IETF 117 HotRFC

Brought to you by
Spencer Dawkins and **Liz Flynn**

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

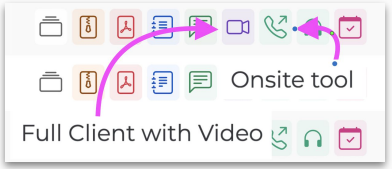
- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

This session is being recorded

IETF 117 Meeting Tips

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*



Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

Resources for IETF 117 San Francisco

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

The Ground Rules

- **HotRFC is how you make a Request For Conversation**
  - It's a good way to find IETF people to talk to, for various reasons
- Each person gets four minutes from "Go" to "Please Applaud"
  - At four minutes, we start applauding (see next slide)
  - When you hear applause, please hand the microphone over 😇
- We don't do questions here -- each person provides follow-up info
  - (in-person attendees can follow presenters to the bar, of course)
- So you can follow along, we're using the datatracker for all slides
  - Let the conversations begin!

Please Applaud!!! (and the crowd goes wild)

IETF117 HotRFC

Domain-based Routing and Forwarding for End-to-End QoS

Haoyu Song

Futurewei Technologies, USA

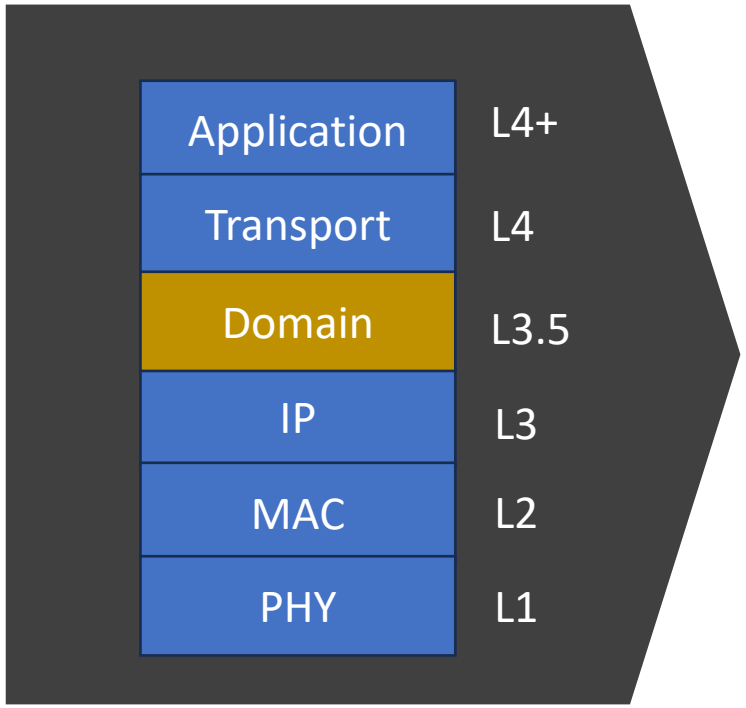


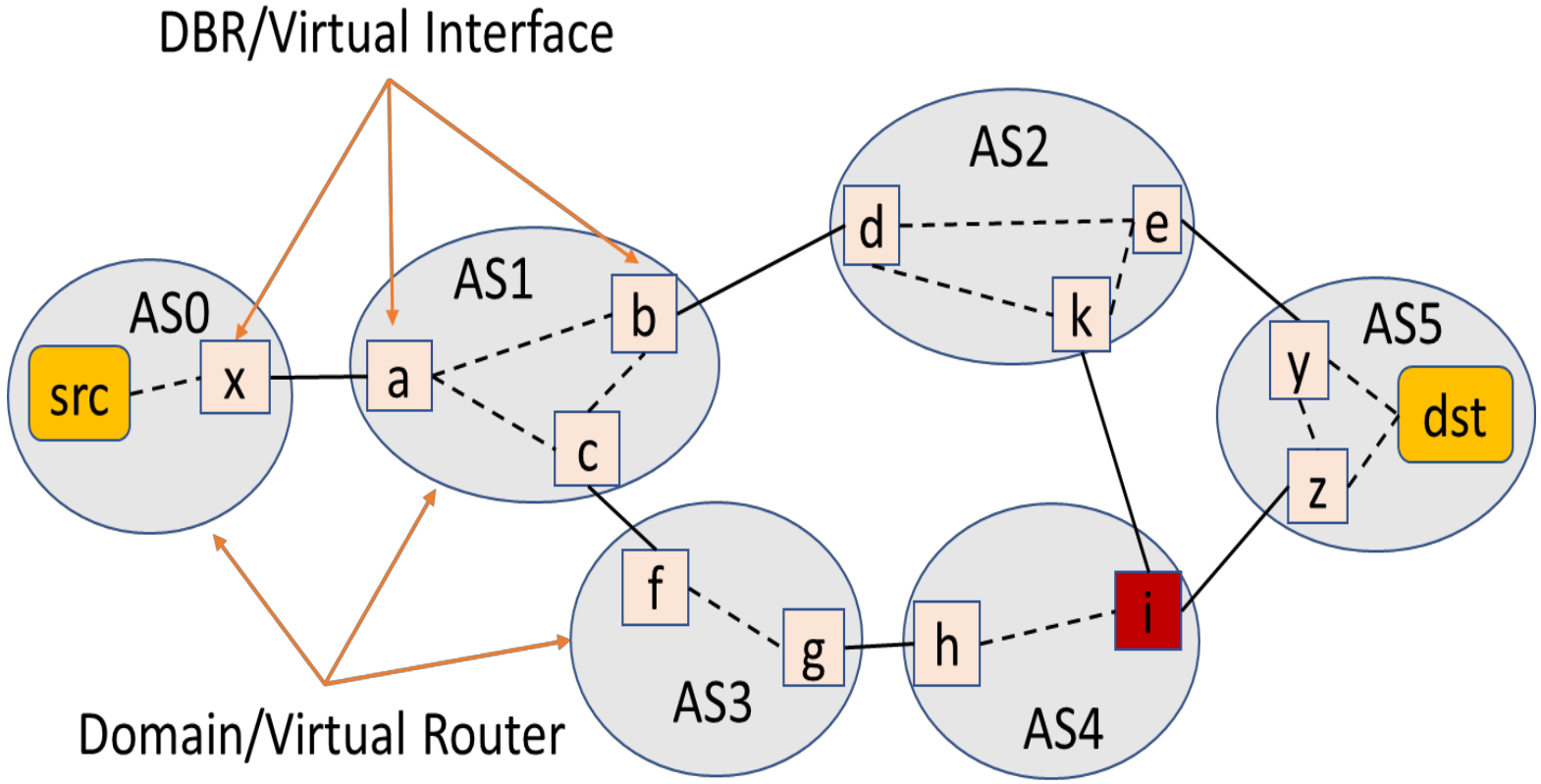

Motivation

5G/6G, Metaverse

- Global reach, internet scale
- QoS sensitive interactive services
- Involve multiple service providers & types of networks
- Time to solve the long-lasting problem!

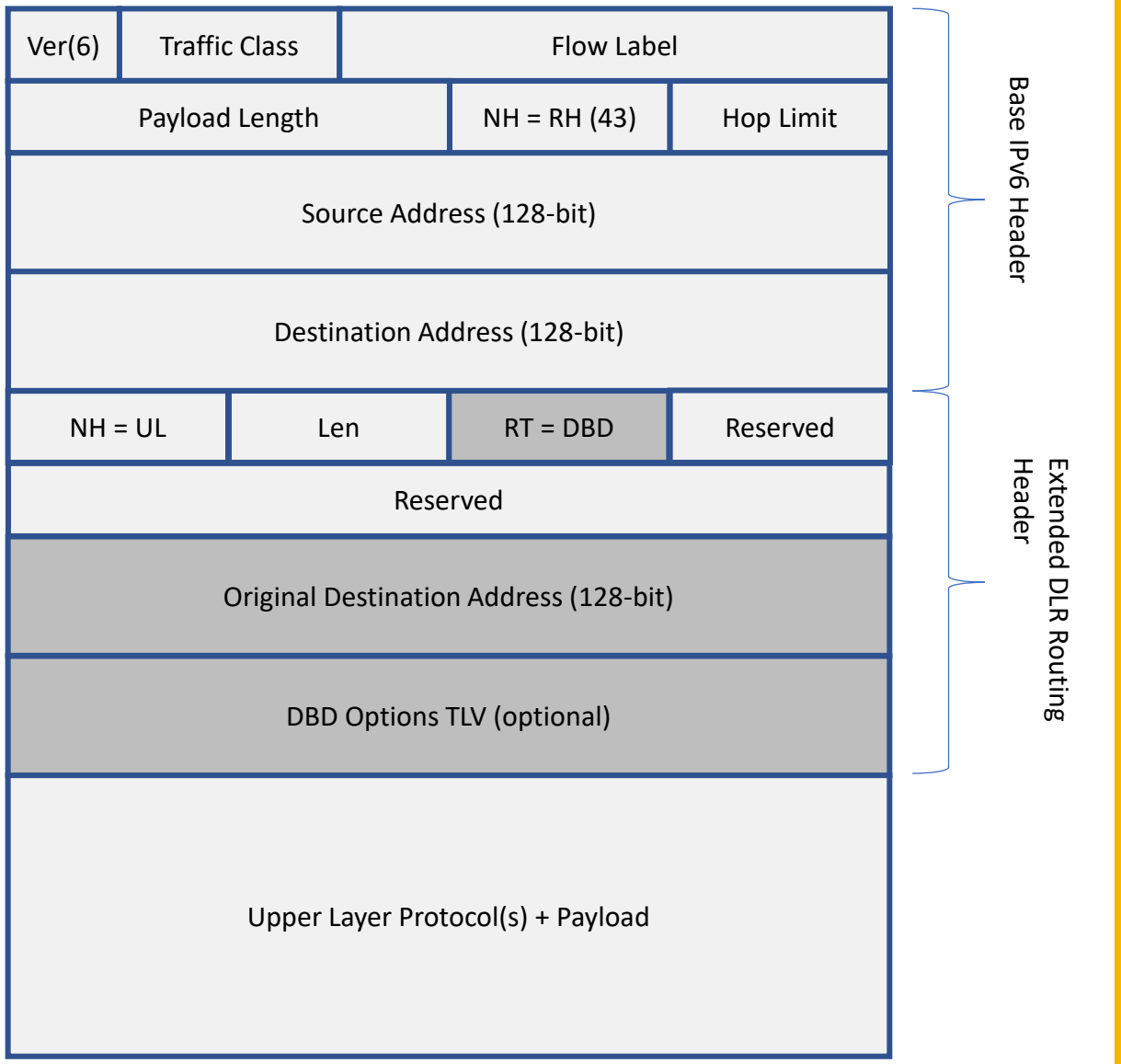
Make Domain Explicit L3.5 Entity



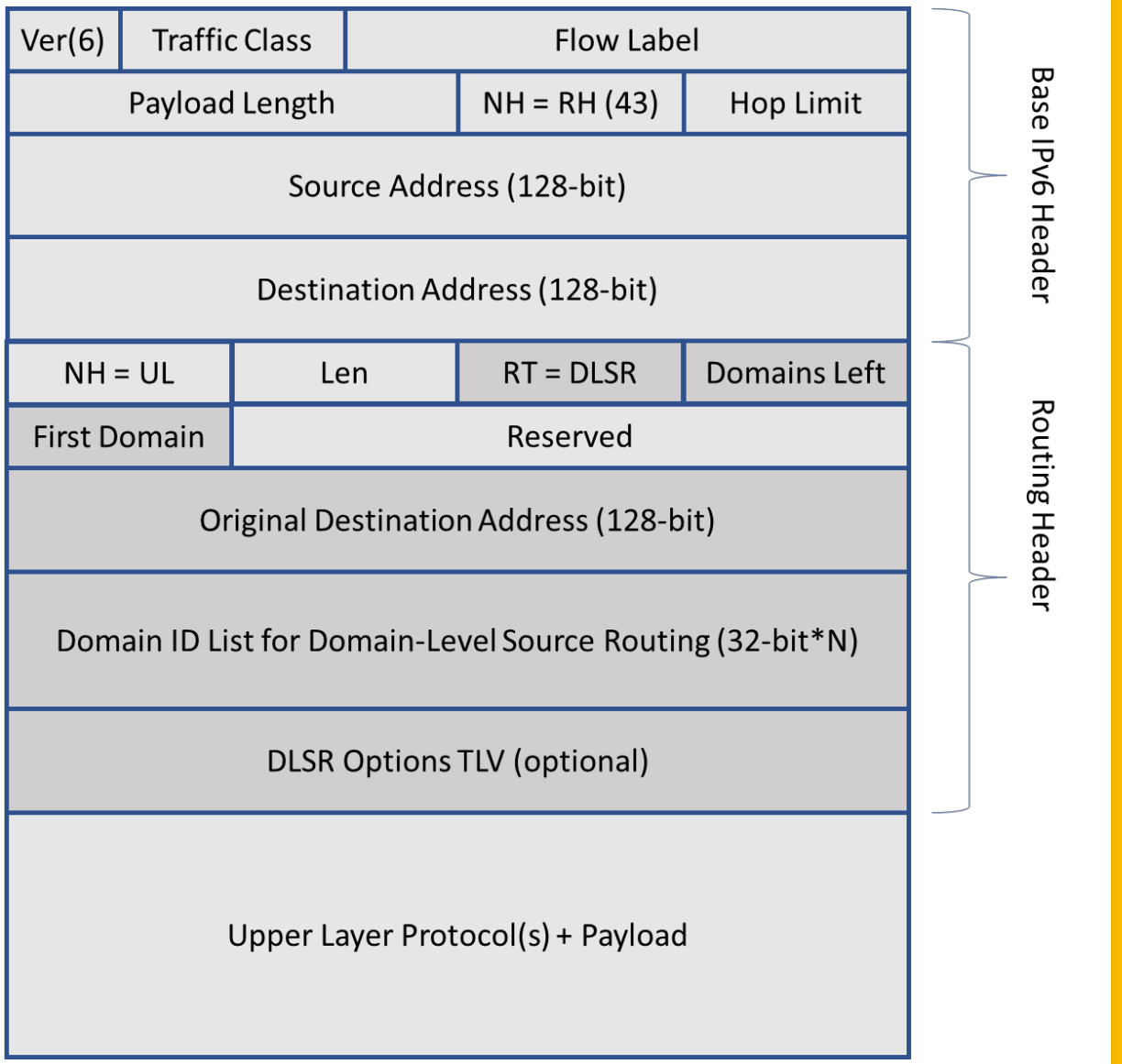


Each domain is a virtual router

Domain-Based Routing (DBR)



Domain Level Source Routing (DLSR)



Benefits of Domain-based Routing and Forwarding

- Forster a business model to enable Internet-scale QoS with the right level of manageable entity
  - Limited number of "hops“
  - Vested service provider interests
  - Authority of control
- Hide the intra-domain routing/forwarding details
  - Clearly decouple the intra-domain and inter-domain
  - Intra-domain routing and traffic engineering as secret sauce
- Same OAM standards/tools can be applied at the domain level
  - Each domain is virtualized as a node
  - Auditable SLA

Thank You!

Feedback & Collaboration Welcome!

Reference:

1. "Towards End-to-End Quality-of-Service by Domain-Level Routing and Forwarding", arXiv:2207.02326 [cs.NI], July 2022

2. "Enable Cross-domain QoS for Internet-Scale Metaverse", IEEE MetaCom, June 2023

Please Applaud!!! (and the crowd goes wild)

Trusted Sensors
For a Greener World

Pascal.Urien@Telecom-Paris.fr

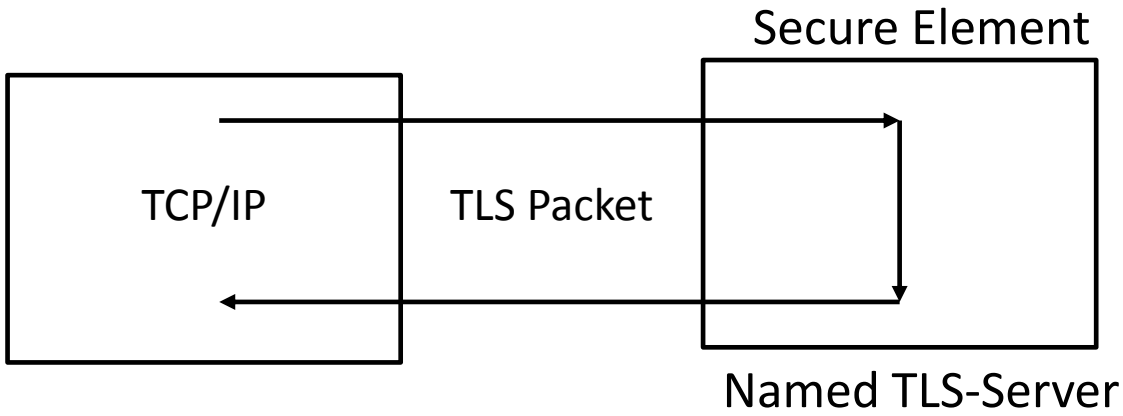
Trusted Sensors

- Sensors and network of sensors are widely used to monitor environmental safety. It is a major topic for the scientific, public and political communities.
- Some examples
  - https://www.pollutrack.net/
  - https://teleray.irsn.fr/
  - https://epa.gov
- Trusted sensors
  - Sensors with tamper resistant resources
  - Based on open technologies
- Benefits
  - Trust for collected measures

Architecture

- Sensors could be organized around secure elements including named TLS servers providing mutual authentication and secure communications.
  - Trust in payments (EMV bank card) or identity (electronic passport) is achieved thanks to secure elements.
- Internal commands for administration.
- Exported commands for Actuators/Sensors interactions.
- On-demand cryptographic resources authorization.

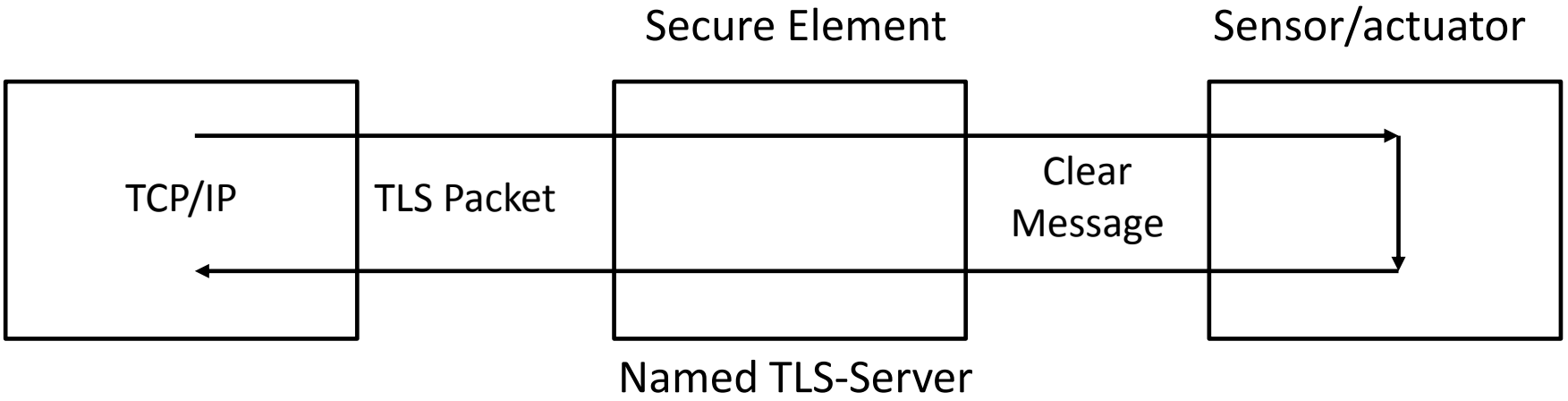
Internal Commands



https://datatracker.ietf.org/doc/draft-urien-tls-se/

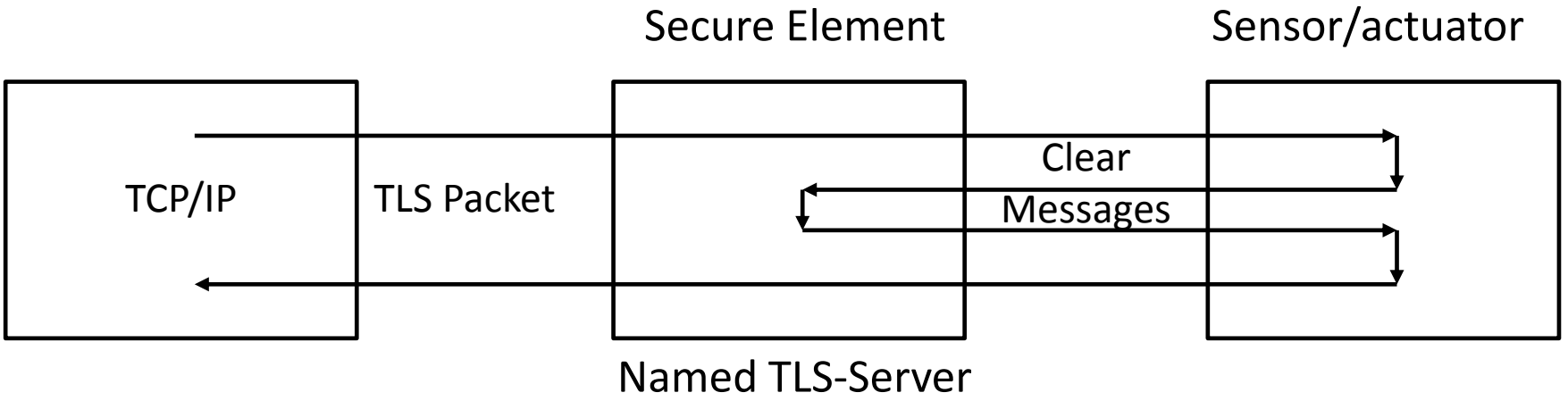
https://datatracker.ietf.org/doc/draft-urien-coinrg-iose/

Exported Commands

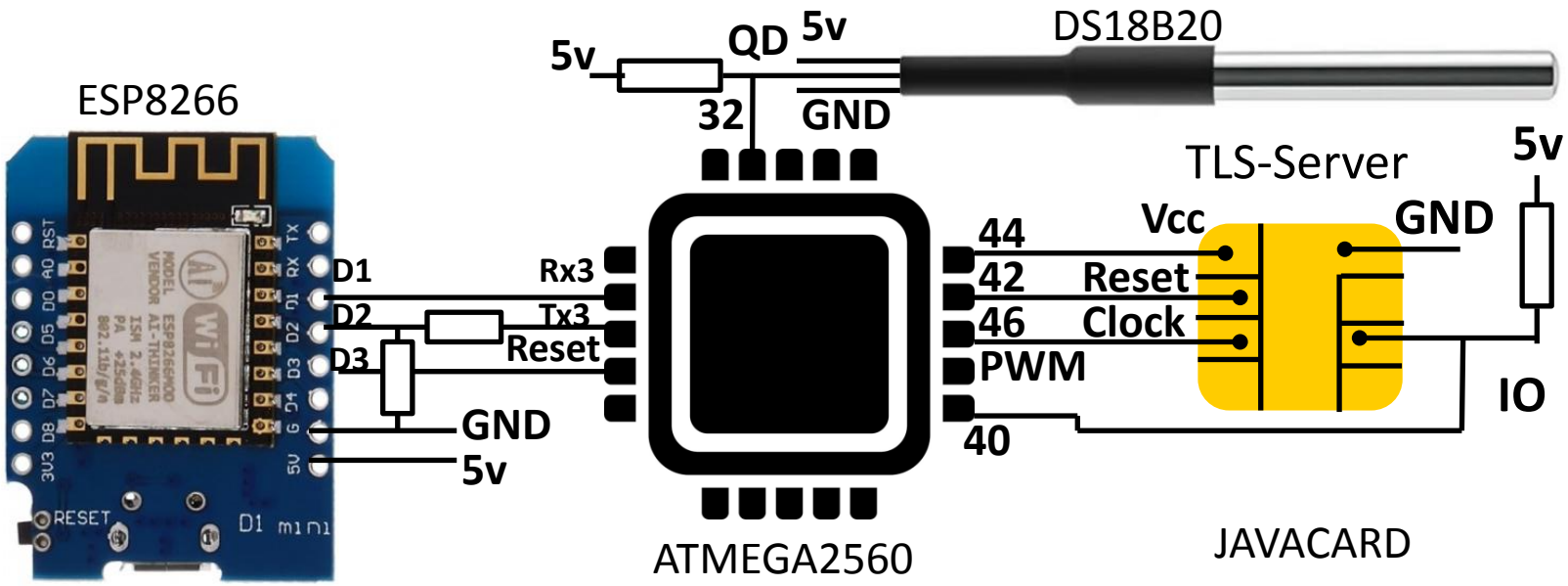


https://datatracker.ietf.org/doc/draft-urien-core-tls-se-io/

On-Demand Cryptographic Resources Authorization



Illustration



https://www.youtube.com/watch?v=74aoCvrtZ0c

Next Steps

- Defining framework for trusted sensors
- Defining network interface
- Design guideline for trusted sensors with open hardware software

Please Applaud!!! (and the crowd goes wild)

On Path Validation and a Possible Solution

draft-liu-on-network-path-validation-00

HotRFC Lightening Talk @ IETF 117, July 2023

Chunchi Liu (Huawei)

Why do we care about path validation?

Routing Security Attacks

- **Routing Hijack**
- **Route Injection**
- **Route Leak**
- **Denial of Service**

Foster

Mitigate

Secure route propagation and authentication in the control plane

- **BGPSec**
- **RPKI**
- **…**
- **Is it enough?**

Cannot guarantee the planned path is *actually* used

Provide transit proof to complement

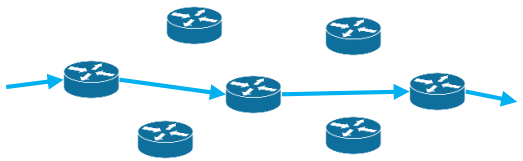
Enforcing and verifying the correct transit of traffic in the data plane

- **Path Validation**
- **draft-ietf-sfc-proof-of-transit**
- **…?**

What is Path Validation?

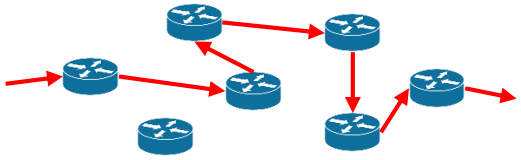
- Path validation is a mechanism that "**ensures**" data packets strictly traverse the chosen network path.

The desired path



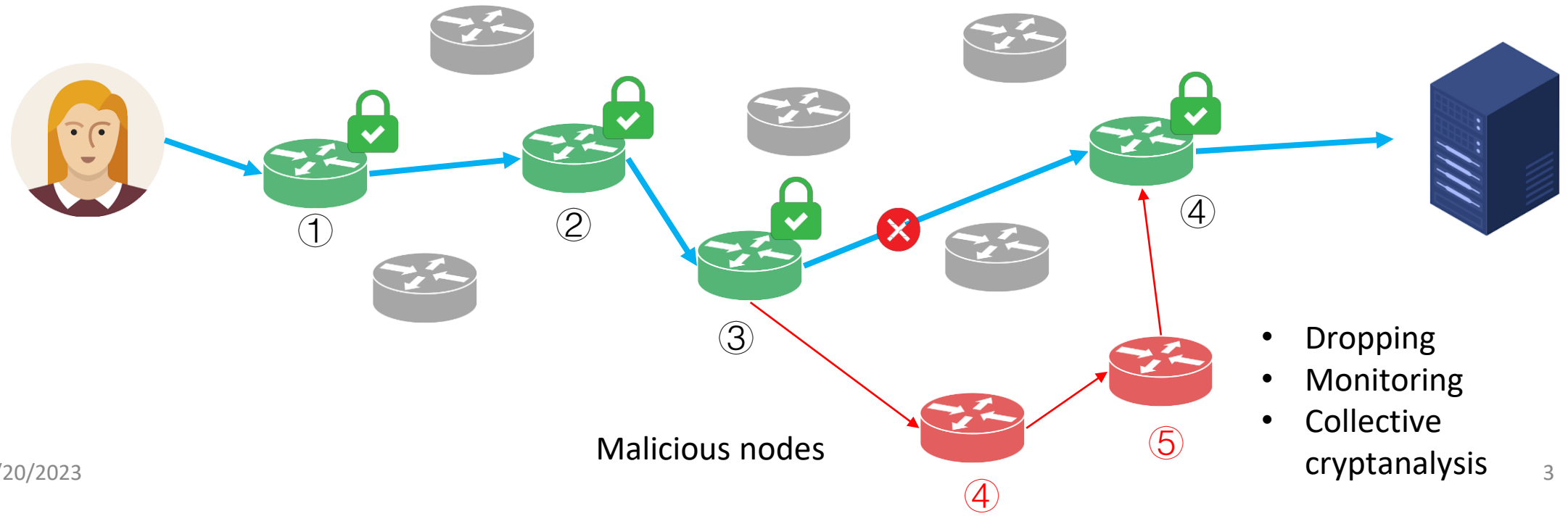
≠

The actual path



In Internet routing, the *actual* path the traffic took may **not** be the path we *planned*

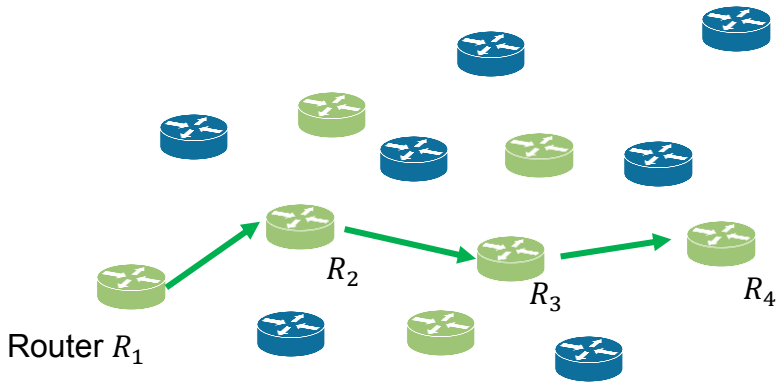
- Alice is having a **confidential** business video meeting or VOIP call.
- She doesn't want any data of this connection be detoured and monitored.



A Graphical Overview of the VC-based Path Validation Solution

✓ Security

- **Position-binding property**: Transit proof P_i successfully passes verification *iff* it was created by the **right node** n_i at the **right position** i **as previously committed**



✓ Advantages

- **Efficient:** Proof creation and verification takes **O(1) time**
- **Succinct:** Transit proof and commitment is **O(1) size**
- **Batch-proof** friendly (same efficiency)

Stage 1: Compute Reference Value

Network Controller $< R_1\ R_2\ R_3\ R_4 >$ → Output 1 **Commitment** C

- **Controller** selects a path
- Computes a **commitment**

Stage 2: Generate Transit Proof

$< R_1\ R_2\ R_3\ R_4 >$ → Output 2 **Transit Proof** P_i

- **Router** R_i forwards data
- Computes his **transit proof** P_i

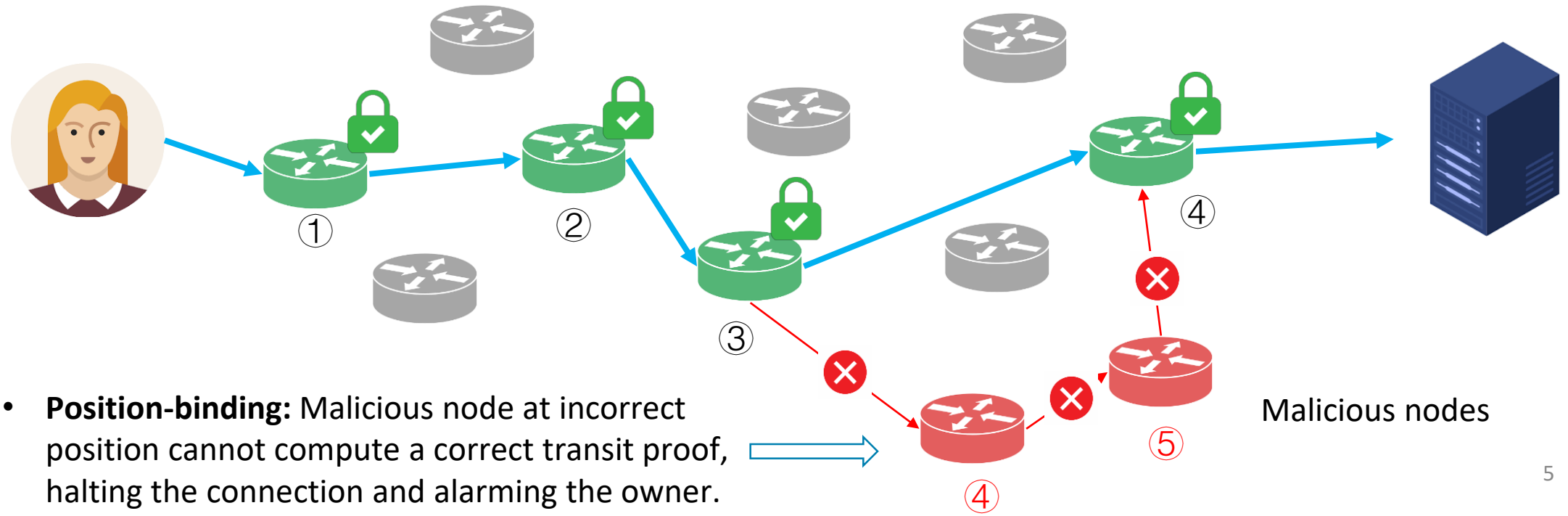
Stage 3: Verification

$Verify(C, P_i) =^? 1$

- **Observer** verifies P_i against C to check if it was the correct router in correct position.

Anti-detour security-sensitive communication

- Alice is having a **confidential** business video meeting or VOIP call.
- She doesn't want any data of this connection be detoured and monitored.



- **Position-binding:** Malicious node at incorrect position cannot compute a correct transit proof, halting the connection and alarming the owner.

Malicious nodes

Looking for interested collaborators to:

1. **Work on the draft**
2. **Joint research for a lot of extending work**
3. **Conduct joint PoC implementation and deployment test**

On OPSEC

Thursday 7.28
15:30 - 16:30

Please don't hesitate to catch me in the venue :)

draft-liu-on-network-path-validation

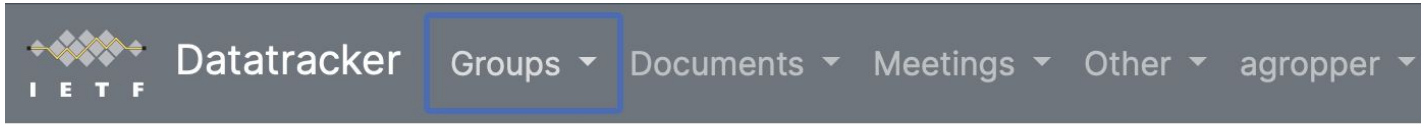
Chunchi Liu, liuchunchi@huawei.com

liuchunchi.com

Please Applaud!!! (and the crowd goes wild)

Essential Protocols to Avoid Forced (Platform) Association

Adrian Gropper
HIE of One Project
for IETF 117 HotRFC
July 2023



draft-irtf-hrpc-association-13

Human Rights Protocol Considerations Research Group — N. ten Oever
Internet-Draft — University of Amsterdam
Intended status: Informational — S. Couture
Expires: 13 October 2023 — Université de Montréal
M. Knodel
Center for Democracy & Technology
11 April 2023

Internet Protocols and the Human Rights to Freedom of Association and Assembly

draft-irtf-hrpc-association-13

Abstract

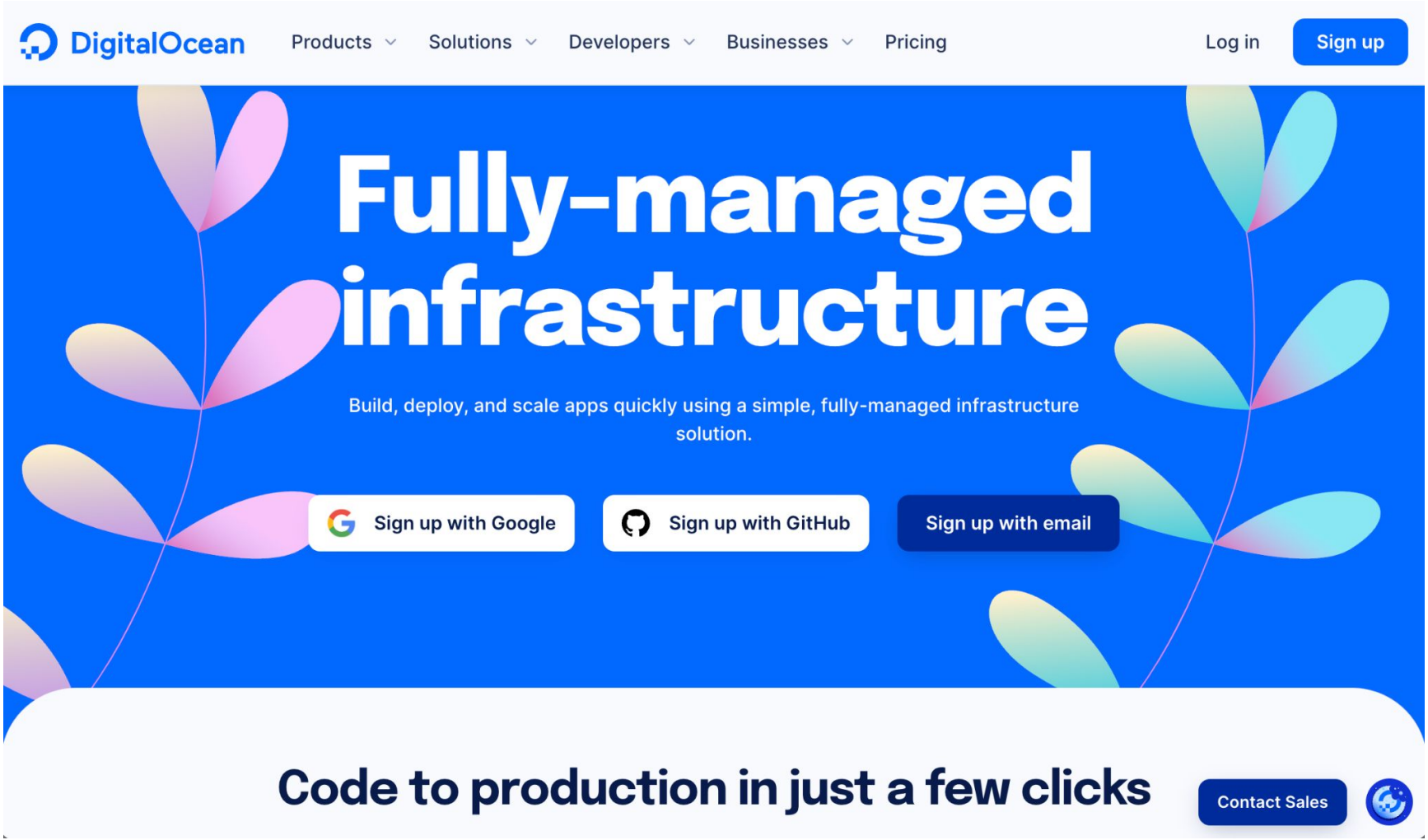
This document explores whether the relationship between the Internet architecture and the ability of people to exercise their rights to peaceful assembly and association online. It does so by asking the

Abstract

This document explores whether the relationship between the Internet architecture and the ability of people to exercise their rights to peaceful assembly and association online. It does so by asking the question: what are the protocol development considerations for freedom of assembly and association? The Internet increasingly mediates our lives, our relationships, and our ability to exercise our human rights. As a global assemblage, the Internet provides a public space, yet it is predominantly built on private infrastructure. Since Internet protocols and architecture play a central role in the management, development, and use of the Internet, we analyze the relation between protocols, architecture, and the rights to assemble and associate to mitigate infringements on those rights. **This document concludes that the way in which infrastructure is designed and implemented impacts people's ability to exercise their freedom of assembly and association.** It is therefore recommended that the potential impacts of Internet technologies should be assessed, reflecting recommendations of various UN bodies and international norms. Finally, the document considers both the limitations on changing association and impact of "forced association" in the context of online platforms.

Essential Protocols to Avoid Forced (Platform) Association

- **Choice of support community** based on default policies
- **Service provider authorization standard:** IETF GNAP
- **App platform** because self-hosting your authorization server does not scale
- **User Experience Integration:** Beckn protocol and related initiatives in India


DigitalOcean
Products
Solutions
Developers
Businesses
Pricing
Log in
Sign up
Fully-managed infrastructure
Build, deploy, and scale apps quickly using a simple, fully-managed infrastructure solution.
Sign up with Google
Sign up with GitHub
Sign up with email
Code to production in just a few clicks
Contact Sales

Datatracker Groups Documents Meetings Other agropper

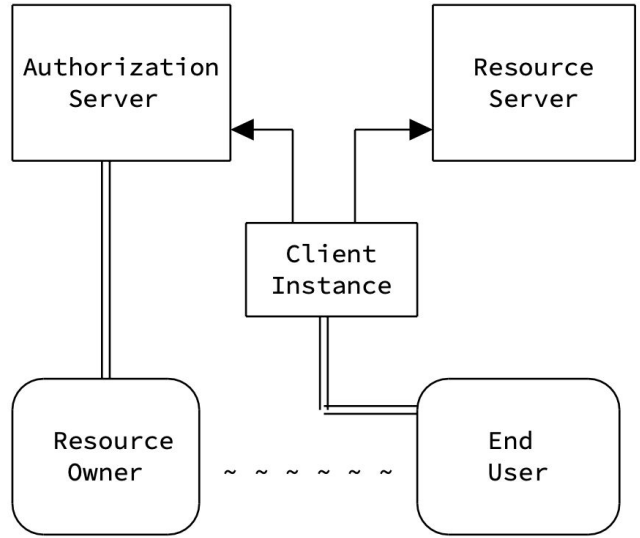
Grant Negotiation and Authorization Protocol (gnap)

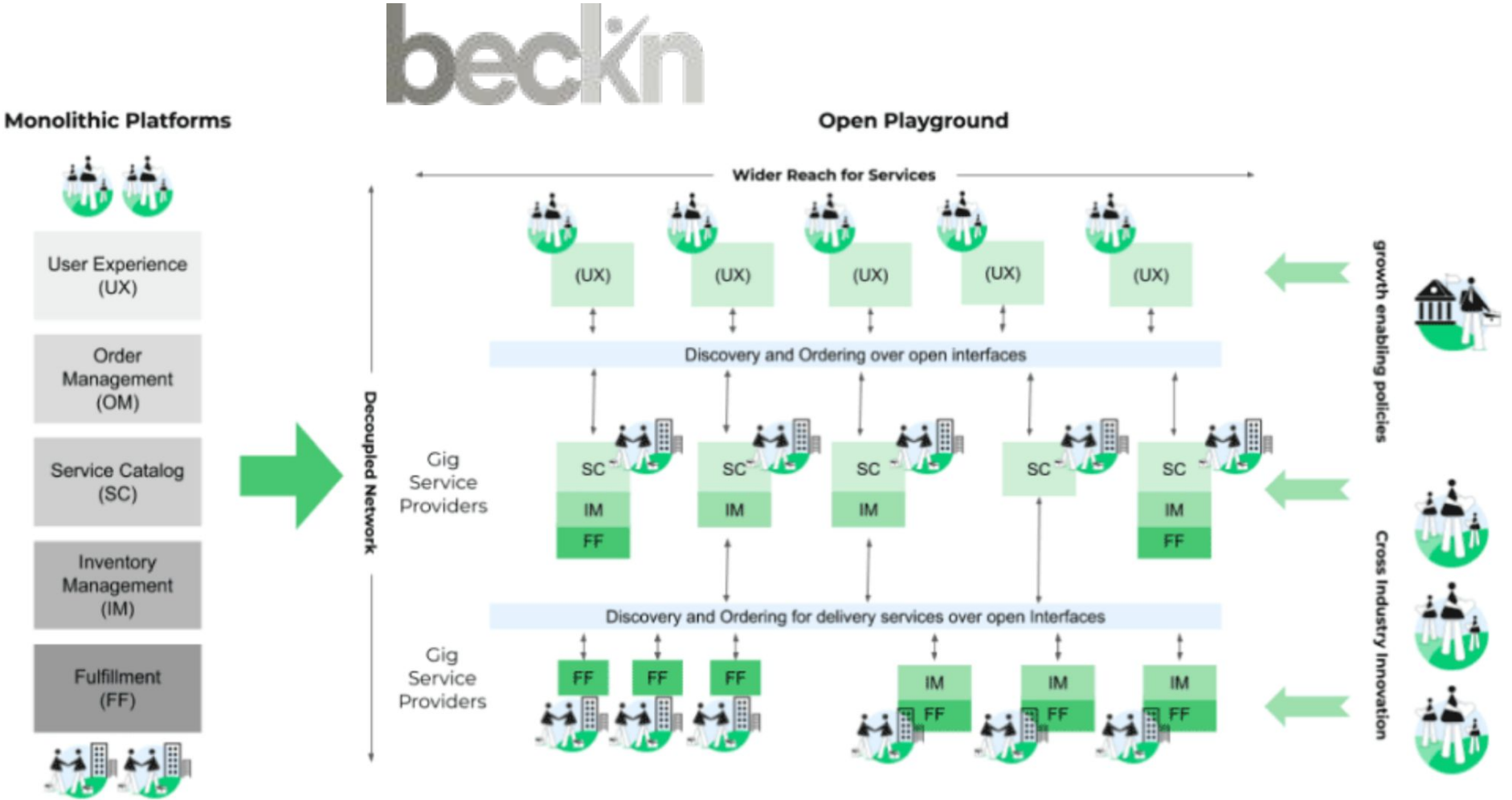
About | Documents | Meetings | History | Photos | Email expansions

WG	**Name**	**Grant Negotiation and Authorizati**
	Acronym	gnap
	Area	Security Area (sec)
	State	Active
	Charter	charter-ietf-gnap-01 Approved
	Document dependencies	Show
	Additional resources	GitHub Organization Zulip stream
Personnel	**Chairs**	Leif Johansson, Yaron Sheffer
	Area Director	Roman Danyliw
Mailing list	**Address**	txauth@ietf.org
	To subscribe	https://www.ietf.org/mailman/listin
	Archive	https://mailarchive.ietf.org/arch/br
Chat	**Room address**	https://zulip.ietf.org/#narrow/strea

Charter for Working Group

This group is chartered to develop a fine-grained delegation protocol for authorization, API access, user identifiers, and identity assertions. The





https://becknprotocol.io/imagining-with-beckn/

Next Steps?

- Contact me agropper@healthurl.com
- Start a Signal Group
- Find a home in IETF

- Example: Standard Patient-Controlled Health Record
  - A focus on mental health and substance use recovery support
- Example implementation https://github.com/HIEofOne
- Principal Developer https://github.com/shihjay2

Please Applaud!!! (and the crowd goes wild)

QUIC in Space

Marc Blanchet

marc.blanchet@viagenie.ca

IETF-117 San Francisco, July 2023

Use Case

- Going back to Moon
  - at a fast pace: hundreds of missions planned
  - Deployment of WIFI and 5G on the planetary body
  - Moon is seconds away of latency
- Going to Mars and else
  - Deployment of WIFI and 5G on the planetary body
  - Mars is minutes (~4-20) away of latency
- Spacecrafts are essentially mobile networks
- Key characteristics: delay, (un-)planned disruptions, …
- Can we use IP between Earth and Space? To which extent?
  - Alternative is to use Bundle Protocol (RFC9171). See dtn working group.
- Multiple layers: IP, Transport, Application transport(aka HTTP), Application.

Transport: QUIC

- QUIC has the right design to possibly work in this use case: UDP, tolerant to change of IP address/port, streams, HTTP3, TLS, …
- TODO:
  - Verify if QUIC can work
  - Implementations (not exhaustive list):
    - Quiche (Cloudflare, Rust), Quiche (Google, C++), Neqo (Mozilla, Rust), Picoquic(Huitema, C), Msquic(Microsoft, C, .NET)

Done So Far

- Testbed of Linux VMs, http3 client and server
- Using Linux Netem for introducing delays
- Using Picoquic (Christian Huitema)
- Testbed with various delays and changing various QUIC stack parameters:
  - Initial RTT, Retransmit timeout, Idle timeout

Results so far

- Christian wrote a test for long delays (20 min.) using its simulated time warp machine (instant results!). it worked (with some mods)
  - See blog
- With no modification to QUIC stack and introducing delays: a storm of retransmissions, takes a long time to converge. So does not work as is.
- Changes to parameters in code/cmdline
  - Setting initial_rtt close equal to 2 x delay introduced in netem. Setting up very large idle timeout (because other parameters are computed based on it). Setting high retransmission timeout.
- Tested and « worked »: 10s, 30s, 1m, 2m, 2.5m, 274s.
  - Flow works, not optimized, to be analyzed
  - Netem max possible delay is 274s… : so need to modify setup. Dummynet on Freebsd max: 10s.
- Found issue if some intermediary (known or unknown) nodes are doing NAT or « transparent » firewalling: UDP timeout of 30s…. (Cloud VMs…)

Help!

- Join to enable IP networks in space!
  - Setup a testbed
  - Modify implementations to make it work. Draw conclusions of what needs to be done.
  - Maybe some internet-draft if extensions or modifications to QUIC are necessary and found.
    - Already wrote one (draft-blanchet-quic-peer-hints) for giving hints to QUIC stack for some destinations.
  - Contact me: marc.blanchet@viagenie.ca
  - Join the mailing list to discuss (https://groups.google.com/g/quic-long-delays, quic-long-delays@googlegroups.com)

Please Applaud!!! (and the crowd goes wild)

Gap between IPv6 User Rate & Traffic Rate

HotRFC Talk, IETF 117

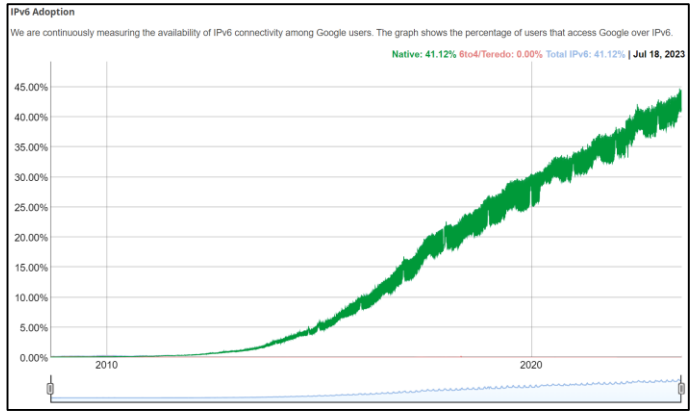
XiPeng Xiao, Huawei Germany & v6ops co-chair
xipengxiao@huawei.com

Problem: Real IPv6 Traffic Rate << IPv6 User Rate Implies

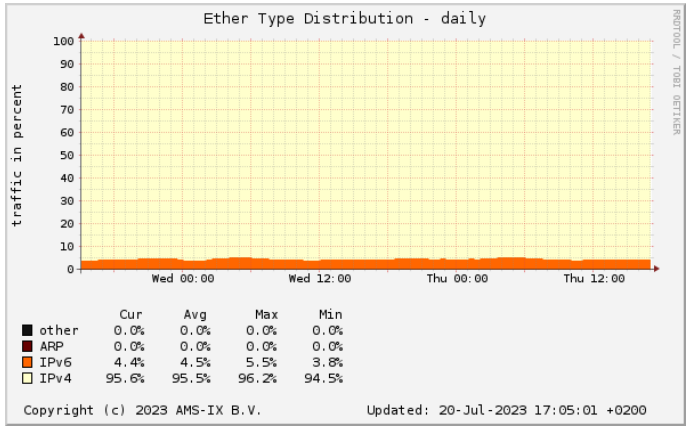
- IPv6 adoption measured by IPv6 user rate looks good
- IPv6 user rate not best KPI, IPv6 traffic rate better
- Implied IPv6 traffic% = IPv6 user% * IPv6 content% * IPv6 connectivity%
- = 41% * 67% * 100% = 27%
- Real IPv6 traffic stats difficult to get, anecdotal data far below 27%

	Traffic %		Date	Source
AMS-IX	5%		2023 07	https://stats.ams-ix.net/sflow/ether_type.html
Akamai	16.4%	41	2022 06	https://www.akamai.com/blog/trends/10-years-since-world-ipv6-launch
		250	2022 05	https://www.linkedin.com/pulse/oops-we-did-again-akamai-technologies/
Facebook	15.0%		2019 05	https://lemp.io/the-growth-of-ipv6-traffic-on-facebook/

IPv6 user 41% - promising



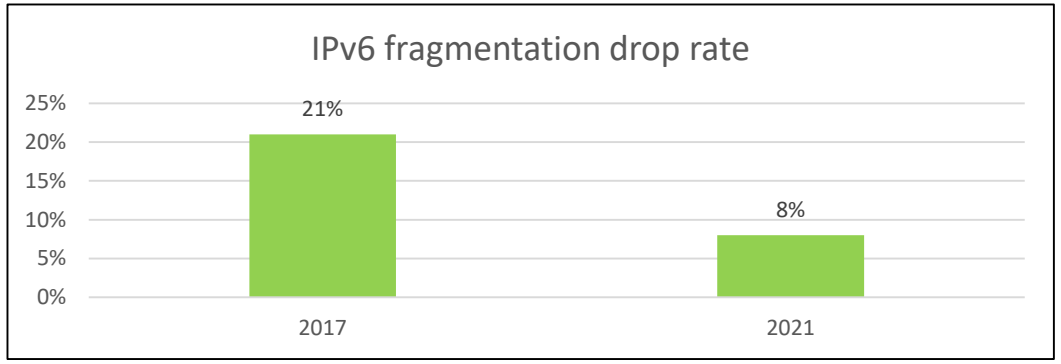
IPv6 traffic 5% - depressing

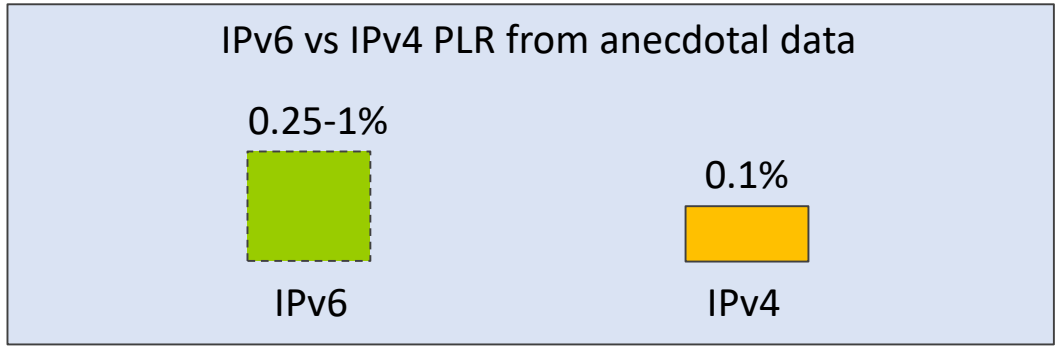


What cause the big gap?

Theory: Dual-Stack Hides Some IPv6 Issues that Cause DS Users to Use IPv4

RFCs 7872/9098 report high PLR for IPv6 packets with EHs. Anecdotal data shows IPv6 PLR is higher (0.25-1%)





Possible issues that may cause Dual-Stack users not to use IPv6:

- RFC6724 prioritizes IPv4 over IPv6 ULA
- Packet drop may cause Happy Eyeball to select IPv4 for Dual-Stack users
  - Packet drop with EHs,
  - NCE exhaustion causing packet drop
  - Rate limiting to prevent /64 scanning causing NCE exhaustion
  - Long headers causing congestion/drop at mobile backhaul links
  - Fragmentation-related drops
  - Flash renumbering-related drops

Proposal: Collaborate to Identify & Solve Issues

- Provide IPv6 traffic stats if you can
- Feedback whether you agree/disagree with our theory
- Join us to identify & solve Issues

It’s time for the community to measure & publish IPv6 traffic stats

Please Applaud!!! (and the crowd goes wild)

IETF117: Path Selection in Multi Tunnel SD-WAN

Altanai B (altanai@outlook.com)
Cisco Meraki

Many options for Path selection

Networks today have various ways to choose path, as

- Tunnelling protocol preference
  - (IPSec, SSL , GRE or proprietary AutoVPN ...)
- split tunnel
- DTLS , WS ...
- MASQUE tunnel
- PoP routing

so on

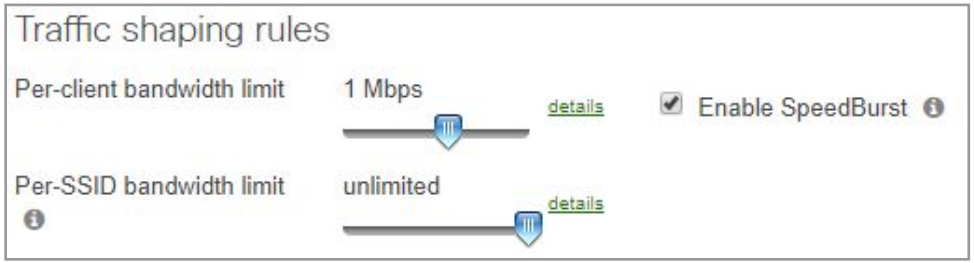
Many options when there are multiple active tunnels

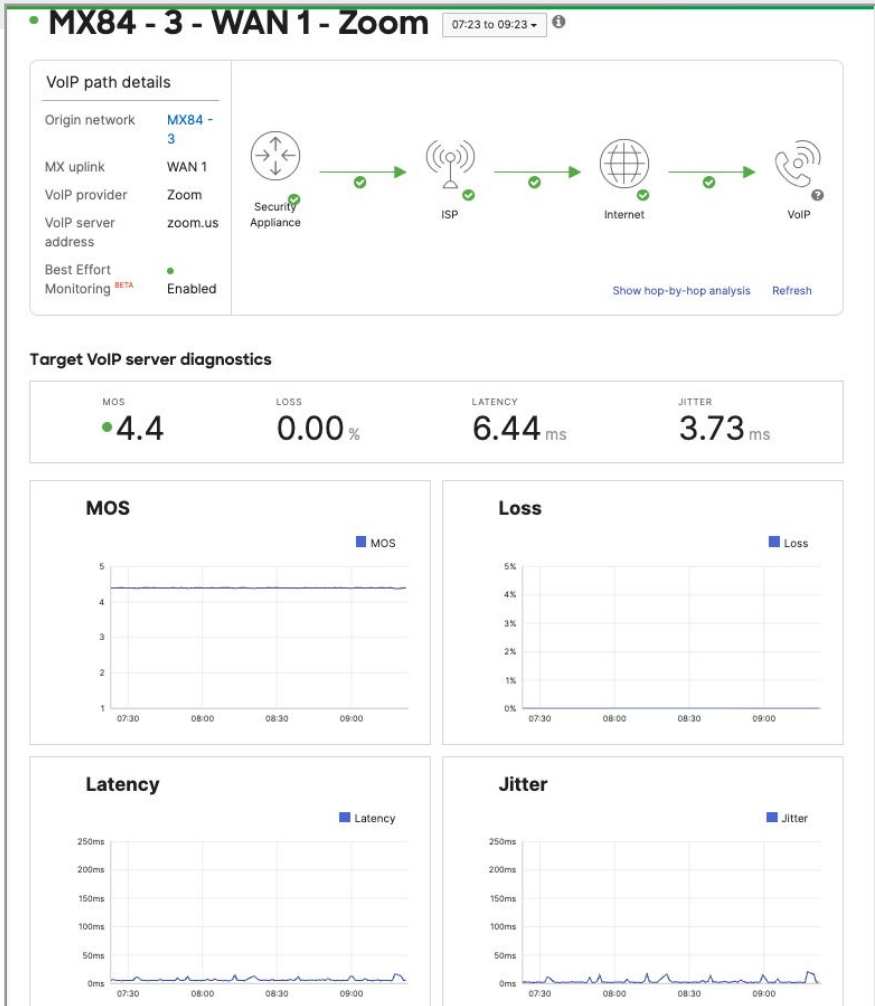
- Full or Split tunnel based on DSCP tags(Diffserv).

Example :

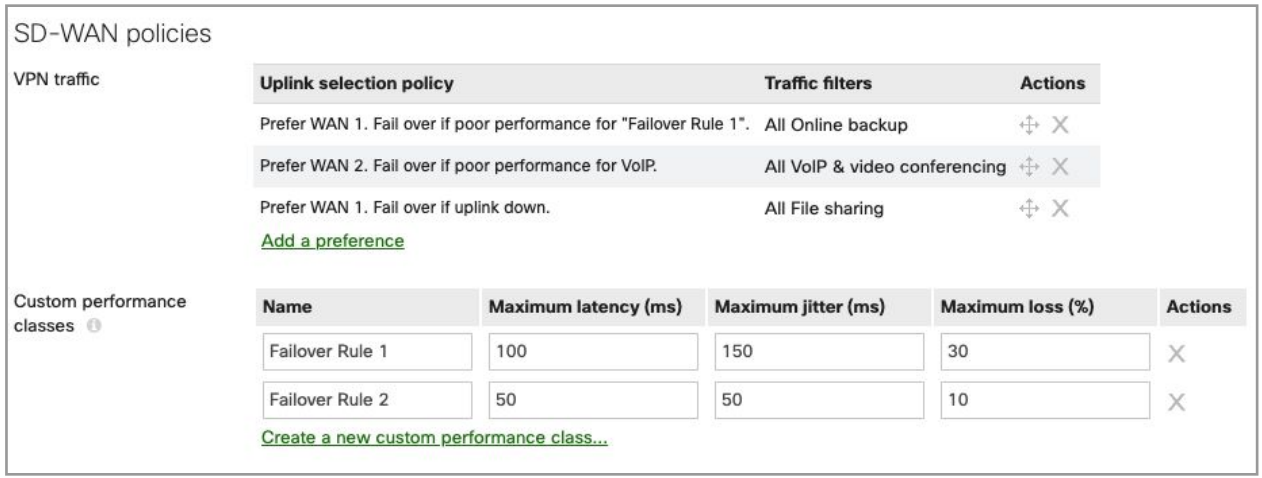
Traffic Type	DSCP tag
SIP (Voice)	46 (EF - Expedited Forwarding, Voice)
All Advertising, All Software Updates, All Online Backups	10 (AF11 - High Throughput, Latency Insensitive, Low Drop)
WebEx, Skype	34 (AF41 - Multimedia Conferencing, Low Drop)
All Video & Music	18 (AF21 - Low Latency Data, Low Drop)

- Weighted round robin order or ECMP
- Traffic Shaping generic rules based on
  - QoS (such as MOS, jitter other customized score)
  - Attributes such as app type or address
  - Client identifier based rules

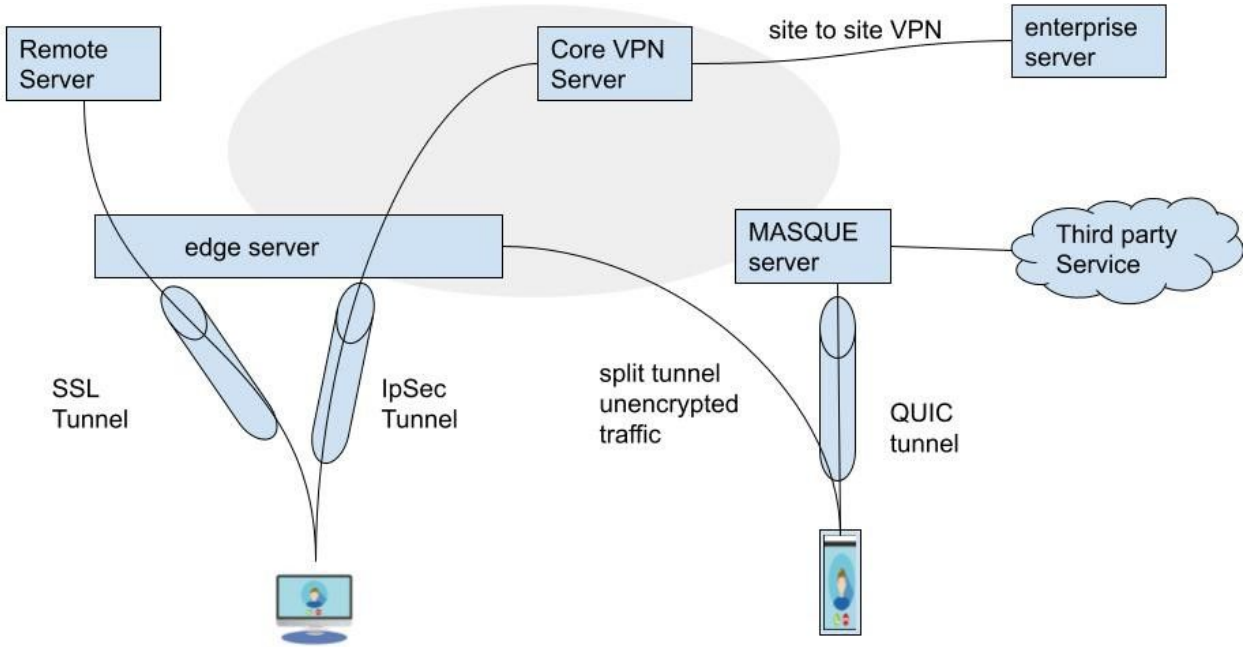




- Policy-Based routing
  - Flow preferences to pin traffic to a particular path.
  - Geo or proximity based rules.



- Dynamic Path Selection such as Network Based Application Recognition (NBAR) from Cisco
- MASQUE
  - QUIC multiplexing



Standardised Algorithm for preferred Path Selection

Overcomes

counter productive use cases as

- added latency on real time streaming
- added encryption for already end-to-end encrypted VoIP calls

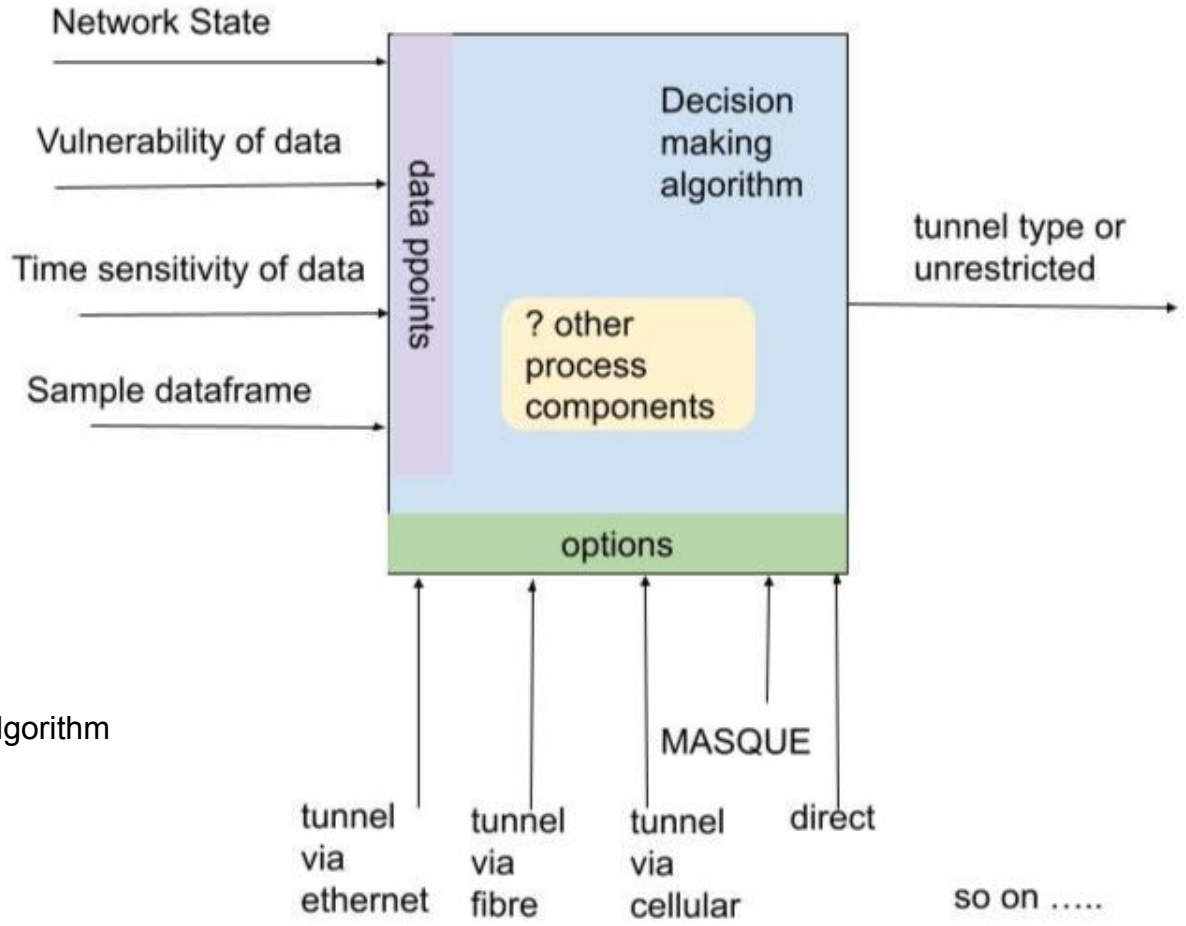
NAT traversal nightmare

nested tunneling and double congestion control

exhausting limited bandwidth available from VPN providers

strategies which unfairly maximize bandwidth usage in the public internet.

Algorithm for preferred Path Selection



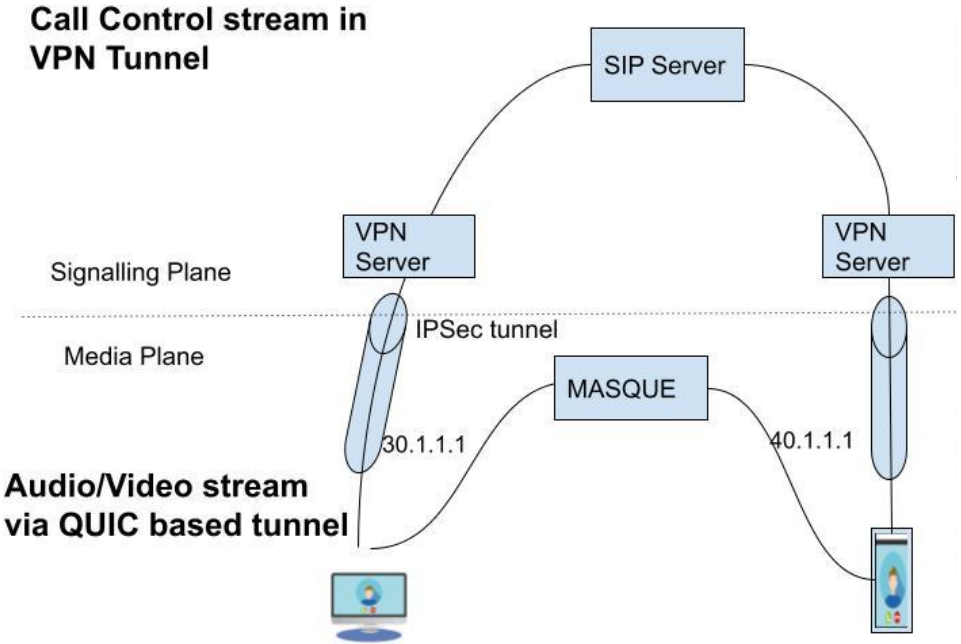
Suggestive data points for Decision making algorithm

Invite Discussions on the Algorithm itself

Sample decisions

1. Direct connection for resource intensive application such as multiplayer games

2. Tunneling the VoIP traffic via separate routes,
   - signaling plane data on VPN tunnel,
   - media via MOQ.



Sample decisions cont.

3. SIP trunk calls may actually benefit from a dedicated IPSec tunnel, pre NATed, pre authenticated and secure, as it would avoid the delay in resetting the path given the volume of calls expected between two endpoints.

4. Heavy file downloads such as VoD could benefit by load sharing between multiple tunnels.

Thank you !

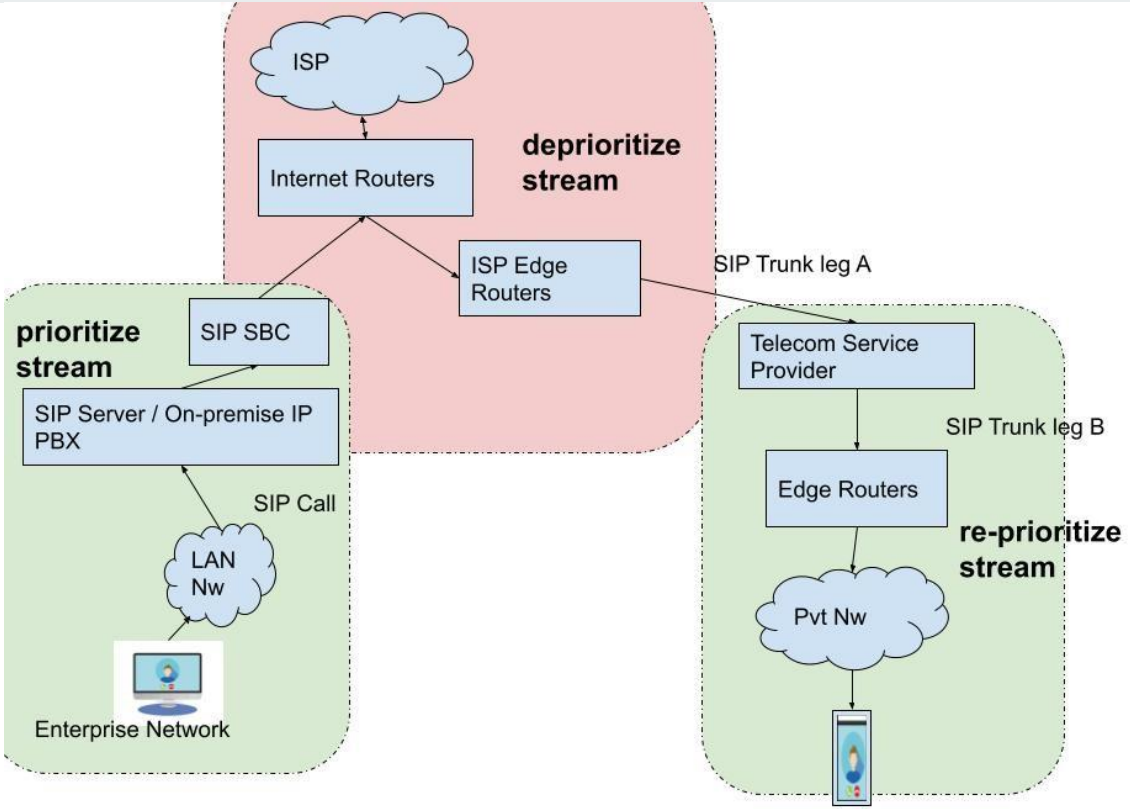
Email : altanai@outlook.com

Scope of Further research

Mismatched prioritization across networks

- Packet marking and queuing of other non critical traffic to optimize for real time streams
- VPN providers, CSPs and/or ISP may employ polar-opposite algorithms to shape traffic based on their interest

Non-synchronized path handling



Same stream prioritized in some networks and deprioritized in others

Advantages of standardized Path selection decision making algorithm

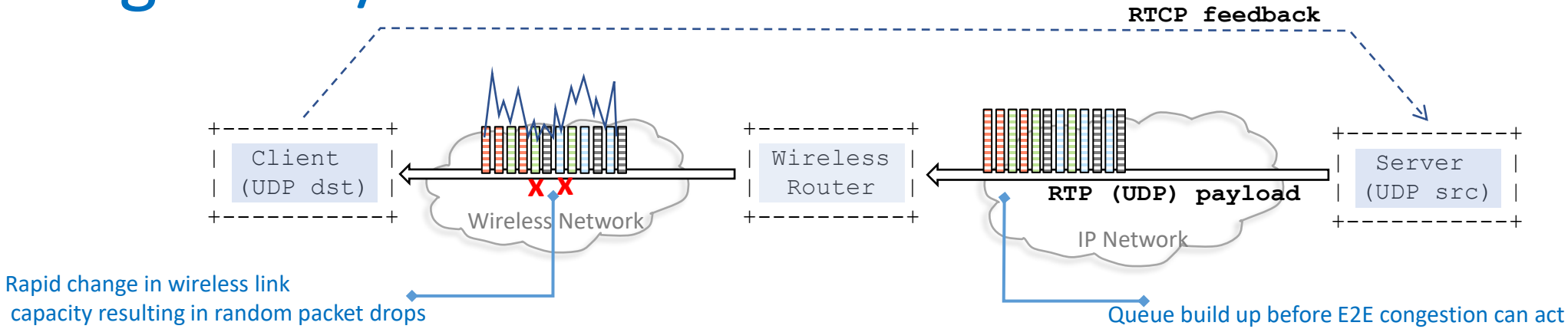
- ensure same treatment of the stream across heterogeneous networks
- edge gateway can decide if data is send to core VPN system be NATed and sent out unencapsulated.

Please Applaud!!! (and the crowd goes wild)

Alternative Optimizations for Low Latency Media Handling

John Kaippallimalil, Sri Gundavelli, Spencer Dawkins

Background/context - media metadata



Large transient variations in link capacity in wireless access, and variations will be even more with millimeter wave radio.

3GPP Rel 18 has specified L4S, selective packet drops for RTP. L4S/ECN feedback reacts in ~100 ms; selective drops ~1 ms.

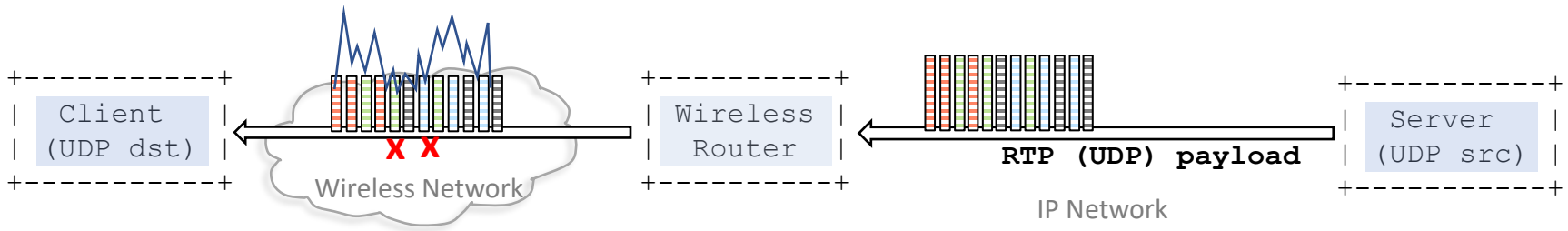
For encrypted media, media-hdr-wireless draft submitted to tsvwg proposes media metadata sent in UDP extensions (used by wireless router to classify, and wireless network optimizes shaping/scheduling and selective drops)

See tsvwg-media-hdr-wireless draft (tsvwg session on Tuesday 17:00 – 18:00 @ Continental 5)

Next 2 slides outline some related but new issues that need further discussion.

- Evolving media encoding
- Feedback to server

I. Evolving Media Encoding



Previous slide looks at metadata to help wireless networks.

However, media applications and encoding are evolving:

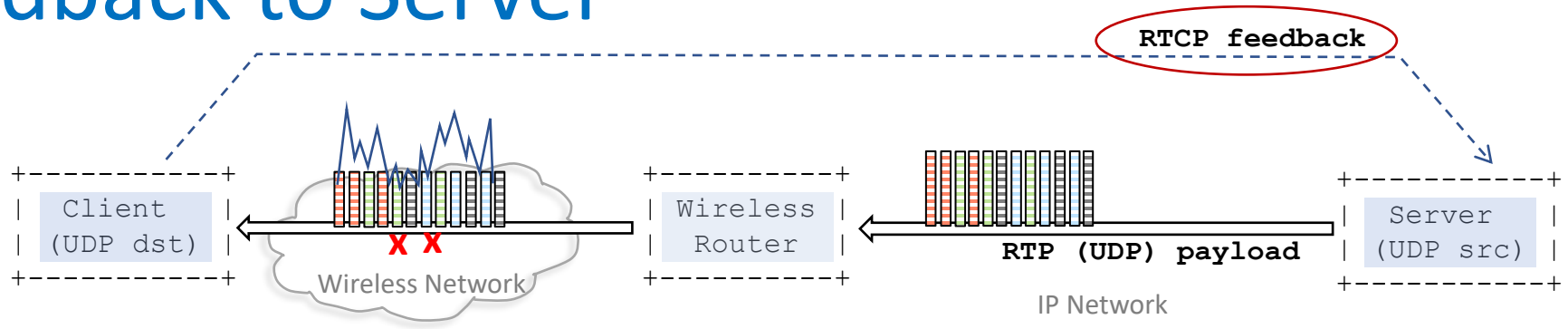
- How will AI-generated content (avatars ?), and video, audio, haptics be encoded?
  - wireless schedulers currently optimize assuming periodic handling (like video I-frames, P-frames, audio …)

- Will different encodings be sent as streams within a single transport?
  Or separate transport connections that need to be coordinated?

- How can applications (server side) provide additional information so that UDP packets on the wire have this additional metadata?

- And the UDP source maybe a streaming server, or it can be a wireless client (UE) that generates upstream content.

II. Feedback to Server



In tsvwg-media-hdr-wireless, the wireless network avoids random drops and instead drops a set of packets affect the media application less (i.e., lower priority, localize to one group of packets)

The feedback via RTCP, etc. is used by the server for pacing and adjusting the sending rate.
However, when a large number of packets are dropped, the server may reach an unexpected conclusion:

- Should the server reduce the sending rate?
  In some cases, perhaps not as capacity variation is transient and still need high throughput/max utilization
- What other impacts/behavior should be indicated in the feedback loop?

Please Applaud!!! (and the crowd goes wild)

Encrypted Client Hello Deployment Considerations

Andrew Campling Andrew.Campling@419.Consulting

Arnaud Taddei Arnaud.Taddei@broadcom.com

Simon Edwards Simon.Edwards@broadcom.com

Paul Vixie Paul@Redbarn.Org

David Wright David.Wright@SWGfL.Org.UK

Context

- Encrypted Client Hello (ECH) is “a mechanism in Transport Layer Security (TLS) for encrypting a ClientHello message under a server public key”
- Builds on the previous Encrypted Server Name Indication (eSNI) proposal
- Being developed within the IETF’s TLS working group
- See https://datatracker.ietf.org/doc/draft-ietf-tls-esni/ for the latest version (currently draft -16)

What is the Issue?

- RFC 8744 – “Issues and Requirements for Server Name Identification (SNI) Encryption in TLS”
  - Includes a brief description of what it characterises as "unanticipated" usage of SNI information (section 2.1)
  - A brief assessment of alternative options in the event that the SNI data is encrypted (section 2.3)
  - Asserts that "most of [the unanticipated usage] functions can, however, be realized by other means“
- The data encapsulated by ECH is of legitimate interest to on-path security actors including anti-virus software, parental controls [and other content filtering] and consumer and enterprise firewalls – there’s a lot of running code!
- Some end user groups (eg Fortune 500 CISOs) are becoming very concerned about the implications for their cybersecurity, orgnisational policy on content access etc

Supporting End Users

The current ECH Deployment Considerations draft includes:

- Observations on current use cases for SNI data in a variety of contexts, clarifying why it is preferred to DNS
- Reasons why the use of that data is important to the operators of both public and private networks (eg enterprises and educational establishments)
- Information on how the loss of access to SNI data will cause difficulties in the provision of services to end-users, complicates support for BYOD and potentially weakens cybersecurity

In addition, some mitigations are identified that may be useful for inclusion by those considering the adoption of support for ECH in their software.

If ECH Deployment Considerations Interests You….

- The current version of the draft is at:
  - https://datatracker.ietf.org/doc/draft-campling-ech-deployment-considerations/
  - To be updated with an -07 version shortly

- To engage on this topic:
  - Speak to Arnaud Taddei (Arnaud.Taddei@broadcom.com) or Andrew Campling (Andrew.Campling@419.Consulting) – both here all week
  - Use the public GitHub page at https://github.com/echdeploy/draft-ech-deployment-considerations

If you want to work on the design of ECH itself, go to the TLS working group

Thank You

Please Applaud!!! (and the crowd goes wild)

Thank you to the presenters!