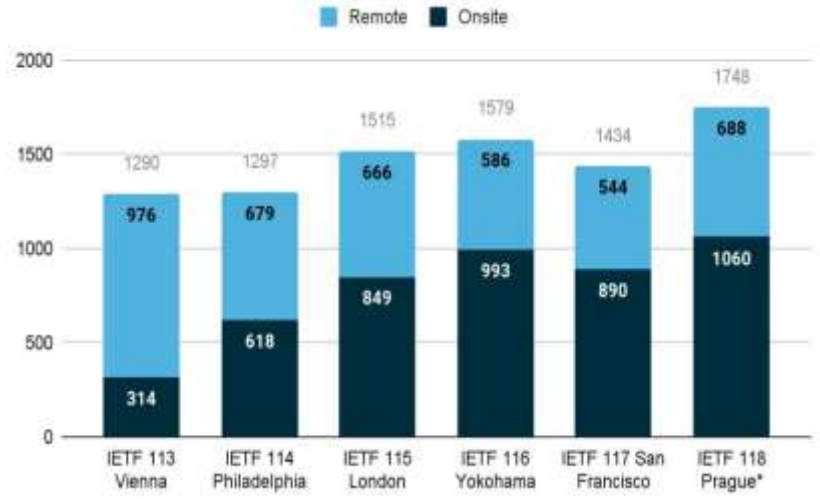
IETF118 Inclusion

Huawei Datacom Research Department

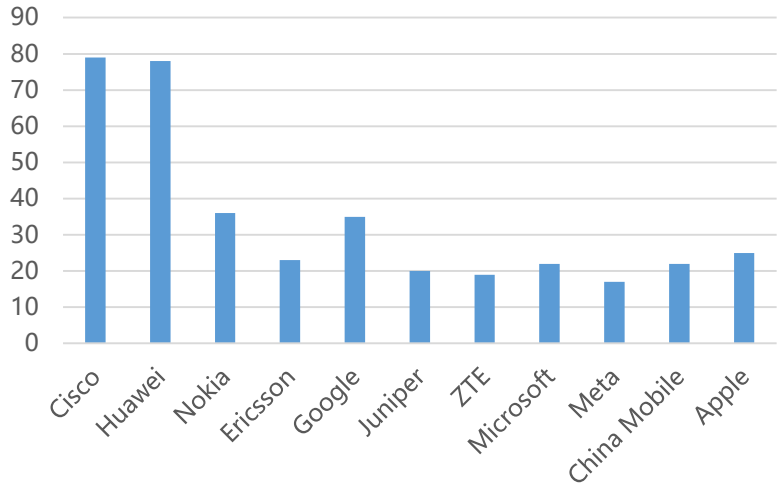
IETF118: attracts more people from both industry and academia, the attendees hit the record high since COVID-19

IETF®

- **1748 Registrations**
  - IETF117 San Francisco experienced a drop, because of the VISA policies.
- **Cisco and Huawei send most participants**, while CT and IT companies keep contributing to IETF.
- **People are keen on running code and real problem**
  - 572 Hackathon registrations: time variant network, path validation, etc.
  - 40 Side meetings: segment routing operations, network management operations, AI for network, network digital map, incident management, sustainability Insights, etc.



Meeting registration over time



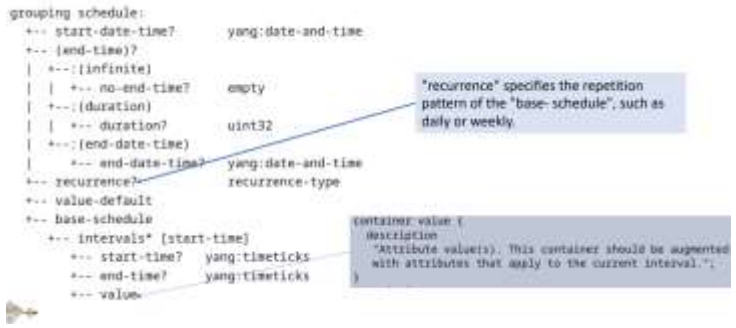
Participants by Company

Green Networking

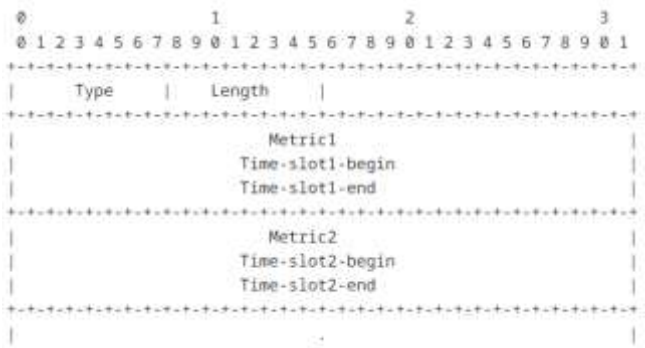
- **Existing Drafts in IETF:**
  - **draft-irtf-nmrg-green-ps** (Futurewei): which outlines a corresponding set of **opportunities**, along with associated **research challenges**, for networking technology in general and management technology in particular to become "greener", i.e. more sustainable, with reduced greenhouse gas emissions and carbon footprint.
  - **draft-wang-cats-green-challenges** (China Mobile): which outlines a series of **challenges and associated research** to explore ways to reduce carbon footprint and reduce network energy **based on CATS.**
  - **draft-cx-opsawg-green-metrics** (Futurewei): which explains the need for network **instrumentation** that allows to **assess the power consumption**, energy efficiency, and carbon footprint associated with a network, its equipment, and the services that are provided over it. It also suggests a set of **related metrics** that, when provided visibility into, can help to optimize a network's "greenness" accordingly.
  - **draft-petra-path-energy-api** (Cisco): which describes an **API** to query a network regarding its **Energy Traffic Ratio for a given path**.
  - **draft-li-ivy-power** (Juniper): which proposes a **YANG model for power management** to support the automated **powering off of network elements in the scenario of traffic fluctuation**.
- **Sustainable Side Meeting:**
  - Cisco introduced **sustainability insights** and **energy efficiency model**(draft-almprs-sustainability-insights-02 , draft-opsawg-poweff-00)
    - The energy efficiency model provides information and data requirements for calculating the Power and Energy Efficiency for specific assets, including hardware, software, applications and services.
    - Sustainability insights describes the **motivation and requirements** to collect asset **centric metrics** including but not limited to power consumption and energy efficiency, circular economy properties, and more general metrics useful in environmental impact analysis. It provides foundations for **building an industry-wide, open-source framework** for the **reduction of greenhouse gas emissions**, enabling **measurement and optimization of the impact on the environment** of networking.
- **IAB Program Eimpact:**
  - Futurewei & Cisco summarized the IETF's existing green networking **challenges, metrics, information models, and sustainability insights**, the main problems raised on site are the **lack of use cases** and how to **use these metrics to reduce energy**.
  - Nokia introduced the overview of **existing standardization work on ICTs & Sustainability**. **ITU-T**' s SG 5 has developed some approaches for **evaluating and reducing greenhouse gas emissions** of communication and digital technologies. 3GPP primary focus on developing standards and **improving mobile communication technologies**. For example, the 3GPP SA Working Group 1 aims to **introduce energy efficiency as a service** in R19.
  - UC3M introduced an **API** to query a network regarding its **Energy Traffic Ratio for a given path**.

TVR (Time Variant Routing)

- **TVR Requirements and YANG are Gradually Stable**
  - Daniel **updated the TVR Requirements draft**, and the content of it is basically completed. **China Mobile**, **Huawei** and **ZTE** are the **Contributors** of this draft.
  - Yingzhen updated the TVR use case draft and added two new example on **Tidal Network and Predicable Moving Vessels**. This draft also applied for the **WGLC.**
  - Yingzhen **merged the existing TVR Yang models** into one draft. There was a discussion on **whether need to include the device function** in the model and **whether should be an independent Yang model**.
  - ZTE introduced **IS-IS and OSPF extensions for TVR**. The WG chair(Tony Li) thinks that IGP extensions are **out of scope** of TVR charter, and Tony(head off) **does not agree with the idea** of carrying time-varying information through IGP extensions. However, the LSR chair(Acee) thinks that **extending Flex-Algo for TVR is a possible direction**, but it need to get the confirmation from TVR.
- **Time Schedule side meeting：Define a Unified Basic Time Scheduling Model**
  - At the meeting, it was agreed that Qiufang from Huawei should define a **unified basic time schedule model** for other work groups (including TVR and OPS).
- **Deepspce IP Side Meeting：Explore End-to-End IP Solutions for Deep Space**
  - Huitema introduced the performance of QUIC in deep space networks. Long delay leads to frequent session interruptions and some congestion algorithms cannot work well.
  - Jean-Philippe introduced the **IP forwarding solution for deep space**, which uses **storage instead of forwarding** when links are unavailable. The possible implementation schemes, including expanding interface queues or adding virtual interfaces.
  - UCL’ s Maxime introduced QUIC's extensions for deep space networks, including adding FEC packets to avoid packet loss and retransmission, and extending the additional address advertisement capability to cope with address switching.



TVR Yang Model



ISIS and OSPF extensions for TVR

Non-routing Information Distribution Side Meeting

Background

- The BGP/IGP routing protocols have been used to convey various types of non-routing management information in addition, and BGP, in particular, has numerous extensions to do this
- The industry has always been concerned about the routing protocol as a "garbage truck" approach, will have an impact on the robustness of routing protocols, has appeared different solutions based on the BGP independent Instance, IGP independent Instance, as well as independent protocols etc.

Meeting Overview

- The meeting was chaired by Sue Hares (IDR co-chair), with 31 attendees (including 7 online), covering operators and vendors such as Orange/Telefonica/China Mobile/China Unicom/China Telecom/China Satellite Networks/Cisco/Juniper/Ericsson, as well as professors from universities such as Beijing University of Posts and Telecommunications/Lancaster University.

Key Points

- Some experts believe that the problem can be solved based on existing technologies, for example, Acee Lindem/Yingzhen Qu, co-authors of OSPF-GT, believe that this technology supports loose topology and decoupling with OSPF, which is an ideal carrier for non-routing information distribution; Toerless Eckert from Futurewei believes that the BGP independent Instance+independent TCP session is good enough to realize the isolation of routing/non-routing data processing.
- More experts, such as Tony Li/Tony P/Adrian Farrer/Joel Halpern etc. believed that the current approach of extending routing protocols to carry non-routing information is difficult to carry on in the long term, including the following concerns:

  1) Complexity: the expansion of various types of information option makes routing protocols more and more complex, development/maintenance costs are very high

  2) Limited expansion space: BGP/IGP can be expanded in a limited space, it is impossible to expand down forever

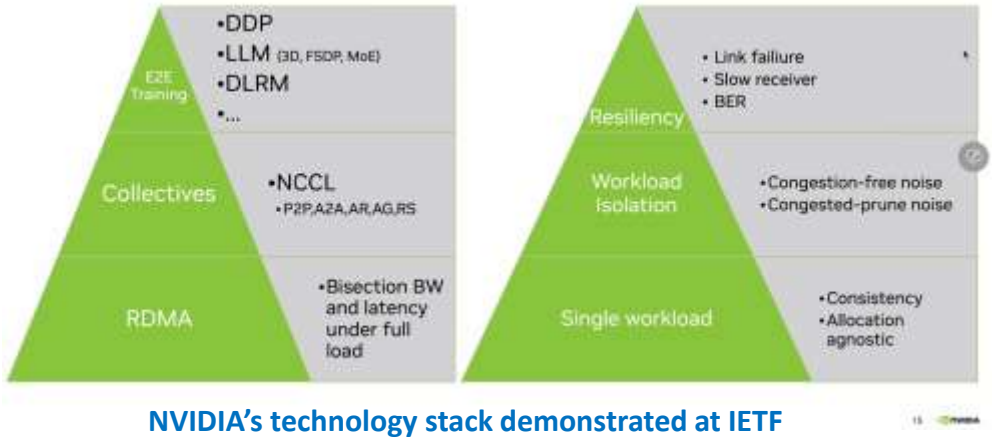
  3) Architectural vulnerability: the distribution of non-routing information is bound to the routing calculation, forming a "fate-sharing", a loss of all losses.

Next Step

- Applying IETF Mailing list: Based on the discussion of the meeting, request the routing domain AD to create a dedicated mailing list to continuously discuss on the topic, gather consensus, and prepare for the next side meeting.

Increasing Attention to AI DCN with In-Depth and Intense Discussions

Futurewei and NVIDIA jointly organized the **AI Data Center Network Side Meeting** at the IETF for two consecutive times. Huawei and China Mobile held the first **collective communication optimization** (a.k.a. in-network computing) Side Meeting. **NVIDIA**, **Broadcom**, **Juniper**, **Google**, and **Tencent** were invited to present more than 10 technical topics. (Load balancing, new topologies and networking technologies, efficient congestion control, offloading collective communication operation). The meetings involved more than 200 participants from **Cisco**, **Huawei**, **Nokia**, **H3C**, **Arrcus**, **Ericsson**, etc..



NVIDIA's technology stack demonstrated at IETF

Agenda for 118 AI Data Center Network Side Meeting

1. 17:00 Opening
2. 17:10 Networking in AI -- Omer Shabtai (Nvidia)
3. 17:35 Astral-Network: efficient large-scale datacenter network for large language model training -- Baojia Li (Tencent)
4. 17:55 Self-Adjusting Networks -- Stefan Schmid (TU Berlin)
5. 18:15 CSIG - Simple and Effective In-band Network Signals for Efficient Traffic Management in Datacenter Networks -- Abhiram Ravi (Google)
6. 18:45 Open Discussions

FUTUREWEI Technologies, NVIDIA, HUAWEI, Juniper Networks, BROADCOM, 中国移动 China Mobile, Technische Universität Berlin, Google, Tencent 腾讯, Yandex

.....

Venue photos of IETF 118 AIDC Side Meeting

Observations:

The number of participants in the 118 meeting increased significantly. In terms of topic content, more emphasis was placed on more understandable and practical training process and the presentation of specific techniques, involving more discussions and feedback onsite as well as on the mailing list.

1. **Google** teamed up with **Broadcom** hardware engineers to promote the **new telemetry CSIG** for congestion control.
2. **NVIDIA** continues to emphasize that Dragonfly is not only used for HPC; bandwidth is never enough; AR and CC need to be **generalized** and **do not rely on** the specific algorithm **pattern** (tree/ring or others), nor on specific **topologies** (such as symmetric topology); when congestion occurs, collective communication should be given **higher priority**.
3. **Broadcom** shared the details of RDMA's **in-network computing** considerations and **multicast** (under development), emphasizing the importance of **multi-tenant** security issues.
4. Some participants are concerned about the **new international alliance UEC** and hope to invite the IETF to introduce the situation.

Agenda for 118 INC (In-Network Computing) Side Meeting

1. Use cases, problem space and requirements: kehan Yao (China Mobile)
2. Challenges in hardware offloading of collective operations: Alex Margolin (Hebrew University of Jerusalem)
3. Signaling In-Network Computing operations (SINC): David Lou (Huawei)
4. In Network Compute: Surendra Anubolu (Broadcom)
5. Open Discussions

Observation: IETFers are unfamiliar with the background of collective communication. This meeting aimed to introduce the multi-target communication model and optimization technology commonly used in AI training scenarios.

BGP：Intent-based Routing not converged, Next-hop draws attention

Intent-base Routing

- IDR WG plans to initiate the second WG LC on BGP CAR and BGP CT, once the WGLC is finished, both documents will be published as **experimental RFCs**.
- According to the feedback from operators, IDR WG still consider to produce **a converged BGP extension solution** for intent-based routing.
- SRv6 is split out from BGP CT base draft, the BGP CT base document only covers MPLS based solution, BGP CT SRv6 is specified in a separate document
- BGP CAR draft covers both MPLS and SRv6 data plane, Cisco claimed that CAR SRv6 mechanism has been implemented
- BGP CPR is adopted as a WG document, which provides SRv6 intent-based routing with existing BGP protocol
- Juniper proposed extensions to BGP AIGP for generic metric types (e.g. latency)，which can be used for intent-based end-to-end path selection

BGP NextHop Related

- BGP NextHop Capability draft passed WG LC, which can be used for advertising the entropy label capability of the next-hop node. It can also be used for carrying other capabilities of the next-hop node.
- Juniper continues to progress BGP Multi-Nexthop extensions，which can carry multiple next-hops in one BGP update, and the encapsulation and forwarding behavior for each next-hop can be customized. Many discussion was raised during the WG adoption poll.

MPLS: Slow Progress of MNA triggers WG Chair Replacement

- Due to the slow progress of MNA, the MPLS WG Chair (Loa Andersson) was asked to stepped down, and RTG AD assigned a temporary new Chair (Adrian Farrel) to handle the MNA work
- MNA requirement draft received many comments during WG LC, and triggers another round of discussion on ISD vs PSD, draft needs to be revised to solve the received comments
- MNA use case is presented on IETF 118, authors mentioned some use cases needs to be revisited, Detnet chair mentioned the bounded latency use case hasn’ t reach consensus in Detnet WG, the use case draft needs another round of update and review
- Juniper is eager to accelerate MNA progress, while WG chairs said there is no definite time plan for MNA, they need to collect opinions from participants, start from the update of the requirement document and follow normal IETF procedure
- Ericsson still claimed that there is no clear use case of MNA PSD, and asked to remove PSD from MNA requirement, architecture and solutions
- Huawei initiates the discussion about the limitations of ISD， and suggests MNA architecture to include both ISD and PSD
- ZTE presents drafts on ISD capability advertisement, MNA based bounded latency and MNA based IFIT solutions

IPv6 Deployment：Google plans to shut down IPv4

- **Google:**
  - Jen from Google presented “Turning IPv4 off in Google”. Currently, 90+% Google official network use IPv6, aim to make it 100%。
  - Use IPv6-Only Preferred Option for DHCPv4 defined in RFC8925 to turn down IPv4 step by step.
  - Shared 5 lessons, including：
    1. The only way to get IPv6 deployed is to run out of IPv4
    2. You do not really operate IPv6 until you turn IPv4 off
    3. Having IPv6 enabled on endpoints ;)
    4. Allowing extension headers
    5. Default Address Selection Rule

- **Students from India：**
  - Two students from India shared the IPv6 ND6 Deployment。

- **Suggest more students to participant in IETF activities to facilitate the development of IPv6.**
- **Will continue to hold the side meeting to share experience of IPv6 deployment.**

SRv6 Ops Side Meeting at IETF 118, building a platform for SRv6 deployment & Operations discussion

[**Status]** Over 50 participants, including major operators like Bell Canada, Swisscom, BT, MTN, Telefonica, Orange, Softbank, and Verizon, joined the meeting.

[Invited Talks]

- Bell Canada: highlighted the ease of deploying SRv6 at the host level, simplifying data center and network edge gateway deployments, also discussed technical benefits like routing and hardware scalability, security, and load balancing capabilities.
- China Mobile: presented their C-SID deployment status, focusing on cloud leased lines and CMNet. They shared key challenges and solutions related to multi-vendor equipment management, cross-domain deployment, reliability, SRv6 address planning compression, and security.
- EANTC: An increase of SRv6 test participating vendors is presented (8 in 2023) and expanded test capabilities to include basic SRv6 forwarding/routing, EVPN/L3VPN, reliability, anti-microloop, Flex-algo, and more.
- MTN: outlined their network evolution goals, including improving user experience, accommodating growth, simplifying O&M, etc. He then presented SRv6 and digital maps as solutions to enhance network capacity and automation.
- Swisscom: Focusing on network visibility and O&M, they emphasized the importance of data collection and anomaly detection. They collaborate with vendors/operators to build a comprehensive Telemetry system, catering to different SRv6 deployment stages and reducing deployment costs through enhanced data plane and routing visibility.
- Telefonica: They showcased interoperability tests with three vendors covering L3VPN, TI-LFA, uSID, and Flex-algo. They also raised technical issues faced during deployment, like interoperability and address planning, seeking discussion with other operators.
- **[Conclusion]** SRv6 adoption is accelerating globally. Operators seek further discussions on SRv6 operation and maintenance, including configuration optimization, broader vendor interoperability testing, and flavor selection, to pave the way for future advancements.

RAW architecture is gradually stabilizing, Wired deterministic continues to discuss scalability requirements and corresponding queuing algorithms

Merging and Charter Update:

- RAW has officially merged into the DetNet Working Group.
- The DetNet charter has been updated to encompass contributions related to wireless determinism.

Wired Determinism:

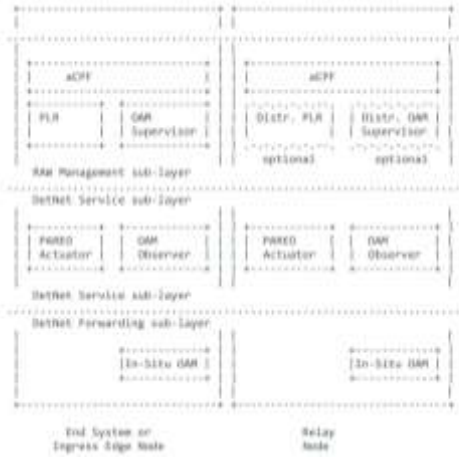
- Extensible data plane remains the core focus. Discussions on this critical topic revolve around two main areas:
  - Queue scheduling algorithms: The Open Design Team has been exploring various algorithms for some time; WG suggests to make evaluation more and leverage existing work from IEEE to maximize efficiency.
  - New QoS and TE-based DetNet data plane: This is a fresh proposal brought forward during this meeting. The use cases and scenarios are not clear, which request further definition and refinement through discussion and exploration.

Wireless Determinism (RAW):

- RAW architecture is nearing stability, with Layer Violation and terminology being key discussion points.
- Carlos presented three contributions on cross-domain, mobility, and MEC integration for RAW.
- The main goal of WG now is to maximize reuse of existing DetNet architecture and materials for better integration.

		C-SCORE/Deadline/TCQF/CSQF/gLBF/TQF	
section	Requirements	Evaluation	Notes
3.1	Tolerate Time Asynchrony	Yes – 5, Partial – 2	Partial: TCQF, CSQF (Partial - within domain. Yes - async across domains & tolerates jitter)
3.2	Support Large Single-hop Propagation Latency	Yes – 7	
3.3	Accommodate the Higher Link Speed	Yes – 3, Partial – 3, TBD – 1	Yes: TCQF, CSQF, queue resizing Partial: C-SCORE, Deadline, TQF TBD: gLBF
3.4(1)	Be Scalable to the Large Number of Flows	Yes – 6, Partial – 1	Partial: queue resizing
3.4(2)	Tolerate High Utilization	Yes – 6, No – 1	No: queue resizing (design non-goal)
3.5 (now 3.6)	Prevent Flow Fluctuation from Disrupting Service	Yes – 7	
3.6 (now 3.5)	Tolerate Failures of Links or Nodes and Topology Changes		Not related to queuing mechanisms directly
3.7	Be Scalable to a Large Number of Hops with Complex Topology	Yes – 5, Partial – 2	Yes: C-SCORE, CSQF, gLBF (flow interleaving TBD), deadline, TQF Partial: TCQF, queue resizing
3.8	Support Multi-Mechanisms in Single Domain and Multi-Domains		Not related to a single queuing mechanism directly

DetNet Queuing Mechanism Comparison



RAW Node Architecture

Multicast: less new work, steady progress on preliminaries, QUIC Multicast triggers discussion

PIM:

- SR P2MP: Replication Segment RFC queue, other drafts progressing. SRv6 additions to Policy Ping being reviewed.
- Address Assignment: GAAP and IPv6 Zeroconf mechanisms discussed, some discussions on supporting both SSM and ASM address ranges.
- EVPN Multicast: Yang model and PFM-SD extension for multi-homing discussed.

BIER:

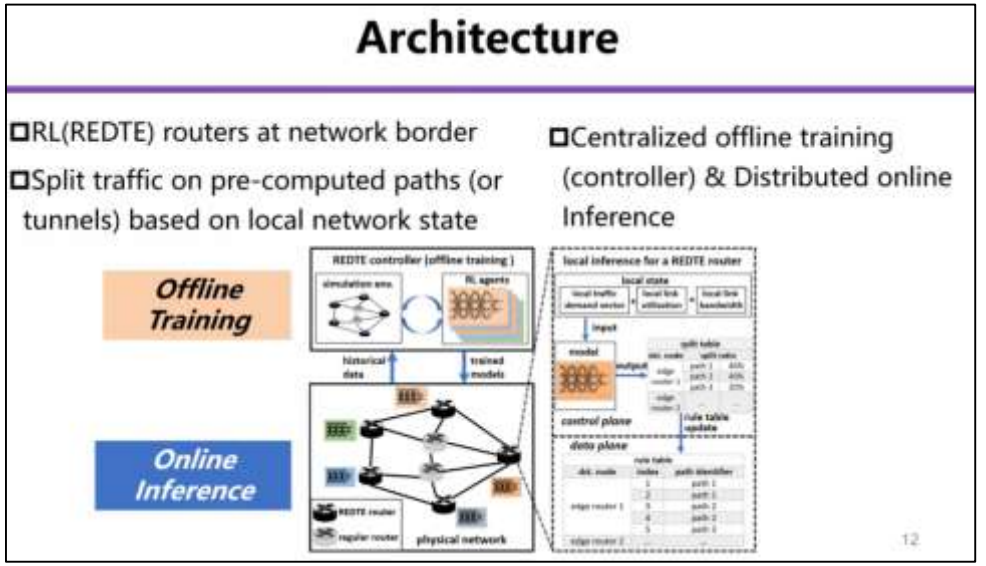
- Mature Drafts: BFD, Ping, and Prefix Redistribution nearing completion, seeking shepherds. BIER TE control plane drafts ready for adoption.
- Implementation and Deployment: P4 implementations, hackathons, and ENTAC testing in progress.
- New Work: Generic Multicast Router Election and BIER uloop under discussion.

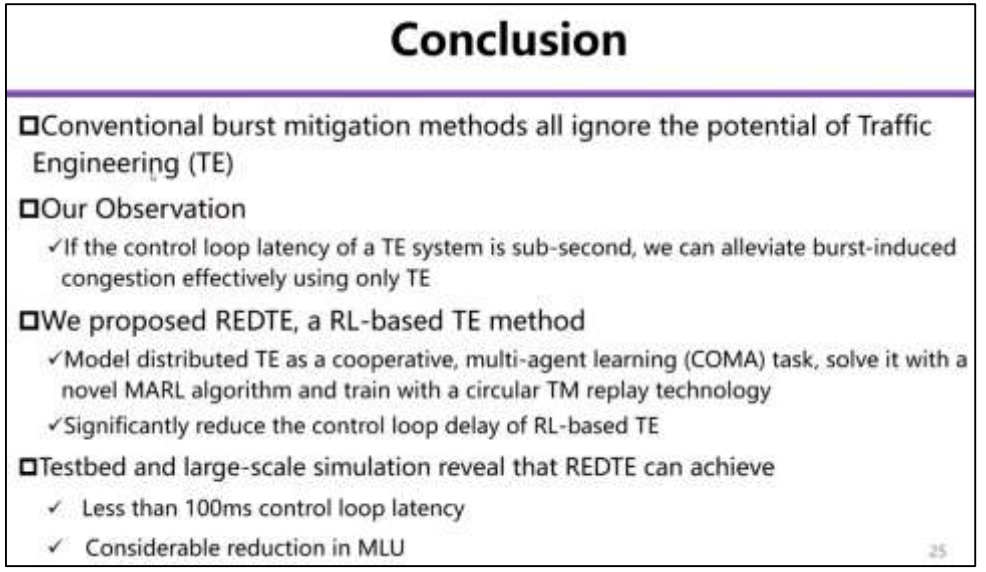
Mboned:

- Limited Applications: Existing drafts like telemetry and AMT YANG still under progressing, seeking reviews.
- QUIC Multicast: Introduction sparked discussion on retransmission and integrity mechanisms. Scalability analysis presented.

AI for Network：Hot topic but hard to be standardized

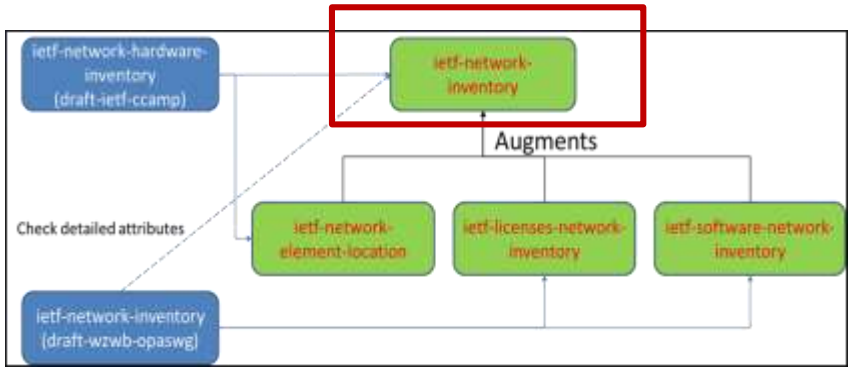
- **Side Meeting Materials**:
  https://github.com/danielkinguk/ai4network
- **5 invited Speakers**:
  - Italy Professor Marco, POLITO 、IEEE Fellow：AI for Network;
  - Professor Dan Li, Tsinghua University: REDTE: Exploiting the Power of Reinforcement Learning for Fast Traffic Engineering in Wide Area Networks.
  - Rajiv Ramdhany, Senior R&D Engineer and Scientist, BBC: AI4ME: Network Challenges and Role of AI in Personalised Object Media at Scale
  - Gadi Singer , Traffic Management Network Architect at Broadcom Core Switch Group: AI Training Network Unique Requirements
  - Weiqiang Cheng, China Mobile: Requirements of AI for Network & Practice in iBNG
- **Conclusion**:
  - Speakers are come industry, Universities, and institute, and people are interested in the topics.
  - But AI4NET is more about research and algorithm, it is a little bit far from standardization



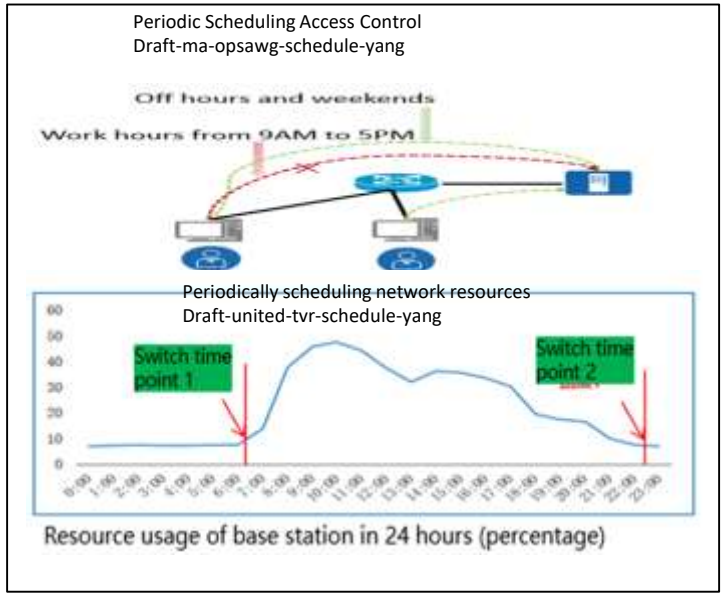


Digital Map Interface Progress: Network Inventory Management, Time Scheduling, and Incident Management

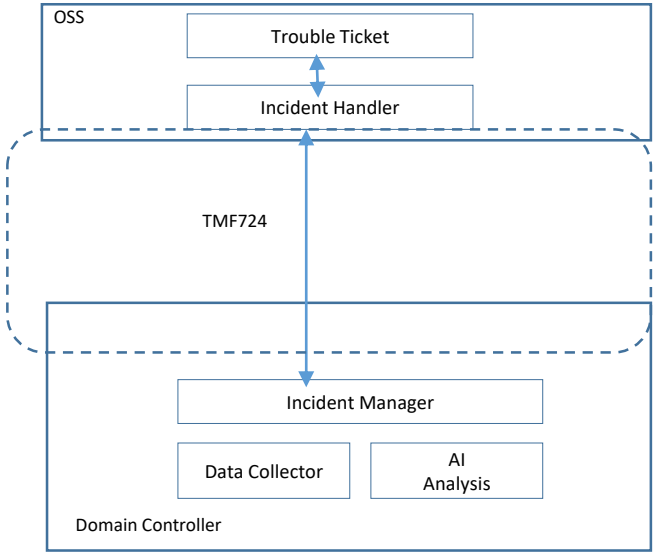
(1) Digital map network inventory IVY WG: The second meeting of the IVY working group mainly discussed network inventory core model, as well as multiple extensions, including software, entitlement, inventory correlation with topology, and power management. At present, the core model has reached WG consensus and been successfully adopted by the WG. Huawei's contribution to the software inventory and inventory topology has been widely discussed and supported.
Participants: Huawei, Cisco, Juniper, Swisscom, Telefonica, and Orange
Next step: Cisco, Orange, and Huawei reached an agreement to promote the convergence of the entitlement management draft. Juniper and Cisco showed great divergences in green and power management solutions, which requires more time to converge and align with other vendors.



2. **Time Schedule Side meeting:** discussion of time scheduling UC which involves two OPSAWG Time Scheduling drafts (UCL policy enforcement, OAM test scheduling) and TVR WG Time Scheduling draft (network properties scheduling) and unified modeling of scheduling(e.g., period, recurrence)
Participants: Huawei, Nokia, LabN, Cisco, Telefonica, and Orange
Next step: A general consensus has been reached that the TVR and OPSAWG OAM drafts are both based on the Time Schedule common model defined by Huawei in the OPSAWG WG.



3. Incident management side meeting: Incident management models are parallel interfaces for traditional alarm management. Based on the TMF Incident API Profile standard, root cause and service impact analysis are resolved. The side meeting focuses on terminology and UC discussion.
Participants: Huawei, Swisscom, Ciena, Ericsson, Telefonica, and AWS;
Next step: Initiate a discussion on incident terms and requirements on the OPSAWG mailing list, reach a consensus, and apply for acceptance by the WG.
Insight: AWS, and Swisscom promote the standardization of **fine-grained packet discard reporting** on the devices, such as TTL expired and checksum errors.



Green Networking Sprouts in IETF OPS Area

Overall progress: The IAB has organized the Environment Impact Workshop and E-impact IAB program to further catalyze the discussion on this direction. The IETF has held many side meetings on sustainability. Currently, multiple vendors from Cisco, Huawei, and Juniper have submitted related drafts in the OPS area.

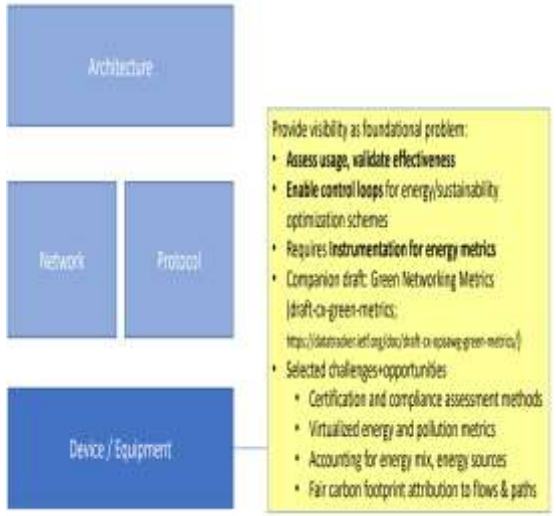
Huawei green networking value proposition:
Analyze the challenges of green networking from architecture, network, protocol, and device levels, and propose solution that green networking from visibility to controllability.

Cisco Green networking Value Proposition:
Power and energy efficiency, traffic visualization, and report power and energy efficiency of an asset, derived from asset lifecycle management model

Cisco Green networking Value Proposition:
Energy-saving for the whole network: collects energy consumption information from network devices, IT devices, and various Telemetry protocols for centralized processing.

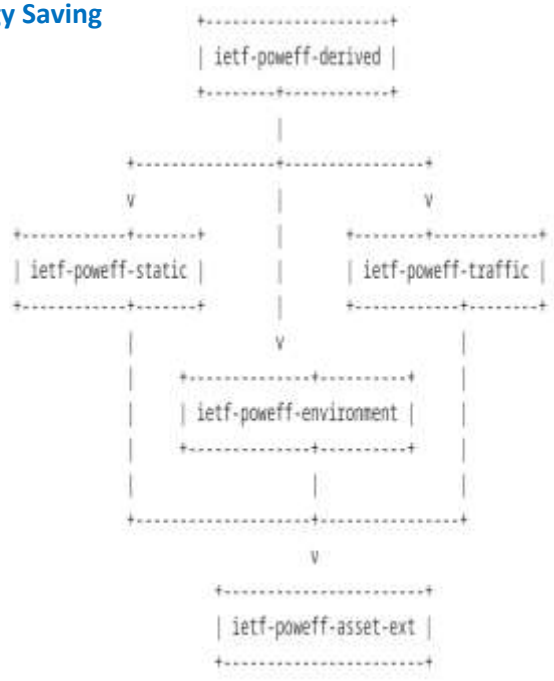
Juniper green networking Value Proposition:
Focusing on inventory core model based power management for network devices, including power off ports/boards of network elements and functional dependency between components;

Huawei: Multidimensional Challenges in Energy Saving



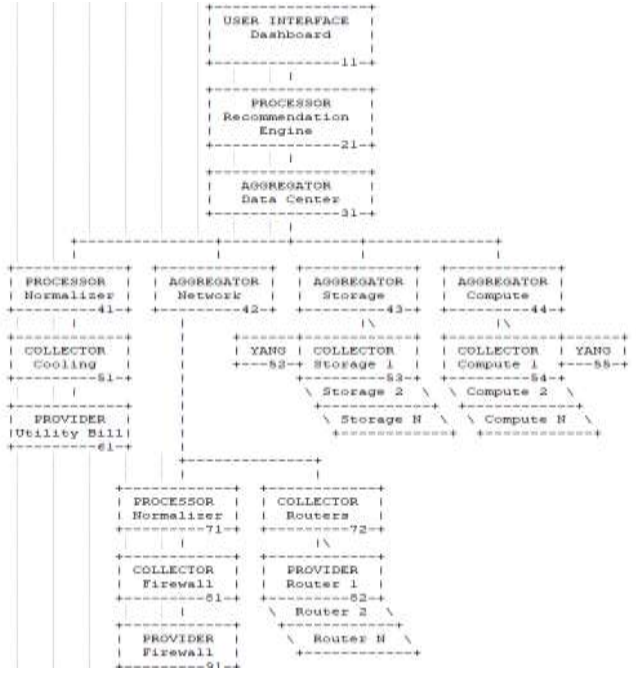
draft-irtf-nmrg-green-ps

Cisco: Asset energy saving + Traffic energy saving



draft-opsawg-poweff

Cisco: Network-wide energy-saving data processing



draft-lindblad-tlm-philatelist

Juniper: Power Management for network devices

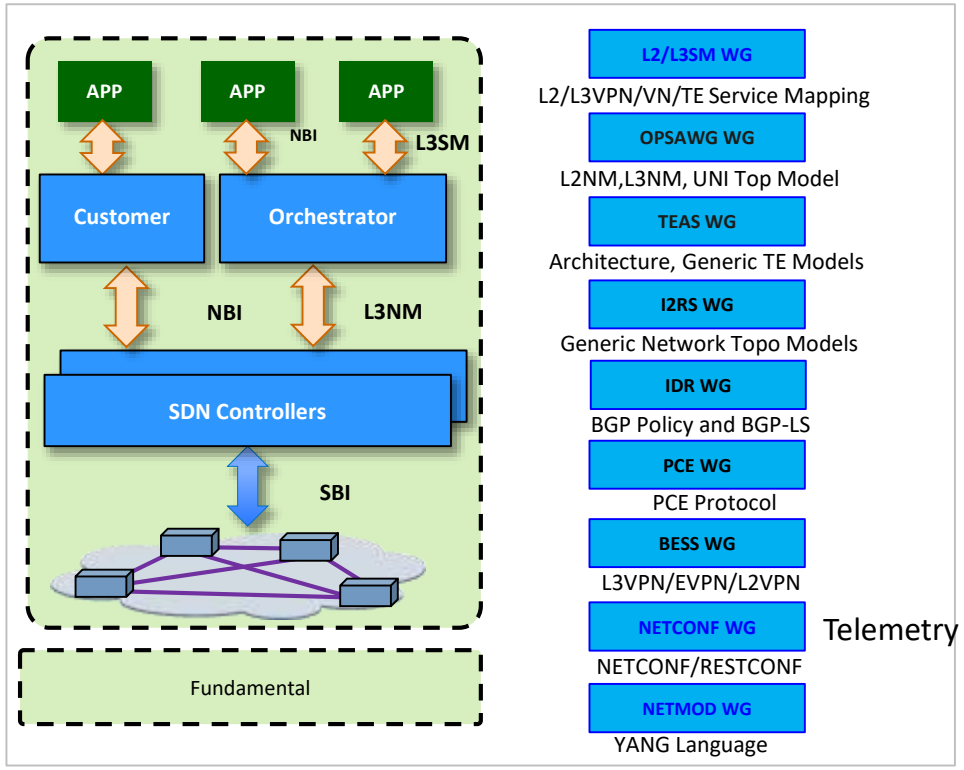
Goal: Enable detailed power management for network elements

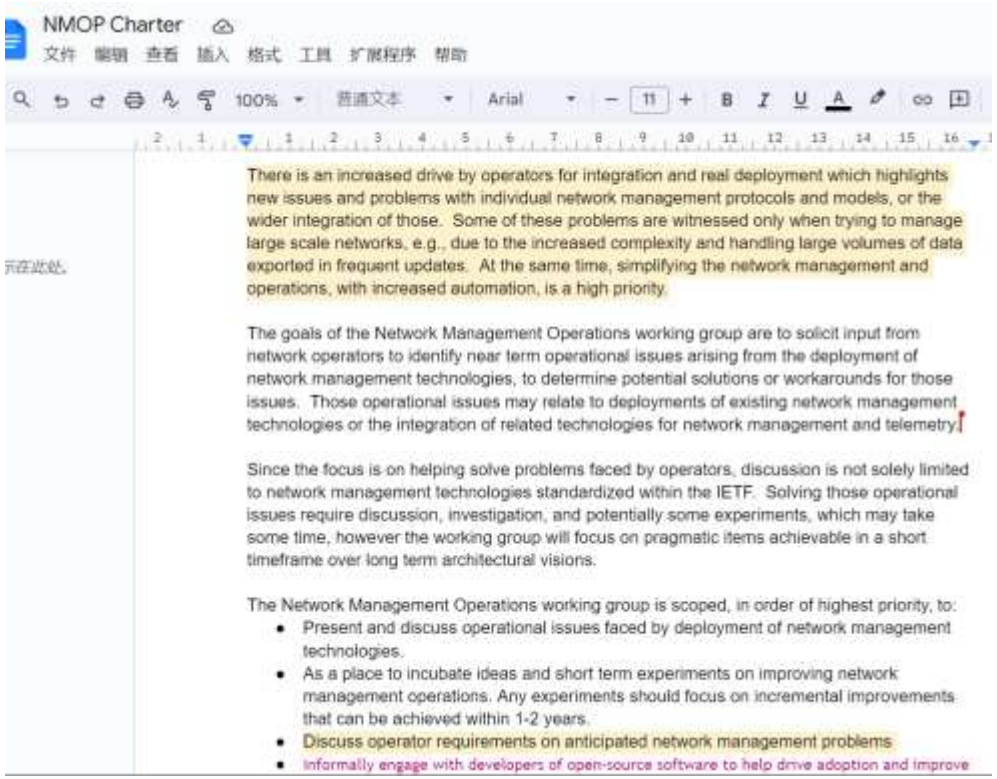
- Report on power consumption on a per-component basis
- Allow the management plane to put a component into power-save mode (if capable)
- Model functional dependencies between components (e.g., this line card requires that switch card)
- Allow the management plane to provide expected traffic to the system for internal power optimization
  - 10% traffic load requires only 10% of the switch fabric

```
+--rw component* [component-id]
   +--rw component-id                string
   +--ro used-power?                 uint32
   +--ro power-save-capable?         boolean
   +--rw power-save?                 boolean
   +--ro required-components*        -> ../../component/component-id
   +--ro dependent-components*       -> ../../component/component-id
```

draft-li-ivy-power

A New WG NMOP Formed to Discuss Operation Issues about Network YANG Model





New WG: Network Management Operations (NMOP)

Summary: Discuss the deployment of network management technologies (not limited to the IETF), focus on the operation management issues faced by operators, and document experience and best practices.

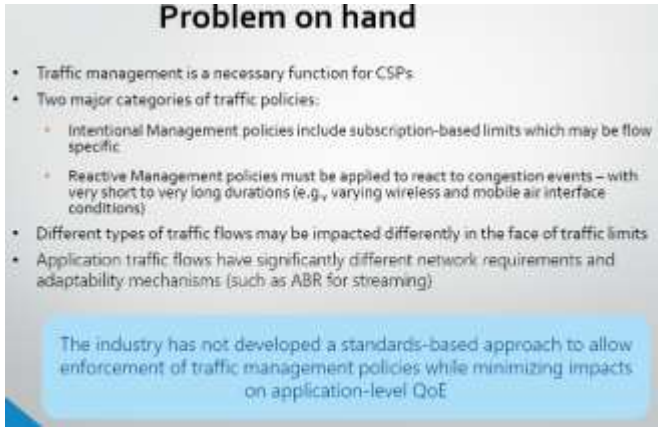
Background: The OPS AD organizes mainstream operators in and outside China to discuss network management and operational issues encountered during network YANG model deployment. Besides, initiated by Bell Canada Daniel and Deutsche Telekom Nils, discuss around the OpenConfig, IETF and vendor specific YANG model happened. Cisco shared the mapping from vendor native YANG to IETF/OC Yang, Cisco, Juniper, Huawei, Bell Canada, DT, Telefonica, and Orange participated in the discussion.

Result: OPS AD announced the initialization process of the new WG. The working group is currently being established.

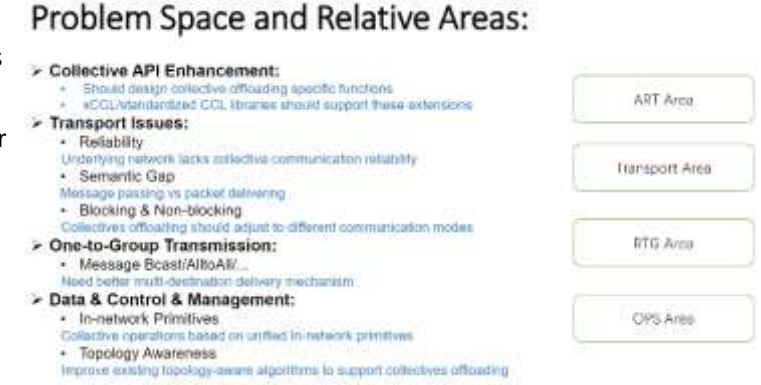
NET-APP Coordination – Metadata Carrying

- **Four side meetings are related with NET-APP Coordination, exploring Net2Host & Host2Net signaling for metadata carrying**
  - **Securing Ancillary Data for Communicating with Devices in the Network (SADCDN) (https://github.com/afrind/sadcdn/tree/main/materials/118)**
    - **Goal:** Consensus on SADCDN Use Cases
    - **Conclusions:** Non-WG Forming BoF @IETF119
    - **Participants:** Meta, AT&T, Google, Tiktok, Nokia, Ericsson, Huawei
    - **Views: An unified mechanism/protocol for NET-APP coordination is desired, and in order to securely carry such metadata, a secure tunnel/channel is required.**

The fundamental problem is *information disparity* between network devices, content endpoints, and end users.



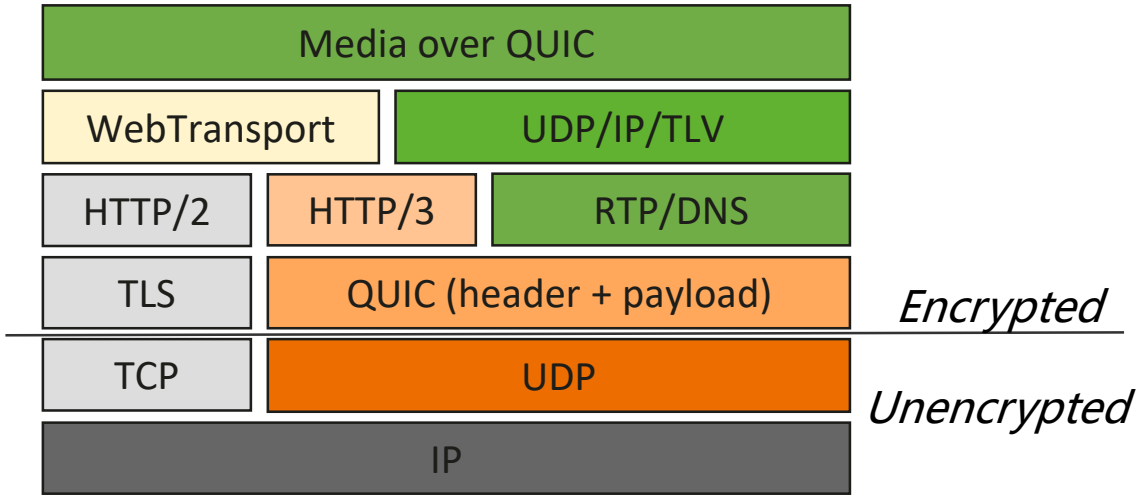
  - Transport challenges and Collaboration Requirements
    - Discussion on current transport challenges and the requirements for newtork&host collaboration (Net2Host and Host2Net signals)
  - Collective Communication Optimizations (CCO) (https://github.com/CCO-IETF/ietf118-side-meeting) ⟶
    - Discussion on cases, challenges, requirements and mechanisms to facilitate the collective communication optimizations
  - APN Virtual Team Meetup – Summary of the work and the future direction
    - An appropriately fine granularity is desired for traffic treatments within network, DSCP too coarse, neither per APP/User

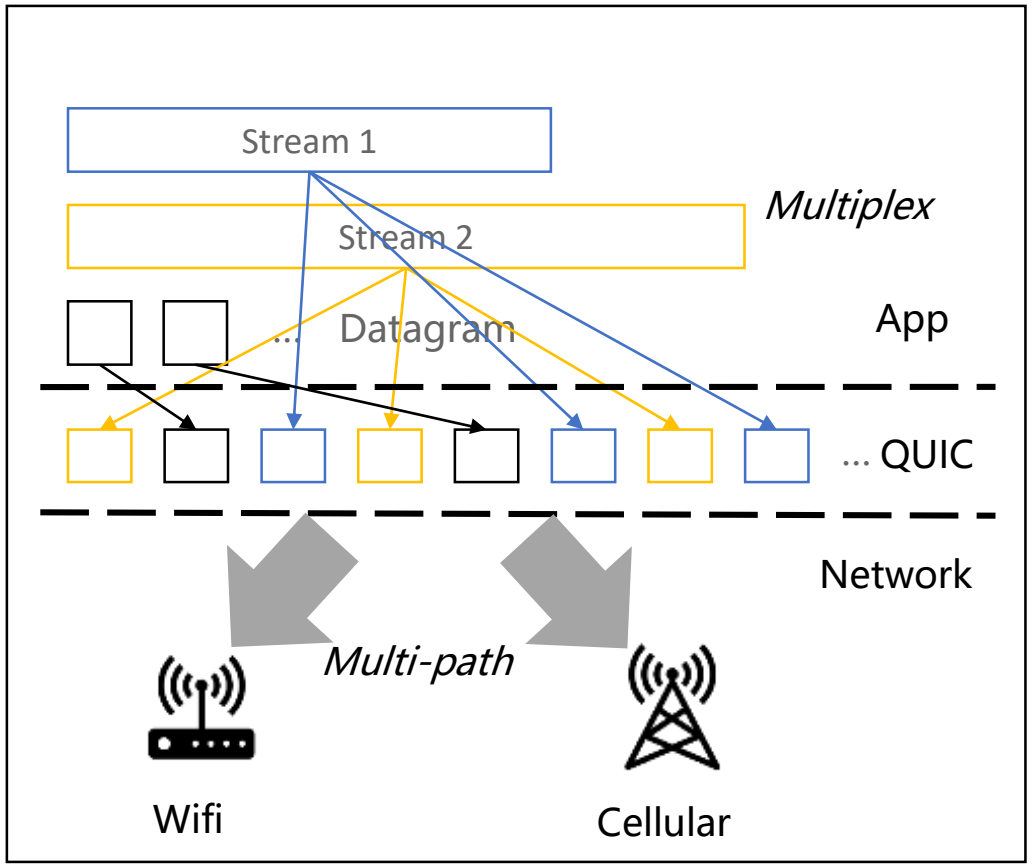


- Several active works are ongoing in IETF on this exact topic
  - IETF TSV Media metadata for wireless (new) – Transport
  - IETF ART MoQ carrying metadata (new) – APP/Transport
  - IETF/3GPP Masque - QUIC
  - IETF FAST – a ticket for service and firewall (restart) – IPv6 HBH

Everything over QUIC

- QUIC is unifying the transport layer = **Encrypted** TCP/UDP/Multi-path:
  - DNS, RTP, BGP, Media is running over QUIC
- MASQUE extends HTTP proxy/relay to tunnel any TLV:
  - RFC 9298: UDP/TLV over HTTP
  - RFC 9484: IP over HTTP(L3VPN)
  - draft-ietf-masque-connect-ethernet: Ethernet over HTTP
  - connect UDP listen: WebRTC over HTTP

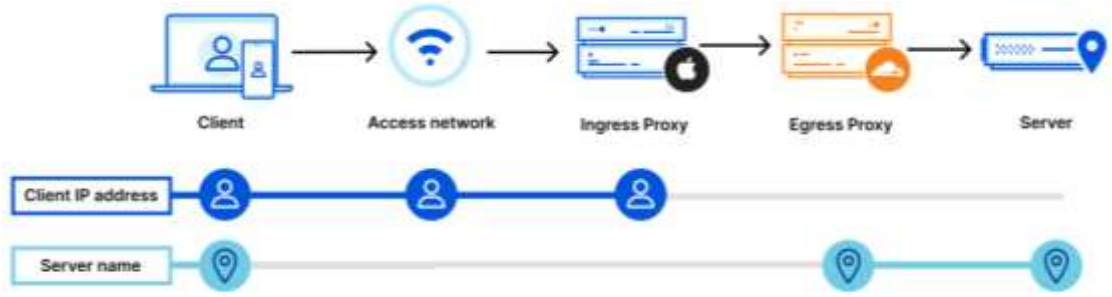




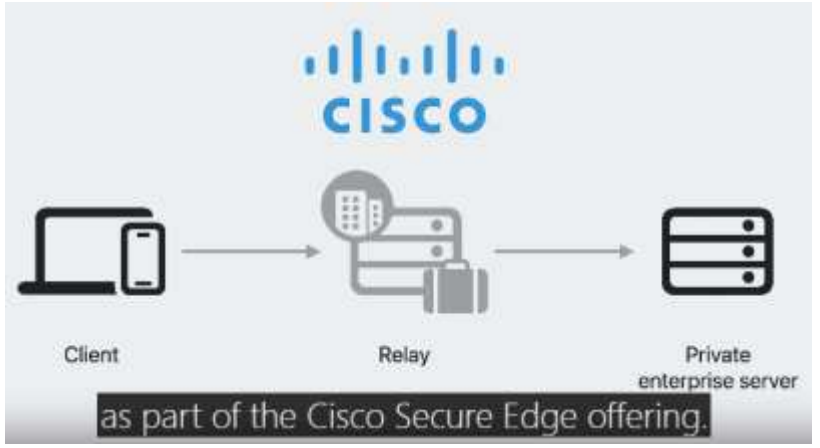
Google: David: This is reinventing turn; we previsouly reinvented socks... ~~"We're running the Internet over HTTP now but don't tell anyone"~~ This is essentially an *un*connected UDP socket.

New Internet Overlay Architecture based on Relay/Proxy

- Apple: iCloud Private Relay:
  - Ingress Proxy(Run by Apple) only knows Client IP
  - Egress Proxy(Run by CDN) only knows Server IP
- Google IP Protection in Chrome: Two Hop Proxy similar to Apple
- Cisco implements MASQUE Relay in SASE product: Claims to be lighter than VPN; Apple iOS 17 provide system level API support to connect to MASQUE Relay
- Apple/Google is the gateway to the internet. Operator can not see the application IP.



iCloud Private Relay By Apple

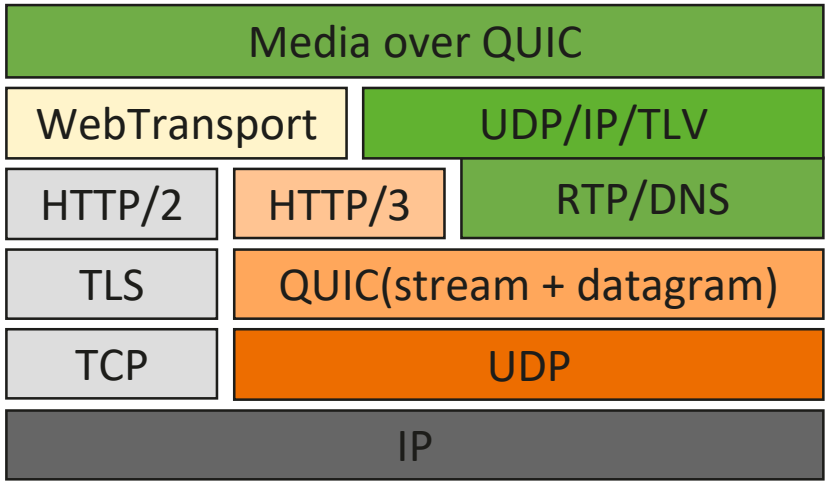


Apple + Cisco Relay

Transport Area(TSV) -> Web and Internet Transport(WIT)

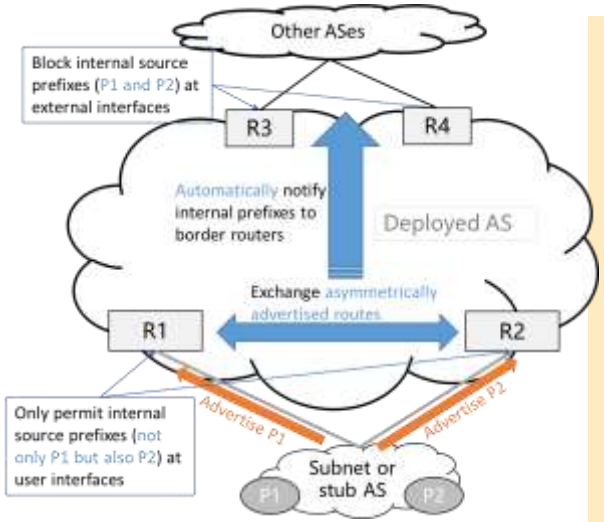
- 8 years ago, APP area and RAI area are merged into ART. Now IETF is restructuring TSV and ART area.
- TSV area ceases to exist, Web and Internet Transport (WIT) area is formed:
  - HTTP is tied closely to QUIC, HTTP/3 over QUIC is becoming the new (web) transport; the Web ecosystem is very strong.
  - QUIC related WG are put together
- OTT dominate the WIT. Ericsson participates in MASQUE and QUIC. Cisco participates in RTP and MoQ
- CCWG is formed to standardize massively adopted Congestion Control algorithm

Change	Web and Internet Transport (WIT)
ART -> WIT	AVTCORE, CDNI, CORE, HTTPAPI, HTTPBIS, MOQ, RTCWEB, WEBTRANS
TSV -> WIT	CCWG, MASQUE, NSFV4, QUIC, TAPS, TCPM, TSVAREA, TSVWG
TSV -> Others	ALTO, IPPM -> OPS; DTN -> INT
ART -> SEC	SCIM, TIGRESS



Routing Security: SAVNET WG focuses on architecture drafts; RPKI-ASPA drafts get stable and will enter WGLC soon

- **SAVNET:**
  - SAVNET WG primarily discussed architectures of Tsinghua&Huawei. Chairs: consider the adoption of intra-domain architecture draft first.
  - Multiple vendors and operators continuously pay attention to SAVNET.
    - (Huawei, Juniper, Cisco, ZTE, H3C, Futurewei, China Mobile, China Telecom, Akamai, WorkOnline, Liberty Global, etc.)
    - A couple of intra- or inter-domain SAV solutions have been proposed and presented.
  - Huawei proposed BGP SAVNET solution and presented it in the idr WG.



BGP SAVNET:
(1) Edges exchange asymmetric route prefixes to get complete prefix list.
(2) Edges advertise internal prefixes to ASBR which blocks the prefixes from outside.

- **BGP Routing Security:**
  - RPKI-ASPA drafts will enter WGLC. RTR v2.0 draft needs further discussion, and there will be a 2nd WGLC of RTR later than ASPA drafts.
  - The direction of BGP routing security keeps active:
    - [sidrops WG] A new RPKI Object called PrefixList for enhancing prefix filtering.
    - [sidrops WG] A new encoding to mitigate scalability and security problems of ROA.
    - [idr WG] FC-BGP for securing both control- and data-plane paths. Optimizes BGPsec.
    - [idr WG] A new signature-based mechanism for securing BGP community.
    - [idr WG] Extend BGP to advertise redirection paths not unknown by control plane.

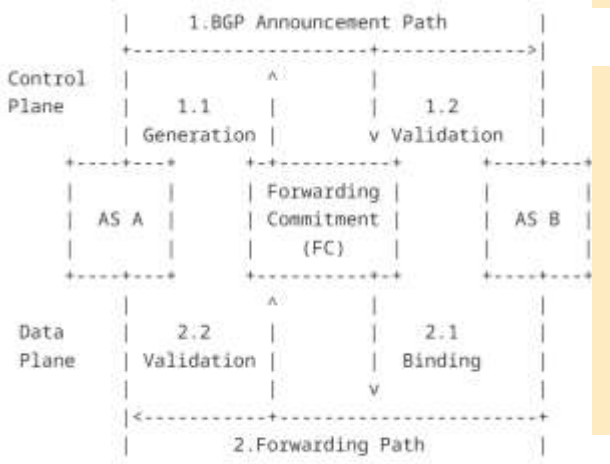


Figure 1: Overview of FC-BGP.

FC-BGP:
(1) Control plane optimizes BGPsec to secure AS_PATH.
(2) Data plane binds prefixes to valid interfaces to secure real forwarding paths.

The side meeting result of path verification new direction is beyond expectations, and the work group level new work is expected in the IETF

- **Background:**
  - **Path verification is a technology used to verify whether a real path of a data packet on a forwarding plane is consistent with a predetermined path specified by a control plane. It can be used to enhance the security of source address routing protocols, protect data from leaving a specified path or area, and filter spoofing traffic.**
  - This side meeting is a framework explanation, that is, how to achieve the above objectives step by step, whether the issue has real business requirements, and overall problem description. Instead of discussing a single point of technology.

- **Attendance:**
  - Representatives of many operators, equipment manufacturers, research centers, and enterprises attended the meeting and received a warm response.
  - TLF, China Mobile, and SCION reported the use cases, and Huawei analyzed the gaps.
  - **The routing domain AD** attends the meeting and indicates that the problem is clearly defined and real use cases exist. Support was expressed for further applications for mailing lists and BOFs.

- **Consensus conclusions reached at the meeting:**
  - Europe, Japan, Africa, and China have encountered routing compliance requirements (mainly the extension of data security protection), that is, how to ensure that the specific trusted attributes of a private line meet the requirements and how to ensure that data on a private line does not leave the private line or the local jurisdiction. This problem is a concern of multiple carriers.
  - Request a mailing list. It is easier to have technical discussions or BOFs.

One of the important trends: Security Becomes a Key Attribute of Network Quality + Remote Attestation Is Expected to Become a Basic Enablement Technology and Protocol for Trusted Networks

Insight: Traditional network SLA: packet loss, delay, jitter, and availability→ Added the cyber security SLA: Trustworthy devices-Remote attestation. Reliable routes: IGP and BGP distribute security status, and routing information such as RPKI and BGPSec verification. Trusted path - PoT, path verification, etc.

Security status of the IGP distribution device (distributed path computation at the routing layer)

- **Cisco: The trusted path document mentions that Layer 2 802.1x and flexalgo of the MACSec+IGP protocol are used as extensions to implement trusted path selection.**
- **Juniper: Newly Proposes IGP Extensions in the Routing Domain to Support Trusted Route Selection**
- **Summary: Compared with Juniper, Cisco's standard solution is based on FlexAlgo and is more mature. Juniper is very early.**

Trust Enhancement Network and Trust Level Definition (Centralized Path Computation at the Application Layer)

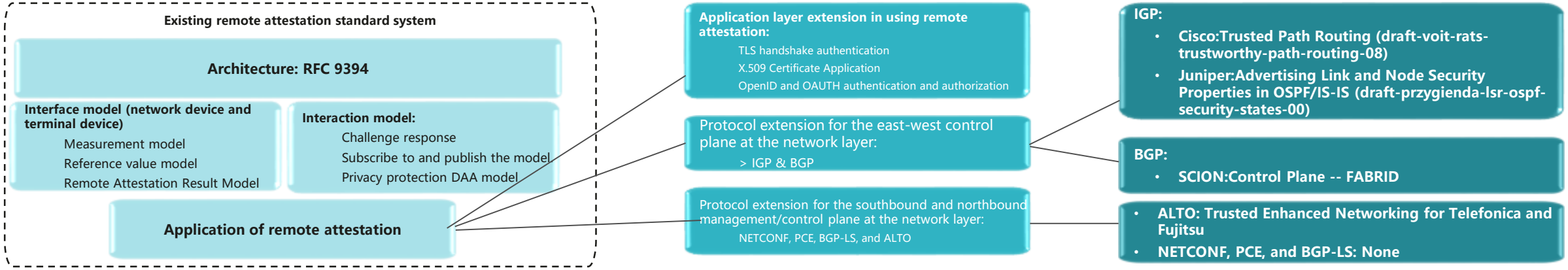
- **Fujitsu: Put forward the Trust Enhanced Networking (TEN) and Quality of Trust (QoT) approach: Geolocation, Trustworthiness metrics, Property Map**
- **Telefonica: The ALTO team proposed similar ideas.**

SCION: Next-Generation Cross-Domain Trusted Network Architecture (at the overlay layer)

- Switzerland Inter-domain Trusted Network Architecture Proposed by Academic and Industry
- **The essence is innovation in the limited domain. Based on the existing Internet IGP and BGP protocols, the reliable overlay network is built.**
- Core technology: control plane PKI + control plane routing + data plane forwarding
- **Emphasize cross-domain path authorization management and verifiable, as well as data border management (Geofencing)**

Insight: The standard system (interaction model, data model, and bearer protocol) of remote attestation is becoming more and more complete and becomes a competitive basic enablement protocol for building trusted networks.

Extended thinking: How to integrate with existing protocols to quickly synchronize device security status, support visible and manageable path security, and form an overall solution that features reliable results, practical functions, reasonable design, and efficient operation.



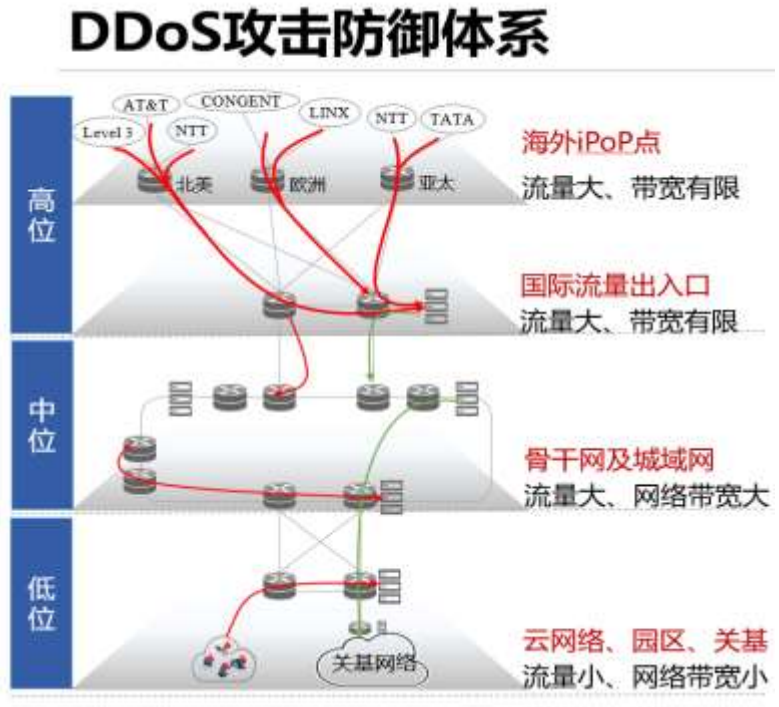
Key Trend Insight 2: New Features of DDoS Attacks in China Raise New Challenges and Requirements for Existing Standards

IETF DDoS mitigation and scheduling signaling standard DOTS

RFC 8903 (was draft-ietf-dots-use-cases) Use Cases for DDoS Open Threat Signaling	13 pages	2021-05
RFC 8973 (was draft-ietf-dots-server-discovery) DDoS Open Threat Signaling (DOTS) Agent Discovery	22 pages	2021-01
RFC 8811 (was draft-ietf-dots-architecture) DDoS Open Threat Signaling (DOTS) Architecture	29 pages	2020-08
RFC 8782 (was draft-ietf-dots-signal-channel) Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification	100 pages Errata	2020-05
RFC 8783 (was draft-ietf-dots-data-channel) Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification	66 pages Errata	2020-05
RFC 8612 (was draft-ietf-dots-requirements) DDoS Open Threat Signaling (DOTS) Requirements	22 pages	2019-05

- **Huawei, Cisco, and Arbor have jointly promoted the formulation of DOTS standards in the IETF for DDoS attack mitigation scheduling. Attackees use DOTS to request attack mitigation from the DDoS cleaning center.**
- **DOTS standards will be released around 2020/21 and has been supported by some vendors, such as Arbor and Cisco.**

New requirements for collaborative anti-DDoS in China



- **Zhongguancun Lab took the lead in the collaborative anti-DDoS project, with the participation of the three tier-1 carriers, our company, and other vendors.**
- Aiming at the trend of large-scale DDoS attacks,new attack methods and intelligence,this paper proposes a collaborative defense system for DDoS attacks based on low,mid and high-level three-layer networks.
- **They aim to extend IETF DOTS standard as interactive protocol, and put forward new requirements such as attack information and intelligence transmission.**

Summarize **Zhongguancun Laboratories cooperates with three tier-1 carriers in collaborative defense against DDoS attacks, posing new challenges and requirements to existing standards.**

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and organization for a fully connected, intelligent world.

HUAWEI