 (8-bit 有符号整数)。

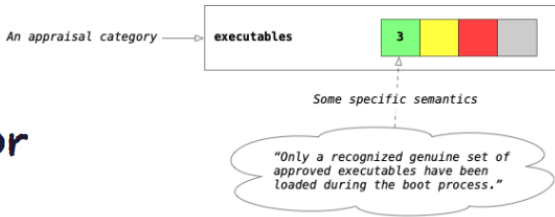
		std	private
<h1>Trustworthiness Tiers</h1> <p>→ y: 256 code-point space (8b signed int) organised in four tiers</p> <p>→ x: two sub-spaces (standard, private)</p>	affirming	2..31	-32..-2
	warning	32..95	-96..-33
	contraindicated	96..127	-128..-97
	none	-1..1	

可信声明 (Trustworthiness Claim), 文稿给出了从 Identity、Integrity、Confidentiality 三个维度定义了共 8 种类别 (configuration、executables、file-system、hardware、instance-identity、runtime-opaque、sourced-data、storage-opaque), 可信声明是对某个评估类别的评估结果, 例如 “executables” 的评估结果是

affirming 且值为 3。

Trustworthiness Claim

Each "trustworthiness claim" is associated to an appraisal category and, for that category, the claim defines its own semantics.



An appraisal category → executables

Some specific semantics

"Only a recognized genuine set of approved executables have been loaded during the boot process."

可信向量 (Trustworthiness Vector) ， 一组可信声明组成了一个可信向量，可信向量是远程证明结果 Attestation Result 中的主要部分之一。

Trustworthiness Vector

The "trustworthiness vector" is a collection of 8 pre-defined "trustworthiness claims".

A missing entry is equivalent to 0 (i.e., no claim in this category).

Worth noting: the vector allows exposing the *quality* of the verifier.

configuration	2				
executables	3				
file-system				0	
hardware	2				
instance-identity	2				
runtime-opaque		32			
sourced-data				0	
storage-opaque				0	

可信声明 (Trustworthiness Claim) 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](#)。

进展：

该文稿只定义了远程证明结果的核心部分的信息模型、并没有定义数据模型，而且 Relying Party 使用远程证明结果时还需要关注其他内容，例如 Verify 的身份、远程证明评估时间、评估策略 ID、Verify 执行环境的可信证明。

作者们基于 EAT 序列化方法实现了远程证明结果的封装，称为 EAR (EAT Attestation Result)，这部分后续会提交一个新文稿。

JSON / JWT Example

```
{
  "eat_profile": "tag:github.com/veraison/ar4si,2022-10-17",
  "ear.status": "contraindicated",
  "ear.trustworthiness-vector": {
    "instance-identity": 32,
    "configuration": 32,
    "executables": 96,
    "hardware": 2
  },
  "ear.appraisal-policy-id": "https://veraison.example/policy/1/60a0068d",
  "iat": 1666529184
}
```

远程证明结果

可信向量 Trustworthiness Vector

可信声明 Trustworthiness Claim

Slides: <https://datatracker.ietf.org/meeting/115/materials/slides-115-rats-an-eat-serialisation-of-ar4si-01>

Entity Attestation Token (EAT)

<https://datatracker.ietf.org/doc/draft-ietf-rats-eat/>

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

背景： 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。

进展： 文稿当前已经进入到 WGLC 阶段，但是还有一些遗留问题未解决，主席在上次 IETF 会后创建了一个遗留问题列表，本次会议主要介绍这些遗留问题的解决情况。目前仍有关于 Endorsements 定义等问题未解决。

Slides: <https://datatracker.ietf.org/meeting/115/materials/slides-115-rats-eat-status-update-and-issue-resolution-00>

EAT Media Types

<https://datatracker.ietf.org/doc/draft-ietf-rats-eat-media-type/>

作者: Laurence Lundblade (Security Theory LLC), Henk Birkholz (Fraunhofer SIT), Thomas Fossati (ARM)

背景: 在 RESTful API 中传递远程证明相关的 payloads 时需要有一个对应的 media type, 该文稿定义传递 EAT payloads 时需要的 media type。

进展: 该文稿于 2022 年 9 月被工作组接纳。本次主要介绍了对文稿的更新, 并且申请 early allocation。

Slides: <https://datatracker.ietf.org/meeting/115/materials/slides-115-rats-eat-media-types-01>

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。

进展: 本次会议同意对该文稿发起 WGLC, 已征求更多 Review。

Slides: <https://datatracker.ietf.org/meeting/115/materials/slides-115-rats-uccs-01>

RATS Conceptual Message Wrapper

<https://datatracker.ietf.org/doc/draft-ftbs-rats-msg-wrap/>

作者：Henk Birkolz (Fraunhofer SIT), Ned Smith (Intel), Thomas Fossati (ARM), Hannes Tschofenig (ARM)

背景：RATS 架构中定义了 Evidence、Attestation Result、Reference Value、Endorsement 等 Conceptual Message 类型，这些消息实际上可能会采用不同的编码与序列化格式、采用不同的传输方式。为了能增强互通性，本文稿提出了对 Conceptual Message 基于 media type 定义统一的封装格式，即采用[type, value]这样的格式，其中 type 可采用 CBOR content-format codepoint 或 media type，value 可采用 CBOR byte string 或者 JSON base64 string。

进展：由于时间原因未展开讨论，后续将在邮件列表征集意见。

Slides: <https://datatracker.ietf.org/meeting/115/materials/slides-115-rats-rats-message-wrappers-00>

An EAT-based Key Attestation Token

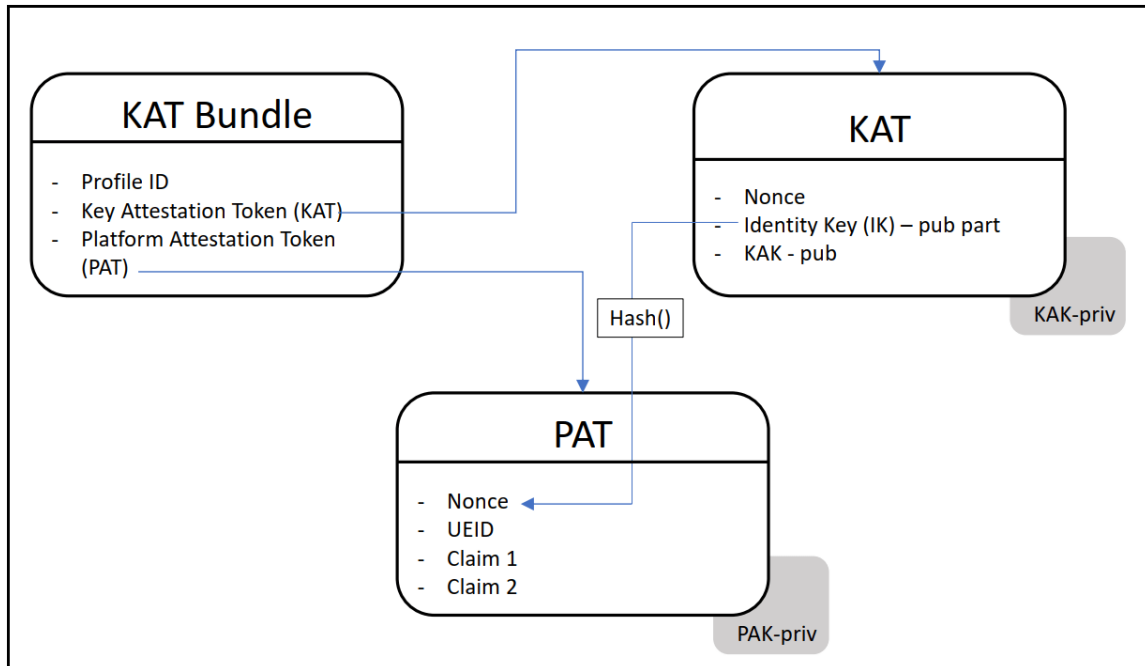
<https://datatracker.ietf.org/doc/draft-bft-rats-kat/>

作者：Mathias Brossard (ARM), Thomas Fossati (ARM), Hannes Tschofenig (ARM)

背景：

本文稿是 ARM 提出基于 EAT 定义 Key Attestation Token (简称 KAT)，用于设备证明其拥有密钥 (proof of possession)。KAT 采用的是将 TEE 等可信根平台的证明与密钥的证明信息绑定。其中，可信根平台的信息称为 Platform Attestation Token (简称 PAT)，这可以看做是对 TEE 等可信根自身的远程证明信息，供对端评估该可信根是否是可信状态。KAT 中记录了设备的身份密钥 (公钥部分)，以及可信根中的 AK 对该身份密钥公钥部分的签名。

KAT 可以取代传统 PKI 方式使用 CA 来证明设备对密钥的拥有。对端先验证 PAT 信息来评估可信根的可信状态，如果可信根是可信的则再验证 KAT 信息，并验证设备身份密钥是否是由可信根签名的。本文稿的设计也可以应用到在 TLS 中应用远程证明的文稿方案中 (draft-fossati-tls-attestation)。



Using the KAT in TLS

- In [draft-fossati-tls-attestation](#) we describe how to use the KAT bundle with the TLS handshake.

- Steps:

1. Generate IK key pair
2. Obtain Nonce from peer
3. Create KAT Bundle with IK and nonce
4. Transmit KAT Bundle to peer
5. Demonstrate possession of IK-priv

- [draft-fossati-tls-attestation](#) is agnostic to the attestation technology used thanks to [draft-ftbs-rats-msg-wrap](#).

进展：本文稿是新提出的文稿，由于时间原因未展开讨论。Henk Birkholz 提出很多术语与 TCG 中定义的相同（如 IK、AK 等），需要避免含义有分歧。

Slides: <https://datatracker.ietf.org/meeting/115/materials/slides-115-rats-attestation-in-tls-and-eap-based-key-attestation-00>

SPRING

MPLS Network Action (MNA) Header Encodings (10 mins)

Presenter: Rakesh Gandhi (rgandhi@cisco.com)

draft-jags-mpls-mna-hdr

文稿主要介绍对 MNA 的几种封装格式。

爱立信 Greg 询问是否能够同时封装两种 NA (HBH 和 I2E) - 是可以携带多个 substack 分别携带的。

SRv6 for Inter-Layer Network Programming (10 mins)

Presenter: Liuyan Han (hanliuyan@chinamobile.com)

draft-dong-spring-srv6-inter-layer-programming

IP 加光的路径场景，定义新的 End.XU。

chenran (ZTE) 表示有类似方案。

Sasha 认为 P3 无法转发报文，Ketan 认为现有 End.X 也可以被用来指示 L2 Bundle member。

Encapsulation of BFD for SRv6 Policy (10 mins)

Presenter: Yisong Liu (liuyisong@chinamobile.com)

draft-liu-bfd-srv6-policy-encap

Greg 和 Gyan 没理解为什么针对 BFD 的封装有什么特别之处，和现有 NP 有什么区别，带来的价值是什么？Joel 认同 Greg 的观点，希望邮件列表继续讨论。

Jeffrey, BFD 主席，指出当前 SPRING 有 5 篇 BFD 相关文稿，希望 WG 能够将这些文稿整合。Joel 同意。

Segment Routing based Solution for Hierarchical IETF Network Slices (10 mins)

Presenter: Liyan Gong (gongliyan@chinamobile.com)

draft-gong-teas-hierarchical-slice-solution

Ted (Cisco) 对文稿方案表示出兴趣, 询问三个问题: 是否是 informational, 是否有 IPR, 是否有具体的部署例子。中移目前有政企用户和子运营商两个场景可以使用。

Path MTU (PMTU) for Segment Routing Policy (10 mins)

Presenter: Gyan Mishra (gyan.s.mishra@verizon.com)

draft-peng-spring-pmtu-sr-policy

没有问题, 申请 adoption.

SRv6 and MPLS interworking (10 mins)

Presenter: Swadesh Agrawal (swaagraw@cisco.com)

draft-agrawal-spring-srv6-mpls-interworking

Dhruv 建议考虑跨域多 PCE 场景。Jeff 希望看到 operational details。Jorge 询问与 BESS 文稿的关系。

SR Policy Group (10 mins)

Presenter: Liyan Gong (gongliyan@chinamobile.com)

draft-cheng-spring-sr-policy-group

Ketan 主要质疑区别于现有机制的地方, 以及带来的好处。Weiqiang 解释主要是便于分层管理。

Network Resource Programming with SRv6 (10 mins)

Presenter: Weiqiang Cheng (chengweiqiang@chinamobile.com), Wenying Jiang (jiangwenying@chinamobile.com)

draft-cheng-spring-srv6-resource-programming

Gyan 询问如果将 NRP 映射进 QoS。类似于 HQoS。

Segment Encoding and Procedures For Multicast VPN Service in Native IPv6 Network (10 mins)

Presenter: Wei Wang (wangw36@chinatelecom.cn), Aijun Wang (wangaj3@chinatelecom.cn)

draft-wang-spring-multicast-vpn-segment

Bruno 倾向于这个文稿应该在 BESS 讲。

Aijun 认为，MVPN 组播场景下，RD 对于所有的 egress node 都是相同的，单播可以是不同的。本文稿只是定义格式，和在 native IP 网络下的流程。

MADINAS

工作组简介

Madinas 在 2020 年组织 BOF，并在 21 年 9 月通过 charter。文稿数量较少，目前只有两篇工作组，一篇个人。原来二层 MAC 是静态分配的，这样会引起隐私问题，SDO 制定了随机和更改 mac 地址 (**Randomized and Changing MAC addresses, RCM**) 的方法。而目前很多上层应用还是认为 mac 地址是绑定好，一成不变的。

madinas 工作组的目标是

- 识别受 RCM 影响的**应用及具体影响**
- 分析现有的除 mac 地址外的服务标识符 (**是否可替代**)
- 识别不需要标识符的**场景**

工作组主要产出是 **BCP (Best Current Practices)**，是个短期工作组 (12-18 个月)。

会议信息

会议时间: 2022.11.10 17:00-18:00 UTC

Chairs: Carlos J. Bernardos (University Carlos III of Madrid 副教授，也是 INTDIR 主席)，Juan-Carlos Zúñiga (Cisco)

Area Director: Éric Vyncke(Cisco)

Scribe: Mathieu Cunche (国立里昂应用科学学院副教授，还没有在 IETF 提交过文稿，目前为该组秘书) 负责笔记。

参会情况: 43 名签到，Cisco 参与人数最多。

会议纪要

Carlos 介绍了会议日程。

Randomized and Changing MAC Address Use Cases

[draft-ietf-madinas-use-cases-03](#)

作者是 **Jerome Henry** , Yiu Lee, 分别来自 Cisco 和 Comcast, 文稿主要介绍了 RCM 对服务的**影响**、探索在 RCM 时是否有其他方法重新恢复用户身份, 以及用户隐私问题。

由 Jerome 做 03 稿的宣讲, 介绍文稿的目的 (主要是定义术语) 和更新情况 (typo 修订, 增加解决方案), 以及文稿更新建议 (删减、移动内容)。

Carlos Bernados 围绕着 requirements 部分提供了两种解决方法, 建议清晰列出 use case; 其他人包括 Eric(AD)也讨论了新起一个 BCP 文件用于安置 existing solutions (已有的可以满足部分 requirements 的方法), 而 use case 和 requirements 在单独的文件中。

MAC address randomization

[draft-ietf-madinas-mac-address-randomization-04](#)

作者 Juan-Carlos Zúñiga , **Carlos J. Bernardos** , Amelia Andersdotter 分别来自 Cisco, UC3M (University Carlos III of Madrid) 和 Sky UK。文稿介绍了来自 IEEE 802, IETF, WBA (Wireless Broadband Alliance) 的一些关于 mac 地址随机化的**实践**, 并对相关策略进行**分类总结**。由 **Carlos** 进行 04 稿宣讲, 主要是增加了第 8 章关于 mac 地址选择策略的分类方法的内容 (目前分为五类) 以及合并 github 上的 pull requests。讨论主要建议把所有的 mac 策略都记录下来, 以供进一步分析讨论, 而不仅限于当前的五类, 其他策略比如 per-session 的策略。

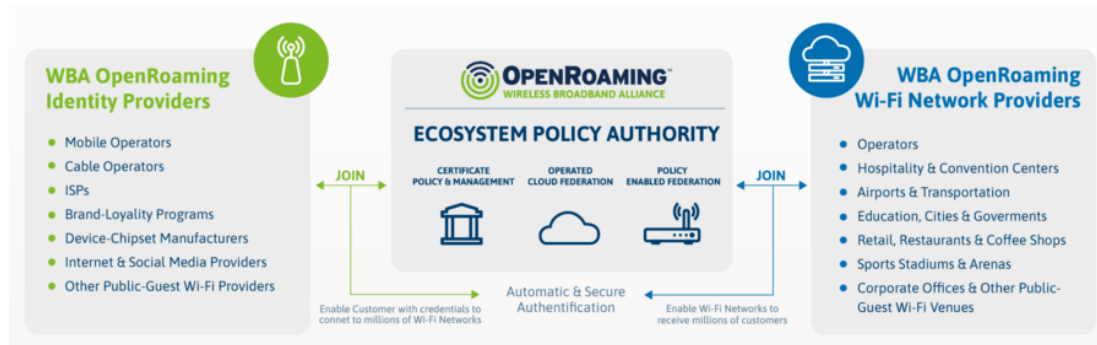
BCP handling RCM document: discussion and next steps

这是个开放讨论。主席 Juan-Carlos 先强调 WG **还需要一个 BCP 文档**, 以及欢迎来自 WBA, IEEE 802 的解决方案。BCP 文档是 WG 其他两个目标文档的后续任务。

Michael Richardson(Sandelman Software Works, 网络安全咨询)关注安全问题, 提出应该停止那些对个人隐私有负面效果的解决方案, 并对那些不适用的 solutions 进行解释。MR 本人申请参与 BCP 的工作。Michael Ackermann(Blue Cross Blue Shield of

Michigan, 提供健康保险的公司)询问关于随机化地址的具体实现, Juan 表示 802 有推荐, 但具体取决于厂商。Carlos 补充说草案中已提供了随机化的方法。

Open Roaming experiment with WBA



针对 WBA(Wireless Broadband Alliance)的 **OpenRoaming** 实验 (用户可以随时随地接入身边的网络, 任何 WIFI 都可以提供一致的身份认证服务, 保障用户隐私, 像在家用 WiFi 一样安全、快捷、简单), 主席提出一些需要解决的问题 (身份标识提供者、用户隐私、不同设备配置、网络搭设需求), 计划在下次 IETF 会中或会前进行场景测试。

Next Steps

主席希望推进包含 BCP 在内的文稿更新, 取得成功的话, 在一年后关闭工作组。

SNAC

工作组介绍

snac 属于新成立的工作组 (2022 年 9 月通过 charter)。Stub Network 是无需任何修改就可以接入到当前基础设施网络中的叶子网络, stub 网最主要的特征是不可以作为其他网络之间的互联。Use case1: 二层接入 (不涉及路由), 如, 基于 IEEE 802.15.4 的娱乐或灯光系统。这种场景的重要需求是提供到已有基础设施网络的透明连接和多 stub network 同时接入。Use case2: 三层接入, 需要路由。目标是: 只考虑 ipv6, 支持接入和被接入网络之间的服务发现(dnssd)和路径可达, 以及对外部 internet 的无差别连接。新工作组目前只涉及两篇个人文稿。目标暂只考虑 adjacent 接入。

会议信息

会议时间: 2022.11.10 09:30-11:30 UTC

Chairs: Kiran Makhijani (Futurewei) , Marc Blanchet (Viagenie, 咨询公司)

Area Director: Éric Vyncke(Cisco)

Scribe: Michael Richardson (Sandelman Software Works, 网络安全咨询公司) 负责会议笔记。

参与情况: 51 名签到, 包括 Cisco, Orange, Google, Apple 等。运营商包括 British Telecom, Orange 等。

会议纪要

Administrivia/Chairs Intro (Agenda Bashing) - 09:30

主席 Kiran 介绍了会议 agenda, 由于是第一次工作组会议, 还简要介绍了工作组内容和目标。

Automatically Connecting Stub Networks to Unmanaged Infrastructure

draft-lemon-stub-networks-07

第一篇文稿宣讲来自 Apple 的 Ted Lemon (有且只有一名作者, 此人在 dns, dhcp 周边会议相当活跃)。文稿主要介绍一些将 stub network 连接到 adjacent infrastructure networks (如, 家庭网络) 的实现, 实现服务发现和可达 (主要解决 addressability 和 reachability 的问题)。这是一篇 BCP 文档, 不涉及新的协议, 主要使用 RFC 4861 (IPv6 Neighbor Discovery) 和 DNS-SD 实现, 考虑了一些特殊场景。

Ted 进行 07 稿宣讲, 主要还是讨论文稿覆盖的场景范围, 删掉 infrastructure support 的内容 (即无需来自基础设施的支持); 介绍了目前文稿包含的内容模块, 以及重点关注的内容 (1) 是否考虑 ipv4, Ted 认为 ipv4 需要被支持的, 列出一系列原因 (如, ipv6 可用性, 不能假定有 nat64。(2) 是否纳入 prefix delegation 的内容。最后 Ted 还谈及需要补充完成的内容 (nat64 状态机、与 dnssd 文稿的关系、partitioning 和 reachability 的细节)。

Michael Richardson、Eric、Tim Winters (QA Café)、Bob Hinden (Check Point Software)、Lorenzo (Google)、Stuart Cheshire (Apple) 都参与了是否需要 DHCPv6-PD 的讨论, 并就此发起了投票 (26 赞成 0 反对), 最后比较一致结论是需要纳入 PD (Prefix Delegation, 相对于单地址的分配, 前缀分配更适用于层次化的地址管

理) ; Juliusz (University of Paris-Cité) 提出是否可以在 stub router 上实现 SOCKSv5 proxy, Ted 觉得太复杂了; Esko (IoT consultancy) 觉得可以在 WG 增加 problem statement 文档, Ted 和 Marc 回应之前做过尝试, 目前缩减过的内容已包含在解决方案文档里了。

IPv6 Neighbor Discovery Prefix Registration

draft-thubert-6lo-prefix-registration-01

作者是来自 Cisco 的 Pascal Thubert, 并由本人宣讲 01 稿。文稿主要基于 RFC 8505 (基于低功耗无线个人区域网络 (6LoWPAN) 邻居发现的 IPv6 注册扩展), 目的是让节点可以将拥有的 prefix 注册到邻居路由器上, 并让其广播到更大的路由域中。作者介绍了历史 RFC 和当前 draft 的关系、两个主要的 use case。另一篇 draft-ietf-6lo-multicast-registration 则是扩展 RFC8505 的 multicast 和 anycast, 但没有在本次 snac 宣讲。

Ted 评论直接用 DHCPv6-PD 协议就可以, 一些工作应该在其他工作组 (如 6lo WG) 。Lorenzo 讨论了 6lo 场景下的通信问题, Michael 发表关于实用性、部署相关的评论。

Discussion on Next Steps

讨论 Ted 的文稿 (见 3.3) 的下一步工作。AD (Eric) 希望在 adoption 之前, 增加一行说明 DHCPv6-PD 应该被支持; Lorenzo 认为大家已经强烈赞同了, 不需要这样, 但也不希望 PD 成为另一篇文稿。Bob 提示 adoption 只是说明工作组同意该工作, 并非同意文稿的具体内容。Ted 当场更新了个文稿, 增加了 PD 的内容 (当 DHCPv6-PD 可用时, 不另外生成本地唯一 IPv6 单播地址, 直接用 DHCPv6-PD 获取 prefix) 。主席发起 poll (26 赞成 0 反对) 。而后大家做了一些 out-of-scope 的讨论, 主席决定结束讨论。

DHC

工作组介绍

产出 DHCP 协议 (IP 地址自动分配、配置、管理) 的历史悠久的工作组, 包括 DHCPv4 和 DHCPv6, 目前主要任务是 DHCP 协议扩展而不是定义 DHCP options (超出 DHCP 的机制和语义的修改除外, options 定义应在各个工作组内完成), 计划 2023 年关闭或 recharter。

具体目标包括:

- 提供 DHCPv6 相关的操作和运维建议的 informational 文档，以及标准化运维、管理 DHCPv6 client, server, agent 的文档
- 协助其他工作组定义 options
- 更新 DHCPv6 的基本规范，推动从 Proposed Standard 成为 Internet Standard

会议信息

会议时间: 2022.11.8 16:30-17:30 UTC

Chairs: Bernie Volz (从 Cisco 退休, 没有参加本次会), Timothy Winters (QA Café 软件公司)

Area Director: Éric Vyncke(Cisco)

31 名签到, 主要包括 Google, Apple, Cisco 等, 国内中移动 (程伟强)、H3C 等参加。

会议纪要

主席介绍了工作组状态, 目前没有 active 工作组文档, 有三篇个人文档要讨论, 强调了 23 年 1 月将 3315bis RFC(RFC 8415)推进为 Internet Standard(IS), 介绍了成为 IS 的要求, 以及未来在 23 年 3 月 recharter 或关闭工作组。

DHCPv6 - RFC 8415 to Internet Standard

draft-dhcwg-dhc-rfc8415bis-00

目前还是个人草案, 只是工作组也在推动。作者 Tomek Mrugalski, Bernie Volz, Michael Richardson, Sheng Jiang, Timothy Winters 分别来自 Internet Systems Consortium, Sandelman Software Works, BUPT, QA Café。在 RFC8415 基础上, 合并了 errata, 不建议 IA_TA 和 Server Unicast option 的使用。

由主席宣讲, 目前状态是已发起 WG Adoption Call, 呼吁站队讨论。实现是比较独立的, 在家庭网关、路由器、电缆调制解调器都有实现; 处理来自 IANA 的反馈; 自#114 会以来做了些更新。仍存在一些问题, 比如是否删除单播传输部分的内容, 放弃 UseMulticast 状态码, 减少 background 部分的内容。

计划在 23 年 2 月发起 WGLC, 以便赶上#116。

Distribute SRv6 Locator by DHCP

draft-cheng-dhc-distribute-srv6-locator-by-dhcp-03

作者 Weiqiang Cheng, Ruibo Han, Changwang Lin, Yuanxiang Qiu, 分别来自中国移动和新华三。文稿在 IGP 不可用时 (CPE 和 BRAS 之间) 利用 DHCPv6 向 CPE 分配/分发 SRv6 locator。

Weiqiang 宣讲 03 文稿, 更新: 在 DHCP 定义了 IA_SRV6_LOCATOR option 来描述 locator 长度、函数长度、参数长度, 介绍了两种场景:

- BRAS 直接分配给 CPE;
- BRAS 作为 DHCP server 的中继。

下一步寻求来自 dhc 和 spring WG 的反馈。

Tim 反馈需要增加介绍 client 接受到多个 locator 需要如何处理的情况 (weiqiang 同意)。Eric 反馈需要先在 spring 引起兴趣, 再在 dhc 进行 (weiqiang 反馈 spring 可能没兴趣)。

Registering Self-generated IPv6 Addresses using DHCPv6

draft-wkumari-dhc-addr-notification-04

作者 Warren "Ace" Kumari, Suresh Krishnan, Sheng Jiang, Rajiv Asati, Lorenzo Colitti, Jen Linkova 来自 Google, Cisco 等。主要目的是, 将自生成的或静态配置的 IPv6 地址告知 DHCPv6 服务器。

由 Jen 进行 04 稿宣讲, 之前在 #114 会议宣讲过具体内容。本次更新主要针对, 增加发送和接受注册信息时的一些限制条件、重传方法、注册刷新、特殊情况, 以及提出采用 DHCPv6 标准 backoff (重传策略) 的建议。下一步主要考虑是否将 registration 改为 inform、讨论重传策略, 以及是否发起 adoption call。

会后讨论围绕每 4 小时刷新注册机制、组播的使用、acknowledgement 使用、release 释放消息发送等技术点展开。

DNSSD

工作组介绍

DNS-SD 配合着 mDNS，可以用来在本地链路上发现和解析服务和域名。DNS-SD/mDNS 一般只支持共享单链路上的 DNS 自动发现，很难在广域多链路中应用，因此需要新的技术/协议支持。dnssd 可以扩展或者开发新的协议，但必须支持后向兼容（对 DNS-SD 等的支持）。

工作组主要目标是对下列五种情况，在多链路路由网络，做可扩展、自动化、可远程的基于 DNS 的服务发现：

- 个人网络（笔记本和打印机）
- 家庭网络
- 无线热点
- 大型企业网络
- 网状网络，如 RPL (IPv6 Routing Protocol for Low power and lossy networks (RPL)) 或者 6LOWPAN (IPv6 over Low-Power Wireless Personal Area Networks)

工作组需要和 homenet 工作组协调工作，把 homenet 的反馈做为 adoption 的参考。

会议信息

会议时间：2022.11.8 15:00-16:00 UTC

Chairs: Chris Box (Orange, 搞过 4G/5G), David Schinazi (Google, 做过 QUIC, 之前在 Apple)

Area Director: Éric Vyncke(Cisco)

参与情况：60 多名签到，主要包括 Google, Apple 等，运营商鲜有参加。

会议纪要

主席介绍了三篇工作组文稿的状态，其中两篇 draft-ietf-dnssd-srp-17 和 draft-ietf-dnssd-update-lease-03 完成了 WGLC，正在做修改，之后提交 IESG；draft-ietf-dnssd-advertising-proxy-01 还需要更多的讨论和推进。

agenda 列有三个主题讨论（实际讨论一个）和两篇个人文稿的宣讲，实际上是 Ted 一个人的“主场外交”。

Interaction between a DNS server and Discovery Proxy co-hosted on same device

这是一个主题讨论，由 Esko(IoTconsultancy.nl)在邮件列表里发起，考虑一种特殊情况下（在同一个设备上），DNS 服务器和发现代理之间应该如何交互，由 Ted Lemon(Apple)在邮件中和会议上做了回应。在会议上，Esko 提出在 SRP 文稿中的 DNS zone 没有明确的命名，是否应默认使用 “home.arpa”等域名。

Advertising Proxy for DNS-SD Service Registration Protocol

draft-ietf-dnssd-advertising-proxy-01

作者是 Stuart Cheshire , Ted Lemon, 来自 Apple。

DNS-SD 一般配合着 mDNS 来使用，但是 mDNS 对于 stub network 或低功耗 host 不适用/实用。01 文稿由 Ted 宣讲，引入新的 proxy 类型：advertising proxy 使用 multicast DNS (mDNS)在多个网络链路上宣告 DNS zone 的内容，这允许旧的客户端通过代理使用组播 DNS 发现使用 SRP 注册的服务。Use case 主要是 stub network 和用 DNS 取代 mDNS。

根据 Esko Dijk 提问，Ted 做了一些所用单词/术语(link)的含义解释，对部署性、使用场景的澄清，讨论新旧设备兼容问题，.arpa 的使用风险。不少人讨论了 IANA 的责任以及域名(.home, .local)分配相关的问题。Ted 最后说可能可以通过对 link 的不同命名来解决部分问题，但做到这点比较难，也没有组织可以负责命名。

Reliable SRP without an operator

由于时间关系，Ted 在会上非常简要介绍了两个文稿的情况。

Automatic Replication of DNS-SD Service Registration Protocol Zones 提高了 SRP 的可靠性（如，单一的 DNS authoritative server 失效时，可以使用 replication service），在 Google 和 Apple 都有部署，并引发了很多的邮件讨论。希望得到更多的讨论，并完成工作组接收。

Multicast DNS conflict resolution using the Time Since Received (TSR)

RR(Resource Record) 解决在使用 mDNS 情况下当 SRP 注册信息变更发生时，新旧数据

存在冲突时的解决办法，可以避免新数据被抛弃。在 Apple 已有实践，文档比较成熟，没有遗留问题，希望得到更多的 review 并完成工作组接收。

RIFT

工作组 charter 介绍

18 年成立的工作组，目前主要有 RIFT 协议 spec, YANG, Applicability Statement 三个重要、较成熟的文稿。在数据中心的 Clos 和 Fat-Tree 拓扑下，结合 link state(如, ISIS, OSPF)和 distance vector(如, RIP, 收敛慢)两种，取长补短，设计特别的动态路由，实现以下：

- 基于链路检测实现 Fat-tree 拓扑自动建立
- 最小化每个拓扑层的链路状态
- 减少拓扑分布交换
- 防止黑洞和次优路由
- 流量引导和重路由
- 提供同步协议收敛后可使用的有限键值数据存储的机制

会议信息

会议时间: 2022.11.8 15:00-16:00 UTC

Chairs: Jeff Tantsura(Microsoft), Zhaohui (Jeffrey) Zhang(Juniper)

Area Director: Alvaro Retana (Futurewei)

与会情况: 24 人签到，来自 Juniper, Google, ZTE, Huawei 等。

会议简要总结

由主席介绍工作组现状，主要是 active 的 (Auto EVPN, Auto Flood Reflection) 和新的文稿(draft-zwx-rift-leaf-ring)以及 RIFT SR 和 Multicast，本次会议日程包括四篇 update 和一篇新宣讲。

RIFT: Routing in Fat Trees

[draft-ietf-rift-rift-16](#)

作者 Tony Przygienda , Alankar Sharma , Pascal Thubert , Bruno Rijsman , Dmitry Afanasiev , **Jordan Head** , 来自 Juniper, Comcast, Cisco 及 individual。草案为 Clos 和 fat tree 网络设计动态路由协议, 可以减少控制平面状态、配置和运维复杂度, 全文有 100 余页内容。

由来自 Juniper 的 Jordan 宣讲。16 版做了一些更新, 增加了一些澄清解释部分, 解决 SVG 排版、编辑问题, IANA 问题等。目前正在过 AD Evaluation。没有提问或评论。

RIFT Key/Value Structure and Registry

draft-ietf-rift-kv-registry-04

作者 **Jordan Head** , Tony Przygienda, 来自 Juniper。key-value pair (如, overlay 协议状态) 可以使用 RIFT 定义的 Key-Value Topology Information Elements (KV-TIEs) 来传播。文稿主要定义了几个 Key Structure。

仍然由 Juniper 的 Jordan 宣讲, 介绍了 04 稿的进展, 目前状态是 Shepherd review 等待 write up, 有参考文献、IANA 相关等一些问题。没有提问或评论。

RIFT Auto-Flood Reflection

draft-head-rift-auto-fr-02

作者 **Jordan Head** , Tony Przygienda , Colby Barth, 均来自 Juniper。RIFT-FR 结合 IS-IS Flood Reflection 技术, 利用协议自带的 Zero Touch Provisioning (ZTP) 功能实现自动化配置 Flood Reflection 拓扑。

仍然由 Juniper 的 Jordan 宣讲, 介绍了 02 稿的进展。增加了 Auto-FR spine 节点角色, 更新了 Auto-FR key-value TIE 内容和模型, 更新了 SVG 在 HTML 的适配性。目前状态是等待重新讨论, 然后通过 adoption, 有一些技术性的分析需要增加, 还有 multiplane 需要考虑。

Jeffrey 问了所属工作组的问题, 是否属于 LSR, Tony P. (Juniper)回答并不需要 LSR specs。Jeffrey 还问了对 ISIS 的适用性 (是)。

RIFT Auto-EVPN

draft-ietf-rift-auto-evpn-03

作者为 **Jordan Head** , Tony Przygienda , Wen Lin, 均来自 Juniper。使用 RIFT 的 ZTP 自动配置 EVPN overlay。

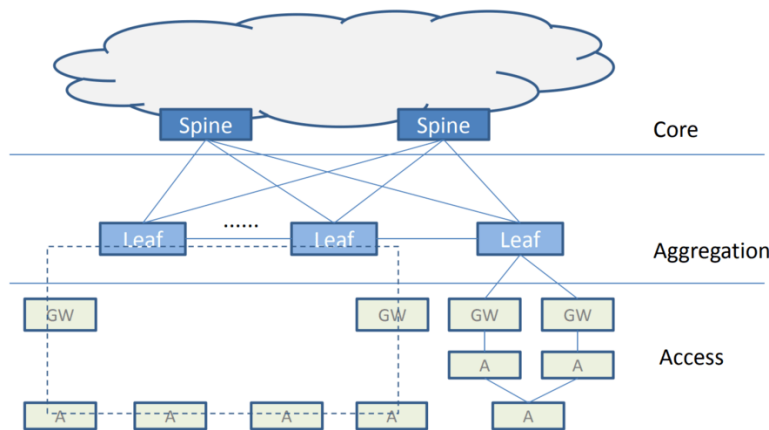
Jordan 做了无胶片更新简述, 目前的 draft 没有实质性更新, 下一个版本会有关于 multi-plane 和 DCI 网关, SVG 问题, operational 部分的整理等。

Supporting leaves without northbound neighbors connecting to a fat-tree network using RIFT

draft-zwx-rift-leaf-ring-01

作者是 **Zheng Zhang** , Yuehua Wei , BenChong Xu, 均来自 ZTE 中兴。

文稿补充考虑了 RIFT 草案里的特殊场景: 叶子节点没有北向链接时 (这些节点通过 ring, chain 等方式相连, 如下图)。Zheng(Sandy) Zhang 介绍了文稿内容, 属于再次宣讲。针对这些场景, 定义了 leaf-transport 能力通告, 并规定了 prefix south TIE 和 prefix north TIE 在无北向叶子节点之间的传递。



Tony P. (Juniper) 认为场景是 corner case (中兴反馈有相应场景), 质疑草案是多余的、过于复杂, 现有方法 RIFT 可以解决, 没有理由和价值。讨论持续了较长时间。

QUIC

本次 QUIC 工作组会议主要讨论了 MPQUIC、QUIC ACK frequency、qlog 等工作组文稿的技术问题, 以及 QUIC reliable stream reset, QUIC FEC 两篇个人文稿。其中 QUIC ACK frequency 和 qlog 都趋于成熟, 即将 WGLC, 而两篇个人文稿都是第一次上会讨论, 比较早期, 有所争论。

工作组相关的进度更新

QUIC Applicability 成为 RFC 9308, QUIC Managability 成为 RFC 9312, QUIC grease bit 成为 RFC 9287, QUIC version negotiation 以及 QUIC v2 已经提交给 IESG, 即将发布 RFC。

QUIC Retry Offload 是从另一篇工作组文稿 QUIC LB 分出来的, 用于将 QUIC retry 数据包的生成 offload 到硬件上, 可以减少 server CPU 的开销。QUIC 的 retry packet 用于应对 DoS 攻击, server 在接收到 QUIC 握手报文之后可以生成 retry 包, retry 包中携带 token, 要求 client 重新握手, 在新的握手包中带上该 token 以证明收到了该 token, server 收到后续握手后校验该 token 是否有效, 有效则建立连接。该机制利用 token 来防止伪造地址攻击和重放握手攻击, 该 token 的生成和校验需要一定的计算量, offload 到安全硬件上可以减轻 CPU 的开销。该文稿的作者与 QUIC LB 的作者相同, 包括微软和 Google。文稿今年 5 月被工作组接纳, 但是 implementation 太少, 所以暂时进入冻结状态, 除非有更多的人有兴趣实现这个功能。

Multipath QUIC by 阿里&爱立信

Single packet number space 还是 multiple packet number space
多路径 QUIC 是否在每条路径使用单独的 packet number space。使用单独的 packet number space 实现起来更加容易, 拥塞控制算法的代码无需改动, 直接把多条 path 视作多个 QUIC instance 即可, 每个 path 使用不同的 QUIC connection ID 区分, 但是缺点是无法支持 QUIC connection ID= NULL 的情况。多个 path 共用一个 packet number space 可以支持 NULL connection ID, 但是需要大量修改丢包探测, ACK 的代码。阿里实现了 single packet number space 的方案验证了其复杂性, 现在 draft 中的写法是默认推荐 multiple packet number space, 同时如果使用 single packet number space 则需要做额外的处理。作者认为 single packet number space 的相关文字使得 draft 变得复杂而繁琐。大家讨论认为可以放弃 MPQUIC 对 NULL connection ID 的支持。现场 Poll 没有人表明特别需要 NULL Connection ID 这个 feature。53-2 同时也讨论到是否直接使用多个 QUIC connection 来模拟 MPQUIC, 但是这样就没有办法把一个 stream 分散到多个 path 上, MoQ 会需要这个 feature (by MoQ chair Ted Hardie)

Keepalive 的设计

讨论在哪个 path 上发送 ping frame, 如果只在一条路上发送 ping frame, 但是这个 path 失效了, 是不是就要终止 MPQUIC 连接。是否需要暴露给应用选择 keep alive 的策略。path 重新建立之后是否需要保持之前的拥塞控制状态, 继续在邮件列表中讨论。

Path 序列号的设计

需要一个 Path ID 来指示在一条路径上的子 QUIC connection 因为子 QUIC connection 的 ID 可能会轮换, 同时这个 Path ID 用作加密的随机数。可以是 CID 的 sequence number 或者是初始的 CID。

ACK Frequency

该文稿设计了调整 QUIC ACK 频率的方案, 默认是每 2 个包一个 ACK, 该文稿设计控制帧调节该频率, 以及立即发送 ACK。

本次主要讨论帧格式的更新, 增加 reordering threshold 字段指示最多能容忍的乱序包的个数上限, 到达上限之后就必须发送 ACK。讨论认为这个字段应该使用 varint, 不必定长。varint 能容忍的大小是 $2^{62}-1$ 肯定是够用的。下个月 WGLC。

```
ACK_FREQUENCY Frame {
    Type (1) = 0xaf,
    Sequence Number (i),
    Ack-Eliciting Threshold (i),
    Request Max Ack Delay (i),
    Reserved (6),
    Ignore CE (1),
    Ignore Order (1)
}

IMMEDIATE_ACK Frame {
    Type (1) = 0xac
}
```

Sequence Number: Allows receivers to ignore obsolete frames after reordering.

Ack-Eliciting Threshold: The maximum number of ack-eliciting packets the recipient of this frame can receive before sending an acknowledgment.

Request Max Ack Delay: The value to which the endpoint requests the peer update its max_ack_delay

Reordering Threshold: An 8-bit field representing an unsigned integer that indicates how out of order packets can arrive before eliciting an immediate ACK. 0 indicates the peer should ignore reordering.

qlog

讨论 qlog 相关的工作组文稿，Main logging schema for qlog, QUIC event definitions for qlog。这些文稿定义了 QUIC 的日志系统，按照固定的格式打印 QUIC 协议栈运行的状态和 event 到 log。

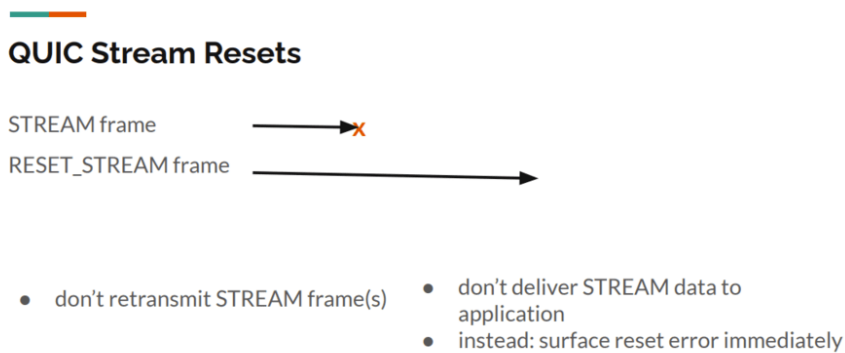
讨论 qlog 是否包含 QUIC datagram 拓展，作者回复说 qlog 目前不包含任何 QUIC 拓展，大家建议把 datagram 加上。也不想有那么多 RFC。

QUIC-LB: Generating Routable QUIC Connection IDs

部署不够多。以及在同一个 server 上将 QUIC 连接分配到不同的线程也是一种 load balancer 的 use case。Envoy 甚至在 BPF 中实现了 L4 的 load balancer

个人文稿 QUIC reliable stream reset

motivation 是目前 QUIC 的 stream 只在不被 reset 的前提下能保证可靠传输，一旦 reset 了，整个 stream 都不可靠了，但是对于 over QUIC 之上的协议来说，stream 里面可能有一些协议的 metadata 需要可靠传输。该文稿设计了新的 stream reset frame，增加了 reliable size 的选项，保证在指定 offset 之前的 stream data 可以可靠到达。



争论比较大，问题是存在的，但是是否要在 QUIC 层解决，这种解决方案动了 QUIC 的状态机，改动较大。主席认为需要和上层协议的工作组协调到底由谁来解决这个问题。

个人文稿 QUIC FEC

学术界做 MPTCP、MPQUIC 的人推的 QUIC FEC 实现，增加了新的 FEC frame 类型来为应用数据包进行冗余的抗丢包保护。

讨论了丢包 pattern, 是否需要保护控制帧以及 datagram 帧等问题。最后时间不够转到线下。

6MAN

Working Group Drafts

IPv6 Hop-by-Hop Options Processing Procedures,

draft-ietf-6man-hbh-processing , Gorry Fairhurst, Bob Hinden, 20 min.

Ron Bonica 建议和 EH Limits 文稿合并, 更新 RFC8200。但作者认为两篇文稿是关注同一问题的不同方面, 面向不同读者, 但可以互引, 也会考虑关于显式说明关于 8200 的更新。Suresh 认为现在的描述会让大家觉得第一个 option 很特殊有高优先级, 而都想用这个位置, 将会提供一些 text 说明 order 是没有限制的。提供了一些测试数据, IEPG talk。Some paths do support HBH Options. However, many currently drop packets with a HBH EH Limiting the size of the EH improved traversal.

申请 WGLC。

Limits on Sending and Processing IPv6 Extension Headers,

draft-ietf-6man-eh-limits , Tom Herbert, 10 min.

这篇文稿也会更新 RFC8504.

Segment Identifiers in SRv6

draft-ietf-6man-sids, Suresh Krishnan, 15 min

等待 SPRING 工作组的意见和建议。

Carrying Virtual Transport Network (VTN) Information in IPv6 Extension Header

draft-ietf-6man-enhanced-vpn-vtn-id, Zhenbin Li, 10 min

没有问题。

Individual Drafts

Carrying a Generic Identifier in IPv6 packets

draft-iurman-6man-generic-id, Justin Iurman, 10 min

设备硬件处理是否容易？不认为应该有 generic option type，但是可以为 option 如何设计提供一些指导。和已定义的 option type 之间的关系如何处理？

IPPM

PM on LAG

draft-ietf-ippm-stamp-on-lag / draft-ietf-ippm-otwamp-on-lag

Presenter: Tianran. Zhou

通过扩展携带 Sender/Reflector Micro-session id 信息的报文/TLV，使 STAMP/OWAMP/TWAMP 支持在单个 LAG 成员链路上建立微会话（Micro-Session），从而实现针对单个 LAG 成员链路的 PM 检测。

下一步：在文稿中增加关于 STAMP 无状态场景处理的描述。

Frank Brockners 提问，如果两个 lag 节点之间存在多段节点，如何使用文稿中的扩展运行 STAMP？答复无法运行，但有机制能识别这种场景，文稿中的扩展只适用于相邻的两个节点（Adjacent nodes），Frank 建议一开始的时候说明上述内容。

Greg Mirsky 补充，本文稿类似 BFD for lag，本文稿不适用于 MC lag。

SEC-DIR Response & Encrypted Mode Discussion: “Test Protocol for One-way IP Capacity Measurement”

draft-ietf-ippm-capacity-protocol

Presenter: A. Morton

文稿更新内容：

- 新增 4 种新的安全操作模式；
- 将现有的 Required 认证模式扩展到整个控制阶段（Control phase）的报文交互；
- 在数据阶段（Data phase）增加一种可选的状态认证模式；
- 新增密钥管理和防火墙配置章节；
- 新增检测建立、检测激活和状态反馈章节内容；

- 针对 IETF 114 提出的攻击场景，新增相关安全考虑内容；
- 新增 IANA 标准化请求；

下一步：

- 希望文稿在工作组内获得更多交流；
- 将完全加密模式加入到文稿中；
- 希望 2023.1 WG Last Call。

IPv6 Performance and Diagnostic Metrics Version 2 (PDMv2) Destination Option

draft-ietf-ippm-encrypted-pdmv2

Presenter: N. Elkins

实施：关键技术从内核补丁转变为 eBPF；在 Ubuntu 上测试 eBPF PDMv1；正在研究 eBPF PDMv2 实施；

IAB 研讨：如何管理加密网络是个难题，PDMv2 可能有所帮助。一旦 PDMv2 部署稳定，将尝试在互联网上多点部署；

IPv6 扩展头能否应用到互联网？v6ops 争论已久，大量研究证明 IPv6 扩展头方案无效。

当前工作：CDN 和云供应商测试；提交两篇 v6ops 文稿；side meeting；Hackdemo。

下一步工作：PDMv2 有 3 种交互方式：S-S/P-S/P-P，PDMv2 目前采用 S-S；P-S/P-P 的主要作用是在所有通信实体之间建立统一的上下文。准备发起 LC。

Responsiveness under Working Conditions

draft-ietf-ippm-responsiveness

Presenter: Christoph. Paasch

已解决 Issues: #62、#17

Issue #62: Working Conditions 算法的缺陷

算法应该在时延停止增长时终止运行，而不是在吞吐量停止增长时终止运行。

Issue #17: 使用知名 URI

WEB 服务器可以默认使用知名 URI

待解决 Issue: #55、#66

Issue #55: 确定结果的可靠性

如果在特定时间帧内没有达到稳定, Responsiveness 可能会过早地返回不可靠的结果。

Issue #66: 允许非 TLS 测量

低端设备没有足够的 CPU 用于加载链路的 TLS 流量。

Integrity of In-situ OAM Data Fields

draft-ietf-ippm-ioam-data-integrity

Presenter: J. Iurman

文稿无变化, VPP 实施正在进行。

A YANG Data Model for In-Situ OAM

draft-ietf-ippm-ioam-yang

Presenter: Tianran. Zhou

解答 WG LC 的评论问题 (Tom 和 Greg) , 根据评论问题少量修改文稿。

讨论:

- IOAM YANG 数据模型的范围仅限于配置, 还是说也能用于呈现 RFC 9197 中定义的 IOAM 数据类型? 建议仅限于配置。
- IOAM DEX 是否是 IOAM 不可或缺的组成部分? 建议遵循 RFC9197。
- IOAM YANG 数据模型是否能在 IOAM-DEX Trace 模式下启用 IOAM 节点配置? 否, 建议遵循 RFC9197。
- 仅控制中转节点上的 IOAM 操作状态 (启用/禁用) , 是否导致针对该节点的 DDoS 攻击向量? 如何减轻这种风险? 仅考虑 RFC9197 的场景。

- IOAM YANG 模型是否应该支持呈现设置了环回标记的环回 IOAM 数据包？否，建议遵循 RFC9197。
- IOAM YANG 模型是否应该使用 Active IOAM 标记，用于测试结果的配置和呈现？否，建议遵循 RFC9197。
- 文稿中是否能加入 IOAM over IPv6/NSH 的内容？Filter 仅用于标识目标流，以及进入 IOAM 处理流量。YANG 只提供了配置界面，不同设备可能实现不同。

Simple TWAMP (STAMP) Extensions for Segment Routing Networks

draft-ietf-ippm-stamp-srpm

Presenter: Rakesh. Gandhi

文稿更新内容：

- 针对 Rick Ringel (Spirent) 的评论，针对 STAMP TLV 中的 Verification (V) Check Flag，增加 Stateless Reflector 相关描述；
- 针对 Greg 的评论，增加关于 V Flag, Destination Address TLV, 和 Return Path TLV 的描述澄清；
- 更新 IANA 分配的标准值；
- 当前所有评论问题已关闭。

其他 WG 基于 STAMP 的文稿：

- draft-ietf-spring-stamp-srpm
- draft-gandhi-spring-stamp-enhanced-srpm
- draft-gandhi-mpls-stamp-pw

下一步：申请 WG LC。

Precision Availability Metrics for SLO Governed End-to-end Services

draft-mhmcsfh-ippm-pam

Presenter: Greg. Mirsky

文稿更新内容：解答评论问题。

- SLO 的总和是否就是 SLA？

- 关于 Ratio Metric 的实用性
- 组合服务 (composite service) 和 PAM 的对比关系
- Metrics: 单个报文如果违背 SLO, 后续是否会把单个报文违背 SLO 的场景也加到文稿中?

下一步工作 (非本文稿范围) :

- YANG 数据模型;
- IPFIX Informational Elements
- 支持统计 SLO
- 定义违反时间单元的策略, 配置度量值;
- 增加二级度量类型, 比如: 最长的服务中断时间。

NETMOD

周二 session1 NETMOD

本次会议约 60 人参加, 主要宣讲和参与讨论的公司, 包括 Cisco, Nokia, Ericsson, Vmware, YumaWorks 等

会议主题:

1) 工作组草案:

- YANG 模型版本;
- subinterface 及 interface extension YANG

2) 新的课题:

- 马秋芳牵头的 immutable flag 草案;
- ACL 模型, Telefonica 通用 ACL 扩展及策略随行 ACL 草案。
- Intent 接口的 YANG gap 分析

AD RW 上次提议对 IETF YANG 草案流程进行优化, 目前没有进展。上次会议后, 他在 OCYANG 参与每月的公开会议, 对 OCYANG, 例如 platform 等草案提意见。

会议资料参考:

<https://datatracker.ietf.org/meeting/115/materials/agenda-115-netmod>

Slides: <https://datatracker.ietf.org/meeting/115/session/netmod>

Drafts (PDF): <https://datatracker.ietf.org/meeting/115/agenda/netmod-drafts.pdf>

Recording: <http://www.meetecho.com/ietf115/recordings#NETMOD>

WG Chairs:

Lou Berger (lberger at labs dot net)

Kent Watsen (kent plus ietf at watsen dot net)

WG Secretary: Jason Sterne (nokia)

Session Intro & WG Status

Chairs (10 minutes)

对本次未宣讲的工作组草案的状态进行说明,

- 吴钦牵头的 node tag YANG,计划 WGLC
- 马秋芳牵头:draft-ietf-netmod-system-config, 会前成功接纳为工作组草案
- Cisco Joe Clark 牵头的 syslog YANG,目前还有一个 TCP 相关问题, 将 WGLC
- 两篇 interface YANG, 目前过期, RW 负责
- draft-ietf-netmod-rfc6991-bis-12 将更新以下内容:
 - a) ip-address-no-zone discussion: add "ip-address-with-zone" ,deprecate "ip-address"
 - b) [date/time]-[with/no]-zone: [date/time]-[with/no]-zone: rename (new "date" to "date-with-zone" and rename "time" to "time-with-zone"

工作组草案讨论:

Common Interface Extension YANG Data Models (10 min)

Presenters: Scott Mansfield (remote)

Draft: <https://datatracker.ietf.org/doc/html/draft-ietf-netmod-intf-ext-yang-10>

给出了更新计划, 会后提交草案更新,如果顺利, 下次会议 WGLC

YANG Versioning Update and Discussion (45 min)

Presenters: Jason Sterne & Joe Clarke

Draft: <https://datatracker.ietf.org/doc/html/draft-ietf-netmod-yang-module-versioning-07>

Draft: <https://datatracker.ietf.org/doc/html/draft-ietf-netmod-yang-semver-08>

*总结:*WGLC issue 及当前 R-07 更新, 没有接纳 Yugan 的 Per node NBC/BC 标记。

相比 RFC7950, 此次 rule 将 import change 修改为 BC, 并只支持 module 级的 NBC 标记。

Per node compatibility indicators: nbc-change-at, bc-change-at, editorial-change-at 建议为在 schema comparison 草案中定义。

Joe clark 宣讲了 YANG Semver, 询问工作组意见是否要限制哪些 branch 版本不允许。

但瑞电等不建议进行过多限制。

*下一步:*解决遗留的 issue, 主要是文字上的内容, 进行 WGLC.

个人草案:

YANG Extension and Metadata Annotation for Immutable Flag (15 minutes)

Presenter: Qiufang Ma

Draft: <https://datatracker.ietf.org/doc/html/draft-ma-netmod-immutable-flag-04>

目的:设备的一些 YANG 节点不支持控制器配置, 通过 flag 让控制器感知

讨论:Ericsson Balázs 支持, 说明 3GPP 有 100 篇 YANG 模型都有类似的标记。Cisco Jan, RW 和 Yuma andy 反对, Jan 认为会使得 NETCONF 和 SNMP 类似不能进行配置; Yuma 认为是厂商的 deviation 实现, 标准不需要这样的功能, RW 认为和 OCYANG variation 功能类似。Nokia Jason 问了澄清性问题。

*结论:*Chair 认为 1/3 参与投票, 有些人反对, 建议针对意见在文稿中详细说明使用方法。

A Policy-based Network Access Control (10 minutes)

Presenters: Qin Wu/Qiufang Ma

Draft: <https://datatracker.ietf.org/doc/html/draft-ma-opsawg-ucl-acl-00>

目的:定义企业园区策略随行的 user ACL

讨论: Cisco Joe 和 Arista Bill 讨论。Joe clark 认为 user group 不清楚, Arista Bill 建议 time period 参考 calendaring group 定义的 time based rules, e.g., <https://icalendar.org/iCalendar-RFC-5545/3-8-5-3-recurrence-rule.html>

结论: Lou 认为这个工作应该在 OPSAWG 继续

Extensions to the Access Control Lists (ACLs) YANG Model (10 minutes)

Presenter: Oscar Gonzalez de Dios

Draft: <https://datatracker.ietf.org/doc/html/draft-dbb-netmod-acl-03>

目的: 通用 ACL 扩展, 扩展基于 prefix set, protocol set 和 port set 定义 ACL; 扩展 action, rate-limit。当前 ACL 模型基于单个五元组定义, 不符合运营商网络的实现。

讨论: Vmware Mahesh,原 ACL 作者之一, 建议 sets 在 ACL container 中定义, 而不是 list entry 中定义; 大建议 rate-limit 在 Qos model 定义。Nokia Jason 建议 grouping 定义 set, 从而被其他模型重用。

*结论: *解决问题, 可以在会后或下次会议进行接纳。

Modelling Boundaries (10 minutes)

Presenter: Ciena Nigel Davis

Draft: <https://datatracker.ietf.org/doc/html/draft-davis-netmod-modelling-boundaries-00>

目的: 认为当前 YANG 模型无法支持 Intent 接口, 因为 user 可能会给出错误的输入, intent 接口可以提供一些参考值, 并与 user 互操作从而逐步获取正确的值。

*讨论: *本次是 00 稿, 内容过于抽象。Cisco RW 建议补充具体的例子说明问题; Benoit 支持, 认为有价值。

OPSAWG

11.9 周三上午 session I

约 80 人参加会议，主要参加单位包括思科，华为，Nokia, Ericsson, Ciena, NIST, Telefonica, Swisscom, Orange, Verizon, KDDI, TIM, Telenor, 乐天, Oracle 等

**Chair: **Huawei Tianran Zhou/ Cisco Joe Clarke / 德国安全研究机构 Henk

参考材料: <https://play.conf.meetecho.com/Playout/?session=IETF115-OPSAWG-20221109-0930>

工作组主要的进展如下:

发布 RFC 9291 L2NM L2VPN 网络模型

已进入 IESG 发布流程的文稿:

- draft-ietf-opsawg-sap : SAP YANG 业务接入点 YANG 模型——提供运营商 VPN, 或切片业务接入点, 是 VPN 业务自动发放的系列模型
- draft-ietf-opsawg-yang-vpn-service-pm- VPN 及网络性能监控模型, 用于聚合设备的 OAM, 统计数据呈现给跨域协同器或 OSS 应用
- draft-ietf-opsawg-sbom-access: lot 设备或应用程序的 sbom 软件物料清单信息获取模型, 用于软件合规安全监控
- draft-ietf-opsawg-service-assurance-architecture:
- draft-ietf-opsawg-service-assurance-yang:
- 业务保障架构及 YANG 模型, 通过业务模型依赖关系, 提供业务健康根因分析
- draft-ietf-opsawg-tlstm-update: SNMP over TLS1.2, TLS 1.3 更新

已通过 WG LC 的文稿:

- draft-ietf-opsawg-mud-tls MUD 设备 TLS ACL 扩展

新接纳的文稿

- draft-ietf-opsawg-add-encrypted-dns DHCP 配置加密 DNS 服务的 RADIUS 扩展, 用与 BRAS 设备支持加密 DNS 服务的 Radius 扩展。

本次会议现场讨论的情况如下

MUD Updates

Michael Richardson 10min

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

<https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud-acceptable-urls/>

目的和当前状态:

已经发布的 RFC 8520 Manufacturer Usage Description Specification 使用 DNS 来定义 MUD device 的 ACL 访问权限, 但在部署时由于越来越多的加密 DNS 部署会遇到问题。这两篇草案对 RFC8520 进行了补充, 包括 DNS 加密部署问题, 以及由于 firmware 固件升级导致的 URL 变更的解决方法。

这两篇草案都已经接纳了一年, 经过了较好的 review, 并且认为 DNS consideration 草案对 rfc8520 没有大的更改, 大多数 IoT 部署场景都是使用 local dns。

下一步:没有展开讨论, 下一步将 WGLC.

IPFIX Proposals IPFIX 数据流统计相关文稿

Swisscom Thomas Graf 20 min

<https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-ipfix-srv6-srh>

本次增加实现 opensource 的 VPP 实现以及 Huawei+Cisco 互通验证, 目前在 IANA 申请 codepoint, co-author Benoit 建议 WGLC

<https://datatracker.ietf.org/doc/html/draft-tgraf-opsawg-ipfix-inband-telemetry>

目的: 更新 ipfix 用于支持 ioam 单向时延, min, max, mean 和 sum 的 metric

申请 WG adoption.

下一步:Chair 将在会后发起 WG 接纳。

An Update to the tcpControlBits IP Flow Information Export (IPFIX) Information Element

Orange Mohamed Boucadair 5min

<https://datatracker.ietf.org/doc/draft-boucadair-opsawg-rfc7125-update/>

目的: RFC7125 Revision of the tcpControlBits IP Flow Information Export (IPFIX) Information Element 解决了一部分 bit 可见性, 本篇草案建议补充更多 TCP 的 bits 可见。

讨论: Benoit 和 RW 给出了意见, 支持 WG 接纳, 但认为可能需要对 TCP 进行全面的 IANA 注册 review, 会导致工作量大。

Asserting Wireless Network Connections Using DNS Revolvers' Identities

Nokia Tirumal Reddy 10min

<https://datatracker.ietf.org/doc/draft-wing-opsawg-authenticating-network/>

目的: 希望通过加密 dns 加密解决 Public wifi 场景下, 防止防冒 WIFI 攻击。认为 801.x 可以解决问题, 但并未大量部署。

讨论: Google AD Warren,认为草案描述的方案在 dns server 变更场景下 user 可能导致无 dns server 可选。

A Data Manifest for Contextualized Telemetry Data

爱尔兰 Benoit Claise 15min

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

目的:

为 Telemetry data 提供背景信息, 定义了两个模型:

- 平台清单 ietf-collected-data-platform-manifest: 描述了采集数据的平台信息。
- 数据收集清单 ietf-collected-data-manifest: 描述了 Telemetry 上报数据的订阅信息, 是否 on-change, 还是周期性上报, 以及上报的数据集, path 等信息。

讨论:

现场 Futurewei Alex, Cisco RW, Hank 以及 Telefonica Diego 认可分析器独立部署场景有实现的问题, 但这个模型和现有 YANG library, hardware, YANG package 以及 YANG push 工作重复。

下一步计划:

这篇为 manifest, 也是 inventory 的一种, 后续可以与 network inventory 一同讨论。

External Transaction ID for Configuration Tracing

爱尔兰团队 Jean Quilbeuf 15min

<https://datatracker.ietf.org/doc/draft-quilbeuf-opsawg-configuration-tracing/>

目的: 层次管理器进行 NETCONF/restconf 跨层 transaction 操作方案。

讨论: Cisco Jan 支持该工作, 认为应该和 NETMOD 组的 transaction 草案合作, Joe clarke 和 RW 也建议在 NETMOD 继续该工作。并对 client-id 的唯一性进行了讨论。

Data Model for Lifecycle Management and Operations

Cisco Marisol Palmero NTT Camilo Cardona 10min

<https://datatracker.ietf.org/doc/html/draft-palmero-opsawg-dmlmo>

目的: asset 管理的目的是确定 asset 的使用价值。

讨论:

约 6-7 人参加了讨论, Chair Henk 和 Michael 从 IOT 管理角度, 认为文稿中定义的 license 的用法应该修改为 entitlement。当前 MUD 文件的 license 是指开源 license 等。Alex 和爱尔兰 olga 认为草案不清楚, 不确定是 network level 还是 device level 草案, 建议定位为 network model。吴波确认 asset 的范围, 作者回复主要定位是软件 asset, 可以用于 IT asset, 此外, Marisol 在 side meeting 认为该 asset 可以包含 hardware asset。

下一步:

吴钦和 Diego 都建议在 side meeting 发起创建的 inventory list 进一步讨论。

注: 周二早 side meeting, 吴钦组织了 enterprise inventory 讨论, 约 20 人包括 Telefonica, Cisco Marisol 团队 3 人, 华为, Nokia, 以及爱尔兰团队 3 人等参加了讨论, AD RW 根据讨论创建了 inventory-yang@ietf.org 用于确定 CCAMP hardware inventory, OPSAWG asset, network inventory 的问题和范围。

An Inventory Management Model for Enterprise Networks

Bo Wu 10min

<https://datatracker.ietf.org/doc/draft-wzwb-opsawg-network-inventory-management/>

目的: 基于网络模型扩展的 Network 及 network endpoint inventory。从而解决跨域 inventory 感知, 从而支持业务随行 policy 下发。

下一步: AD RW 建议后续进一步和其他相关 inventory 草案讨论。

A Policy-based Network Access Control

Qiufang Ma 10min

<https://datatracker.ietf.org/doc/draft-ma-opsawg-ucl-acl/>

目的: 企业园区业务随行 policy 定义。

讨论:

Cisco RW, Joe clark 以及乐天 Rakuten 的 David 参与讨论。RW 建议是否可以将 time period 作为 condition。Arista Bill Fenner [in netmod]建议重用 ican 的 time rule; Rakuten david 建议增加 domain 的定义。

下一步:目前为 00,下次会议计划征求接纳。

PCAP and PCAPng and PCAP Link Types

Michael Richardson 5min

<https://datatracker.ietf.org/doc/draft-richardson-opsawg-pcaplinktype>

AD 支持工作组采纳, 并计划在 115 后同时接纳 3 篇文稿。

OPS area 宣讲:

Requirements DetNet in large scale networks

draft-liu-detnet-large-scale-requirements-05

<https://datatracker.ietf.org/doc/html/draft-liu-detnet-large-scale-requirements-05>

Detnet Torless 宣讲，希望 OPS area 的运营商提供意见，定义 detnet 在大规模网络以及高带宽 100G 以上网络部署的需求。当前 Detnet SLA 解决方案包括，Bandwidth 通过 per-flow path 建立解决，latency 通过 per hop QOS，Loss 通过重传。

NETCONF

NETCONF 本次安排在周一下午 Session III，时间是 3:30-5:30。参会人数 50 人左右。本次会议讨论的个人文稿均是 00 稿草案，分别由瑞电，思科，华为和诺基亚牵头。会议讨论的热点主要是配置追踪管理（draft-ietf-netconf-transaction-id-00, draft-quilbeuf-opsawg-configuration-tracing-00, draft-rogalia-netconf-trace-ctx-extension-00）和 private candidate 数据集（draft-jgc-netconf-privcand-00）。

Introduction

Chairs (10 minutes) Session Intro & WG Status

主席介绍 NETCONF 工作组的现状。目前 NETCONF 工作组草案的进展是，http-notif 在 AD review 阶段；client-server 系列草案均在 shepherd writeup 阶段，相关 shepherd review 的 comments 都已经解决；udp-notif 和 distributed-notif 持续推动；既上次 IETF 会议后，分页系列三篇草案接纳，变频采集草案接纳，netconf over tls1.3 接纳，transaction-id 草案接纳。本次 non-charted items 的讨论均是 00 稿草案。

Chartered items:

UDP-based Transport for Configured Subscriptions (15 min)

<https://datatracker.ietf.org/doc/html/draft-ietf-netconf-udp-notif-06>

Discussion Leader: Alex Huang Feng

INSA-Lyon 的 Alex 宣讲的 UDP 上送和分布式上送文稿。本次上会主要是讨论文稿刷新，以及目前的遗留问题。

讨论 1: YANG 模型前缀命令。Tom Petch 在邮件列表建议一系列的草案使用一个公共的定义方式。目前草案模型名称是 ietf-udp-notif, 前缀是 un。http-notif 前缀是 hnt, yang-push 模型前缀是 yp。AD Rob 认为当前 un 可行，或者采用 yp-un。

讨论 2: receiver 的地址类型，目前使用的是 ip-address, 是否需要更换成 ip-address-no-zone。IETF 曾经关于 IP 地址类型的错误使用有过讨论，但是并没有达成明确的一致结论。AD 认为为了避免造成歧义，建议 receiver 的 IP 地址类型使用 ip-address-no-zone.

讨论 3: http-notif 和 udp-notif 草案对于 receiver 的处理配置不同，但都是考虑基于不同的传输协议承载 notification。UDP-notif 直接扩展 8639 的 receiver, 新增 DTLS 等配置信息；HTTP-notif 则在一个新的模型中定义 receiver-instance, 再扩展 RFC8639 中的 receiver 引用 receiver-instance。UDP-notif 遵从 RFC8639 的建议定义，但与 HTTP-notif 不同，二者是否有必要采用同样的配置方式？

Kent 作为 HTTP-notif 草案的作者澄清，http-notif 基于 TCP 承载，需要建立 session 连接，这种配置方式可以使得多个 subscription 共用一个 session，UDP 没有类似的技术需求，但是出于一致性考虑可以使用跟 http-notif 同样的配置方式。

讨论 4: Joe Clark 建议在文稿中指出 DTLS 的配置可能会对性能产生一定影响。是否有必要指出？Kent 认为没有其他类似的涉及加密的文稿中提到过，所以这里也没有必要提及。但 Joe Clark 澄清说，这里需要提到性能问题是因为线卡在这里需要做 notification 的加密和数据发送，这跟以往的普通加密机制不同。Beniot 说 IPFIX 文稿也没有写性能问题。

这篇草案补充 DTLS 配置相关示例后，作者认为已经 ready for SECDIR review.

此外，INSA 在做 yang-push 相关的实现时发现 RFC5277 只定义了 xml schema, 没有定义 YANG 模型的 gap, 该问题曾在 NETCONF 邮件列表上讨论，并得到 Andy 的认可：

https://mailarchive.ietf.org/arch/msg/netconf/b8gaPsk8i_XaZ47pLd6kb8SvIJk/ ;

Alex 指出他们下一步会在 116 之前提交一篇一篇新文稿补齐 gap。针对此问题，瑞电 Thomas 询问是准备提交 5277 更新还是单独的文稿。

Subscription to Distributed Notifications (2 min)

<https://datatracker.ietf.org/doc/html/draft-ietf-netconf-distributed-notif-04>

Discussion Leader: Alex Huang Feng

分布式上送文稿没有更新，等待跟 udp-notif 草案一起 WGLC。爱立信的 Balazs 让 Alex 参考 Notification Message Headers and Bundles 文稿。

List Pagination (10 min)

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

<https://datatracker.ietf.org/doc/html/draft-ietf-netconf-list-pagination-nc-00>

<https://datatracker.ietf.org/doc/html/draft-ietf-netconf-list-pagination-rc-00>

Discussion Leader: Per Andersson

分页草案相对稳定，IETF114 之后没有刷新。主要的遗留问题在于，对于高度动态 list/leaf-list 分页检索时，是使用 cursor-based pagination 还是存储快照的方式。Cursor-based pagination 需要引入额外的 cursor 参数指明一个查询的 starting point；snapshot pagination 则是在数据查询之前首先存储一份快照数据，再分页检索快照。

对于该讨论，诺基亚的 Jason 认为需要区分考虑到底检索的是配置数据还是状态数据。Kent 回应主要考虑的是 operational 的状态数据，配置数据的变化可以使用 etag 或 timestamp 来追踪。

AD Rob 则询问关于 snapshot 的方式，是只存储 list 的 key 值，还是存储完整的 list。存储完整 list 保证的是所有的数据一致性，存储 list 的 key 值则仍然返回每个条目的最新值。Kent 回复应该是对所有的数据都打快照。但诺基亚的 Jason 认为快照适用于高度动态且数据量规模大的 list 查询，缓存所有数据会造成很大开销；但同时 client 端检索到的数据不断变化也会导致不一致问题。Kent 认为主要是 use cases 是查询 logs，所有的动态数据都是从 list 底部开始追加（这种情况下不需要 snapshot）。Andy 认为 YUMA 的场景下大部分动态查询的都是 counters，不仅仅是 logs 数据。Snapshot 可以解决，但 cursor 在这种情况下没有意义，因为不断有新的条目被添加和老的条目被删除。Juniper 的 Jeffrey Haas 认为造成这种查询混乱的原因是因为草案中定义了 limit 和 sort 查询参

数，client 只需要知道下一个要查询的 key 值是什么就能够还原出动态变化的 list。Kent 想用更细粒度的 snapshot 支持方式解决 snapshot 开销大以及某些 case 不需要 snapshot 的问题。

NETCONF over TLS 1.3 (10 min)

<https://datatracker.ietf.org/doc/html/draft-ietf-netconf-over-tls13-01>

Discussion Leader: Sean Turner

NETCONF over TLS1.3 草案与 transactionID 草案同时接纳，草案规定了 TLS1.3 承载 NETCONF 报文时禁止使用 0-RTT。另一部分是需支持 TLS1.3 相比 1.2 加密套件的更新。目前已经没有遗留问题，Sean 请求 WGLC。工作组投票全部支持，预计会后该草案会发起 WGLC。

Transaction ID Mechanism for NETCONF (10 min)

<https://datatracker.ietf.org/doc/html/draft-lindblad-netconf-transaction-id-02>

Discussion Leader: Jan Lindblad

思科主导的 transactionID 草案，本次上会主要是跟 NETCONF 工作组的一些现有工作进行对比，澄清几者之间的关系。

关于 transactionID 支持 client 端下发指定的场景，transactionID 草案之前有覆盖，但因为邮件列表中 Andy 的反对被删除，华为 Benoit 联合瑞电，Telefonica, 中国电信提出的 configuration-tracing，以及思科联合 DT 提出的 w3c-trace 都是解决此问题实现配置追踪。Kent 认为在 transactionID 草案中恢复这一功能比独立 solution 单独定义更为方便。但是也需要对比一下其他 solution 是不是更好解决了此问题。但爱立信 Balazs 不太建议此功能重新定义在 transactionID 草案中，认为可能会和其他草案产生冲突。Olga 也认为其他两个草案更好解决配置追踪问题，解决不同的 use cases。Jean 也赞成 transactionID 和 configuration-tracing 草案同时推动（Jean 是 configuration-tracing 草案的作者）。

Adaptive Subscription to YANG Notification (10 min)

<https://datatracker.ietf.org/doc/html/draft-ietf-netconf-adaptive-subscription-01>

Discussion Leader: Qiufang Ma

华为主导的变频采集草案，本次上会主要宣讲草案接纳后的更新情况。本次收到一条修改意见，Jean 建议将变频采集模型中的条件表达式 Xpath-external-eval 修改为 activated-xpath-eval。

Non-Chartered items:

Support of Versioning in YANG Notifications Subscription (10 min)

<https://datatracker.ietf.org/doc/html/draft-tgraf-netconf-yang-notifications-versioning-00>

Discussion Leader: Thomas Graf

瑞电联合华为，INSA-Lyon 推动的 notification-versioning 草案。主要是扩展 YANG-push 的定义，允许配置订阅和动态订阅在创建和修改订阅时能够支持指定模型的 revision 和 revision label，扩展 8641 中定义的 push-update 和 push-change-update 的 notification，增加 module，namespace，revision，revision-label，datastore-xpath-filter，datastore-subtree-filter 的信息。

诺基亚 Jason 认为需要在每个 notification 中都带上相对静态的模型信息会造成一定开销，尤其是当 notification streaming 的频率很高。如果想交换模型版本信息，可以使用 NETCONF 的其他机制解决。AD Rob 认为接收端需要的不应该只是 single module 的信息，应该是 a list of modules 或者是 yang package 的信息。并且认可 Jason 关于这种方式效率低的观点。爱立信 Balazs 询问这篇草案和 Benoit 在 OPSAWG 推动的 draft-claise-opsawg-collected-data-manifest 的关系。Thomas 解释二者有类似的想法，都是传递描述数据的元数据信息，但是一个用来传递被采集的数据本身的信息(subscription ID, datastore, period...), 另一个是传递 semantic reference(module revision-date,namespace...). Jean 补充这两篇文稿可以互补。

NETCONF Extension to support Trace Context propagation (10 min)

<https://datatracker.ietf.org/doc/html/draft-rogalia-netconf-trace-ctx-extension-00>

Discussion Leader: Jan Lindblad

思科联合德电提出的 00 稿草案，解决在网络级数据分析时数据追踪的问题。数据追踪可以用于故障定位和性能分析。使用 W3C 中定义的 traceContext 的概念，traceParent header 中包含了 trace-id 和 parent-id 的概念，trace-id 相当于一个端到端的事务概念，而 parent-id 则会携带直接对接的客户端的信息（如某个网元、某个控制器）。Trace parent 由客户端生成，可以在任意的 netconf RPC 请求中携带，服务器在返回信息时则需要将该 traceParent 属性带回。

对于该宣讲的讨论主要有，诺基亚的 Jason 询问该 traceID 的 tag 是怎么对 leaf 节点操作，服务器是否需要在数据库中存储该 ID？Jan 澄清该 traceID 不是绑定在具体的节点上，而是与 RPC 操作相关联，也不需要存储在数据集中。

瑞电的 Ahmed Elhassany 询问关于 ID 的生成方式是否会被标准化，还是与实现相关。

Olga 询问如何保证多 application 之间的 traceID 不会产生冲突？Jan 答复 W3C 规定了不同的 service 使用不同 tracestate 的值。

思科的 Charles 询问 W3C 制定的此标准是否有一些应用的示例？Jan 回复此标准刚制定 1 年，与此相关的 W3C baggage 还处于 draft 状态，但是已经有一些相关的工具。

External Transaction ID for Configuration Tracing (10 min)

<https://datatracker.ietf.org/html/draft-quilbeuf-opsawg-configuration-tracing-00>

Discussion Leader: Jean Quilbeuf

华为联合瑞电，Telefonica 和中国电信在 OPSAWG 组提出的 00 稿草案，解决在网络级数据分析时配置数据追踪的问题。可用于配置错误追踪，多网管并行修改配置，意图冲突等场景。草案在思科 transactionID 的基础上，引入 external transaction-id，NB transaction-id 是上层传递过来的，SB transaction-id 是由本层产生并发送给下层的。

在服务器侧提供一个模型可以查询哪些本地 commit 关联的 NB transaction-id 和 SB transaction-id，这样从端到端来说就是可以追踪数据源了。可以根据此 ID 跟踪配置更改，从而做到端到端的数据源追踪。

关于此草案的讨论主要是，爱立信的 Balazs 询问 client-id 是怎么来的，比如像 CLI 没有 client-id。Jean 认为如果实现了 transactionID 机制，就必须携带 clientID。但爱立信认

为 server 不应该强制 client 端提供 clientID。Kent 认为 RESTCONF 和 NETCONF 是对等的，如果扩展 NETCONF 支持此机制，RESTCONF 也应当被支持。Benoit 觉得不太确定这篇草案应该在 OPSAWG 还是 NETCONF 讨论（Benoit 也是这篇草案的作者）。Mahesh 觉得首先应该理清清楚 transactionID, W3C trace 以及这篇草案三者之间的依赖关系。

NETCONF Private Candidates (10 min)

<https://datatracker.ietf.org/doc/html/draft-jgc-netconf-privcand-00>

Discussion Leader: James Cumming

思科和诺基亚联合推动的 private candidate 草案。该文稿要解决的问题是多用户（客户端）并发的场景，使用共享的 candidate datastore 可能会出现客户端 2 无意中将客户端 1 的配置提交的问题。历史上 Ladislav Lhotka 曾提出过类似的想法(<https://www.ietf.org/archive/id/draft-lhotka-netconf-restconf-transactions-00.txt>)，Andy 在邮件列表也表达过对这篇草案的支持。这篇草案提出了 private candidate datastore 概念，并给出相应的处理机制。

- 提出了 private candidate 能力，通过能力交换获知对端支持 private candidate 的能力。
- 通过 RPC(e.g., edit-config)连带自动创建 private candidate datastore。
- private candidate 为 session 独占的，其他 session 不可见。
- 提出了 private candidate 同步的两种模式。（手动执行 update 更新同步和自动更新）
- 提出如何解决配置冲突的方法。

对于此宣讲的讨论主要是，思科的 Charles 询问能否允许多个 client 贡献同一个 private candidate 数据集，思科的 Robert Wills 答复当前考虑的 use case 是一个 session 使用一个 private candidate datastore.某些集合的 session 共享一个 candidate 会增加复杂性。AD Rob 认为对于 private candidate，很多厂商都有自己的私有实现，标准化要尽量做到灵活，允许像 with-default 机制让 server 广播不同的能力供 client 参考。Jeo Clark 觉得当多个 client 存在合并冲突的时候，应该可以允许 commit 失败或者自动解决，而不是要求手动解决冲突（中断自动化）。Andy 认为需要先理清清楚 requirements 再考虑 solution 细节，private candidate 应该是 per-user，不是 per-session，比如

RESTCONF solution 独立于 session。关于 private candidate 数据集的管理也需要注意，不能是自动生成。关于是否允许 private candidate 自动和 running 数据集同步的问题，Kent 建议草案作者参考华为在 NETMOD 推动的 with-system 草案中关于系统自动更新 running 数据集的原则。来自 Ciena 的 Walid Elbokl 指出还需要考虑 confirm commit 的情况，client1 先提交 commit 操作，client2 的 private candidate 和 running 同步以后，如果 client1 没有 confirm 会导致 running 配置回退，这时候 client2 需要再次同步 running 到回退前的配置。

BoF 和 Side Meeting

TVR

会议日期：2022 年 11 月 10 日

参会人数：70

主要议题：

Draft/topic	Duration	Presenter	Role/Company
Time Variant Routing Problem Statement	20min	Rick Taylor	Ori Industries
Use Cases	20min	Ed Birrane	JHU/APL
Topology management challenges for Satellite Constellations	15min	Dan King	Old dog/Airbus
Carbon-aware networking Use Case	15min	Eve Schooler	Intel
Technology Gaps / Potential WG Topics	15min	Rick Taylor	Ori Industries
Open discussion	30min		

BoF Objectives

- We are here to answer a few questions:
 1. What is the problem to be solved?
 2. What new work is to be done?
 - By “work” we don’t just mean create protocols
 - Includes identifying gaps in existing solutions
 3. Is there sufficient interest in working on this problem?
 - ... to get the work done in reasonable time
- And provide input to the AD and the IESG

Time Variant Routing Problem Statement

现有的路由协议希望在网络上维护端到端连接路径，链路改变被认为是必须纠正的特殊情况。纠正措施包括尝试重新建立丢失的邻接关系，以及重新计算或重新发现功能拓扑。但是有很多情况中，路由拓扑的更改是可预测的，这种可预测的拓扑变化应被视为非中断事件。

主要问题包括：

- 一个还没有 up 的链路或节点如何发布他未来的连接；
- 预期出现的节点或连接的事实如何与预测的可用时间和可用窗口一起发布？
- 预期一个节点或链接将中断的事实如何与预测的停机时间和停机窗口一起发布？

The Problem (*continued...*)

The problems in this space include:

- How does a node or link that is not up have its future presence advertised?
- How does the fact that a node or link is expected to come up (i.e., the future reachability of a neighbor) get advertised along with the predicted up time and up window?
- How does the fact that a node or link is expected to go down (i.e., the future removal of reachability to a neighbor) get advertised along with the predicted down time and down window?

The same two questions apply to advertising known variations in metrics which might not be limited to existing metrics, but might also include local, node-based resources.

问题/讨论：现场的讨论主要是针对拿到规划信息后怎么处理，如何最小化中断的影响，以及动态拓扑在不在考虑范围内。

Use Cases

主要介绍了 TVR 的一些场景用例，包括资源受限网络、适应外部条件网络（链路 cost 随环境影响）、移动设备网络。对每个场景的假设和收益进行了介绍，并且每个场景都介绍了一个案例。

Topology Management Challenges for Satellite Constellations

卫星星座网络正在快速发展，对传统的网络拓扑控制提出了新的挑战。主要介绍了卫星网络在拓扑和链路上面临的一些主要问题，包括分布式集中式、如何管理链路状态、如何平衡能耗和路径距离等。最后总结了一下对 TVR 的需求，包括对卫星链路的管理、以及对移动性的管理等。

Carbon-aware networking Use Case

主要介绍了碳排放感知的网络场景，比如将碳排放成本作为一种新型的 metric 开销、尽可能使用清洁能源的电力。碳排放感知网络包括碳感知路由、碳感知传输、碳感知流量工程等。

针对以上 3 个 use case 问题/讨论：

Adbussalam 指出目前解决方案不清晰，主席 Russ 表示目前就是尽可能找较多的 use case 和模型，然后再解决。Dean 表示这个问题的维度太大，IETF 可能没有足够的专家来解决这个问题，放在 IRTF 可能更合适。主席 Lou 表示路由域能做什么是一个大挑战。其他域可能也有一些工作。

Technology Gaps / Potential WG Topics

对现有的路由协议和使用环境进行了分析，分为固定网络和动态网络（MANET）。固定网络中假设节点不会移动并且采用被动响应的方式来维护路由；动态网络中节点运动无规律，连接时暂时的，同时也是被动响应的维护路由。但对 TVR 来说都会导致丢包和不必要的浪费。另一方面 DTN 是传输协议，不是路由协议，TVR 运行在 DTN 之下。

后续的主要工作内容包括：TVR use case, Approach/Framework, 与其他工作组合作进行扩展。

Open discussion

有人提议，在管理方面，需要有类似 NetConf 的东西。不希望在每次发生更改时都有一个单独的管理组织来处理计划和时间，主席 Lou 表示希望重用现有的创建调度表模型。

Jari 表示能耗相关的例子是比较复杂的，卫星的例子相对简单，建议以后工作重点放在简单易定义的用例上。Colin 说现在的范围还是比较大，太空网络和水下网络差很多，希望有一些具体点的工作。Dean 建议不要把 TVR 作为垃圾堆解决所有的问题，看看目前能解决哪些问题，收窄工作范围。

投票部分：94%的人同意 IETF 需要来解决这些问题，74%的人认为需要成立工作组，86%的人愿意成为 tvr 的 author 或者 reviewer。

最后 AD 说这个领域感兴趣的人很多，并且存在问题，但是需要缩小工作范围，做一些我们能做到的事，这个还需要在邮件列表继续讨论。

RADEXTRA

主席：Stephen Farrell (Trinity College Dublin)

背景：EAP/RADIUS 的开发厂商和用户根据过往的开发和运营经验，总结出 RADIUS 协议的不足，希望扩展协议。相比 Diameter，RADIUS 适用场景更广泛；Diameter 设备昂贵，RADIUS 设备相对便宜很多。Diameter 主要用于 3G/4G 场景。RADIUS 适用于 WiFi、企业、大学、Eduroam、OpenRoaming、ISP 等场景。

但是 RADIUS 也面临许多问题：安全性不足，RADIUS 之前定义的安全实践无法满足现代的密码学要求。例如使用不安全的 MD4/MD5 摘要算法。许多云提供商仍然使用 RADIUS over UDP 在 Internet 上发裸 RADIUS 数据包，需要使用 RADIUS over TLS/DTLS。扩展性不足，8-bit RADIUS ID 的限制导致一个连接中不允许同时传输超过 256 个数据包。

推动者及支持者：

FreeRADIUS、Eduroam 的提供商和运营者（如美国 Painless Security 和德国 DFN）、Microsoft、Radiator Software 等。

Charter 工作内容：

- 更新 RFC 6421，废弃使用 UDP 传输 RADIUS。
- 将 RFC 6613 (RADIUS/TCP)、RFC 6614 (RADIUS/TLS) 和 RFC 7360 (RADIUS/DTLS) 升级为 Standards Track。
- 根据 RADIUS/TLS 的经验，定义 RADIUS 漫游的最佳实践。
- 扩展 8-bit RADIUS ID 空间，允许在一个连接中同时传输超过 256 个数据包。

- 允许 CoA/Disconnect 数据包在 RADIUS/TLS 或 RADIUS/DTLS 连接中逆向发送。这个功能允许前向和反向路径是相同的，帮助解决 NAT 穿越问题。
- 定义 RADIUS 的安全变体，该变体不使用废弃的加密方法，如 MD4 和 MD5。这个变体将适合在符合 FIPS 的系统中使用。传输将被要求是 TLS 或 DTLS。数据包的格式与 RADIUS 没有变化。然而，数据包不再需要被签名。属性格式与 RADIUS 没有变化。然而，像 User-Password 这样的属性不再需要被混淆，可以按原样发送。需要 MD4 或 MD5 的属性是被禁止的。简而言之，“没有 MD4 或 MD5 的 RADIUS”。

BOF 运作和讨论情况

- 工作组的目标清晰，对 RADIUS 协议的改进及安全性增强都是来源于实际部署中的经验，因此与会者对于成立该工作组的态度都是正向的，更多的是讨论 scope 和技术细节，例如 TLS 1.2 和 TLS 1.3 版本的强制要求。
- 实现者及运营者都在投票中表示愿意实现及部署这些功能。
- BOF 的三个主要推动者 (FreeRADIUS、Painless Security、DFN) 互相之间打配合，在一家进行宣讲时另两家并不是单纯支持、而是会提出一些反对意见引发更多讨论。体现出并非提前“结盟”，将现场气氛带动地非常好。
- 后续工作组应该可以成立成果。

相关链接：

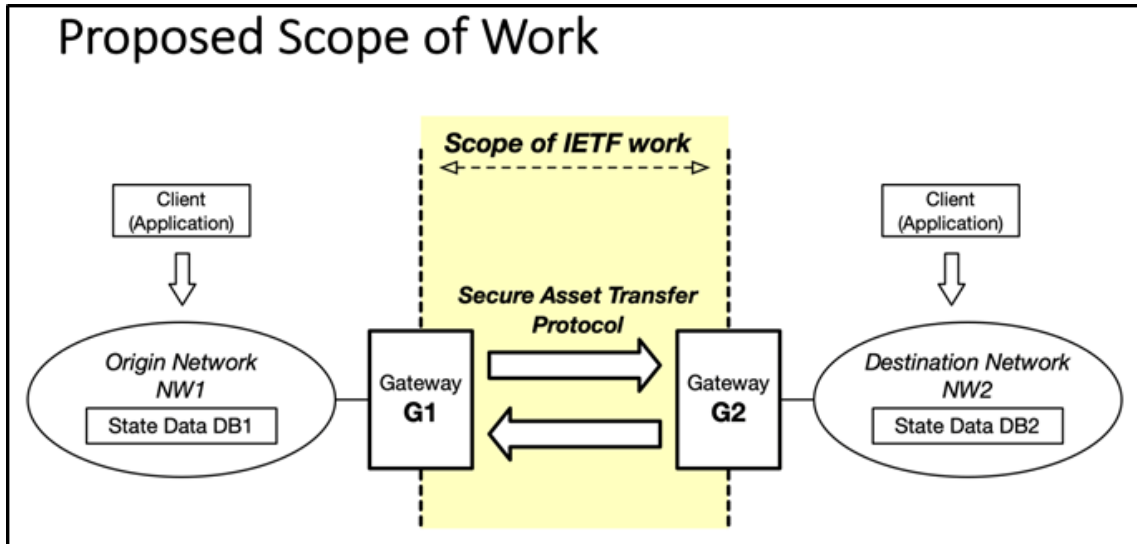
BOF Request:

<https://datatracker.ietf.org/doc/bofreq-dekok-bofreq-dekok-radius-extensions-and-security-00/>

SATP

主席：Wes Hardaker (University of Southern California)

背景：安全资产转移协议 SATP 的目标是开发一种在两个网关之间运行的标准协议，目的是在网络或系统之间转移数字资产。每个网关代表一个网络或系统，SATP 执行数字资产从源网络到目标网络的单向转移，该转移可被第三方验证。



SATP 将在协议的各个方面使用现有的 IETF 标准，包括安全通道建立 (TLS)、有效负载格式 (JSON/JWT)、数字签名和加密 (JOSE/JWE)、数字证书 (PKIX) 等。

SATP 工作组初始范围包括：

- SATP Use Cases
- SATP 架构
- 资产转移消息流
- 资产相关数据共享消息流

应用场景：

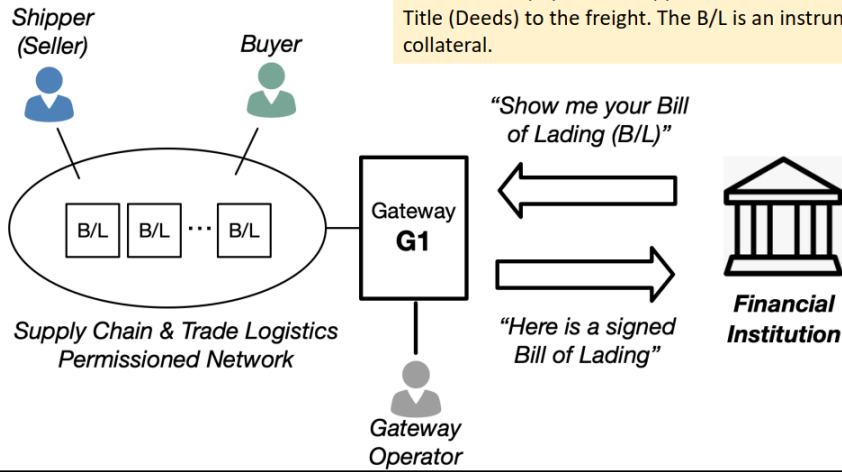
供应链和贸易物流场景：

如下方图 1 所示，买方向卖方购买商品时会拿到提货单 (B/L)、买方以提货单为担保从金融机构贷款、买方再用贷款的钱支付给卖方以最终提货。再进一步，如图 2 所示，金融机构可以提供 Letter of Credit 转账义务证明，买方可以将 L/C 出示给卖方。

当前买方和卖方之间是供应链贸易物流专用网络、B/L 是该网络中的“资产”，金融机构侧是贸易金融专用网络、L/C 是该网络中的“资产”，这两个网络之间是独立分开的。因此想要通过 SATP 在两个网络间完成“资产”的交流。

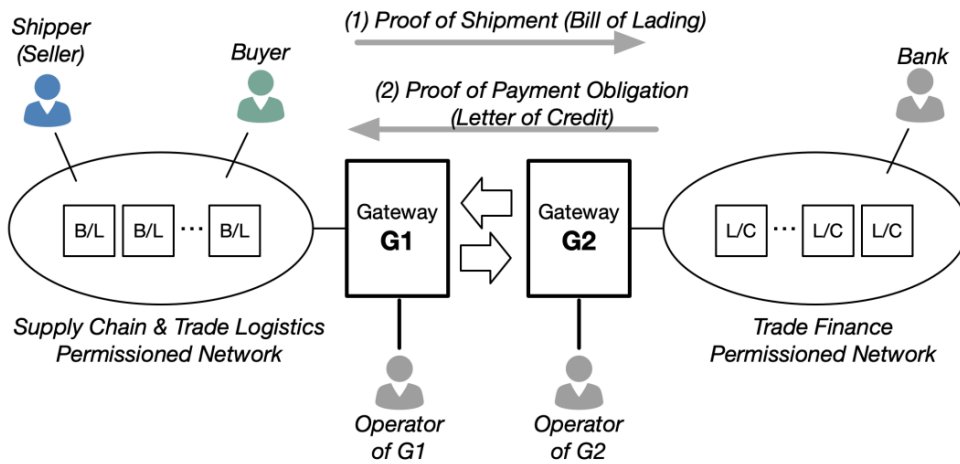
SATP Asset-Related Data Sharing Flow

The Buyer requires short-term loan from the Financial Institution to pay Seller/Shipper. The Bill of Lading (B/L) is the Title (Deeds) to the freight. The B/L is an instrument of loan collateral.

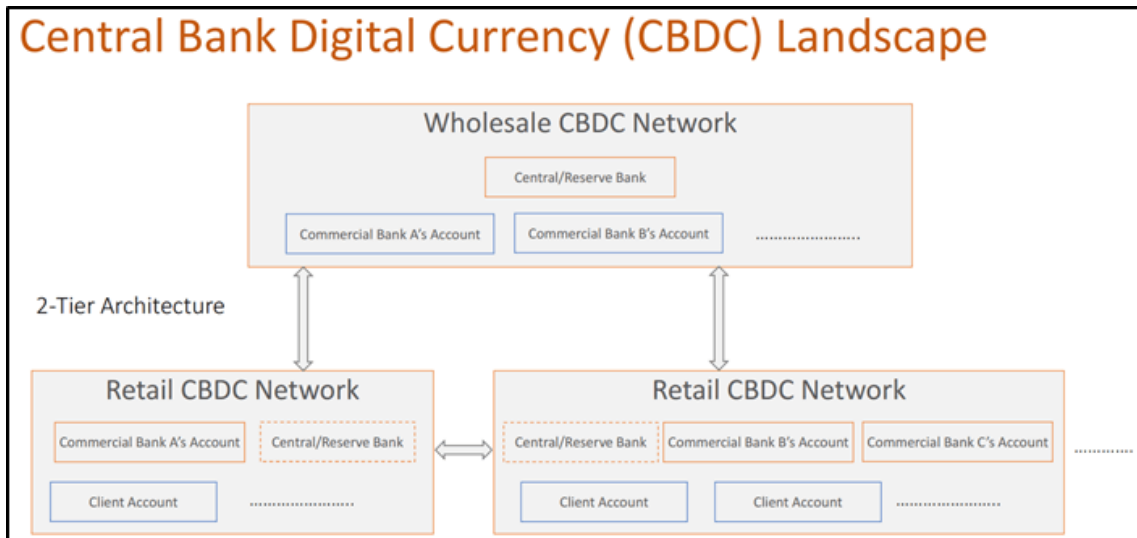


SATP Asset-Related Data Sharing Flow

The Letter of Credit (L/C) is a guarantee of payment based on the Bill of Lading (B/L)



数字货币交易场景：



推动者及支持者:

- 实施者: MIT、IBM、Quant (这三个也是工作组的主要推动者)、Compellio、CSIRO/Data61
- 部署者: IBM、Quant、TradeLens/Maersk
- 观察者: Swisscom、SWIFT、Digital Dollar Project、Gov of South Australia

进展:

SATP 在 IETF 114 时组织了第一次 BOF, 当时被认为 use case 不明确, 场景要满足的前提条件等不明确, 缺少部署和应用等, 未能同意成立工作组。

本次会议时第二次 BOF, 与上次相比, 明确了约束和假设条件、重新校对和简化了 use cases、开始对通用消息流程进行了部署。

讨论:

本次会议上安全域 AD Roman、Mozilla 的 Eric Rescorla 是主要的挑战方, 主要质疑点是该工作是否有实际价值 (如, 谁是该协议的使用者和开发者, 是否愿意参加 IETF), 担心参与人不够变成少数人的一言堂、且做出的标准也没有意义。并且在投票阶段对投票问题进行了特别设计:

对于“该问题是否应该解决”和“IETF 是否是正确的地方来解决该问题”大部分都投了 yes (30+)。

对于“是否愿意 Review 文稿”有 28 人投了 yes，“是否愿意编写文稿”有 12 人投了 yes。

应 AD 和 Eric 的特别要求，增加了“参与者是否愿意实施或者部署该协议”及“运营者是否愿意使用该协议”的投票，前者 12 票 yes，后者 4 票 yes。

这些质疑在第一次 BOF 时也曾被提出来。MIT 等推动者展示了其每周例会的参与情况（平均每次 10 人参加）、邮件列表讨论活跃情况、并且列出来包含企业客户在内的支持者（如 Swisscom、SWIFT 等），希望打消 AD 等的顾虑。

相关链接：

BOF Request: <https://datatracker.ietf.org/doc/bofreq-hardjono-secure-asset-transfer-protocol-satp/>

架构文稿: <https://datatracker.ietf.org/doc/draft-hardjono-sat-architecture>

协议文稿: <https://datatracker.ietf.org/doc/draft-hargreaves-sat-core/>

Use Case: <https://datatracker.ietf.org/doc/draft-ramakrishna-sat-use-cases/>

Metaverse Side Meeting

Agenda

- QuicR and standardization of the metaverse - Cullen Jennings, Cisco
- ICN and networking for distributed AR/VR - Dirk Kutscher, The Hong Kong University
- Low Latency, Low Loss, Scalable Throughput (L4S) Internet Service - Koen De Schepper, Nokia
- Network innovation and standardization for metaverse - Robin Li, Huawei

邮件列表已经生成，如果感兴趣请大家订阅

- List address: metaverse@ietf.org
- Archive: <https://mailarchive.ietf.org/arch/browse/metaverse/>
- To subscribe: <https://www.ietf.org/mailman/listinfo/metaverse>

ETSI-IETF IPE Side Meeting

1. Around 70 attendees including IESG member, 5 IETF ADs, IAB members, several WG chairs; IPE management team; operators, vendors, government delegates, etc.
2. Both EC(DG Connect) and UK(Cybersecurity Centre) attended the meeting, showing the interests from the 2 governments. They will probably report back to the government ETSI delegates.
3. Some challenging questions like IPE position and value was raised from some IETF attendees, and Latif together with Tayeb, and operators in IPE provided answers to clarify.
4. The future cooperation between the two organizations was discussed, achieving a rough consensus that each organization works on its own scope, and use "touch points" to cooperate. The moderator proposed to have IPE-IETF meeting in future IETF meetings, transforming this into a periodical event.
5. This joint meeting allowed IPE to talk directly to IETF community and explain them IPE's position and opinion from Industry Players like Swisscom, Sky and Cisco. It is more efficient than a formal liaison approach.

Main outcomes of this IETF – IPE side meeting are:

- Recognized that the work in IPE is complementing the work of IETF
- Recognized that IPE is helping to increase the awareness and the deployment the IPv6 standard specified by IETF
- Emphasized that IPv6 is helping to accelerate the Digital Transformation
- Expressed Interest to transform this side meeting into regular appointments for the coming IETF meetings or as a formal collaboration between the two SDOs, which needs investigation from administrative and governance perspective

MIMI

MIMI: More Instant Messaging Interoperability, ART 域的新工作组。

Chair 是 Alissa Cooper, Pete Resnick

即时通信应用互联互通, 微信, QQ, iMessage, WhatsApp 等等。Motivation 之一是欧盟的 DMA 法案要求互通。

Problem Statement by Rohan Mahy

各家的即时通信应用不互通, 用户体验不好。希望能做一个通用的互联互通的 Instant Messaging 协议, 类似邮件协议。

这样的一个协议需要定义如下内容:

- 消息层: 公共的消息格式,
 - 加密层: 端到端加密的 profile (端到端意味着服务器也无法获取消息内容, 只有消息的发送者和接收者能看到) 使用 MLS (Messaging Layer Security)
- Architecture
- 传输层: 如何传输 MLS message
 - 如何加好友, user ID 和 email、phone number 等等的映射。

其他内容包括 SPAM 预防, 和内容监管。

讨论: 查找一个人的账号的时候是否暴露他在所有平台的账号, 允许其他用户从哪个平台联系他。respect user preference regarding discoverability.

End to End encryption message 是不足够的, 需要同时保护好每个人的 public key, maybe PKI system?

本工作组的目标不是 enable 全新的 messaging service, 而是在已有的 message service 之间提供互通服务, possibly 以 gateway 的方式。

Charter Discussion

讨论 discovery (给定 ID, 找到这个 ID 的用户在哪个 service) 和 introduction (给定 ID+service, 跟他加上好友能开始聊天) 要不要放在 charter 中。introduction 是肯定需要的。discovery 未必, 可以有其他 out of band 的解决方案。

讨论防止 SPAM 要不要放在 charter 中

BoF Questions problem statement is unclear? SPAM 和 DMA 是否要放入 charter 中。

IETF is a not an appropriate venue for solving the problem?

Object to forming the WG? No.

Willing to review author/chair? 都有响应

Implementation? 也有

结论，会后修改 charter，大概率会成立。