WiFi: attwifi

MaRNEW Workshop

24-25 Sept 2015

iab.org/activities/workshops/marnew/

09:00 - 09:20
Introduction

Chair: Joe Hildebrand
Minute Taker: Ben Campbell

Thanks

- AT&T for providing the location (Dan Druta)
- ISOC for sponsoring the dinner (Karen O’Donoghue)
- GSMA for sponsoring the food and managing logistics (Istvan Lajtos)
- Cindy Morgan

Technical Programme Committee

- Joe Hildebrand, IAB / Cisco, USA
- Stephen Farrell, IETF AD / Trinity College Dublin, Ireland
- Jari Arkko, IETF Chair / Ericsson, Finland
- Natasha Rooney, GSMA, UK
- Spencer Dawkins, IETF AD, USA
- Kathleen Moriarty, IETF AD / EMC, USA
- Barry Leiba, IETF AD / Huawei, USA
- Alia Atlas, IETF AD / Juniper Networks, USA
- Ben Campbell, IETF AD / Oracle, USA
- Karen O’Donoghue, ISOC, USA
- Phil Roberts, ISOC, USA
- Kevin Smith, Vodafone, UK
- Sanjay Mishra, Verizon, USA
- Istvan Lajtos, GSMA, UK
- Salvatore Loreto, Ericsson, Finland
- Diego Lopez, Telefonica, Spain
- Dan Druta, AT&T, USA
- Brian Trammell, ETH Zurich, Switzerland

Agenda

Thur 24

09:00 – 09:20	Introduction: welcome, introductions and announcements
09:20 – 10:00	Scene Setting: defining goals, layouts and key in and out of cope topics.
10:00 – 11:15	Session 1: Encryption Deployment Considerations
11:15 – 11:45	Coffee Break
11:45 – 13:00	Session 2: Trust Models and User Choice (Privacy)
13:00 – 14:00	Lunch
14:00 – 15:45	Session 3: Sending Data Up for Network Management Benefits
15:45 – 16:15	Break
16:15 – 17:30	Session 4: Sending Data Down for Network Management Benefits
17:30 – 18:00	Day 1 Wrap Up

Fri 25

09:00 – 10:30	Session 5: Application Layer Optimisation, Caching and CDNs
10:30 – 11:00	Break
11:00 – 12:30	Session 6: Transport Layer: Issues, Optimisation and Solutions
12:30 – 13:30	Lunch
13:30 – 14:30	Session 7: Technical Analysis and Response to Potential Regulatory Reaction
14:30 – 15:30	Parking Lot: time to review open questions from the last two days
15:30 – 16:00	Break
16:00 – 17:00	Roundup

Chairs & Minute Takers Today

09:00 – 09:20 Introduction: welcome, introductions and announcements
Chair: Joe Hildebrand, Minute Taker: Ben Campbell

09:20 – 10:00 Scene Setting: defining goals, layouts and key in and out of cope topics.
Chair: Stephen Farrell, Minute Taker: Sanjay Mishra

10:00 – 11:15 Session 1: Encryption Deployment Considerations
Chair: Kathleen Moriary, Minute Taker: Istvan Lajtos

11:45 – 13:00 Session 2: Trust Models and User Choice (Privacy)
Chair: Karen O'Donoghue, Minute Taker: Ben Campbell

14:00 – 15:45 Session 3: Sending Data Up for Network Management Benefits
Chair: Joe Hildebrand, Minute Taker: Diego Lopez

16:15 – 17:30 Session 4: Sending Data Down for Network Management Benefits
Chair: Dan Druta, Minute Taker: Phil Roberts

17:30 – 18:00 Day 1 Wrap Up
Chair: Istvan Lajtos, Minute Taker: Natasha Rooney

Today’s Slides

Please send slides to:

nrooney@gsma.com

Or get ready to present them from your machine!

Administrivia

Chairs: Joe Hildebrand, Natasha Rooney

- Audio Bridge and Recordings
- Restrooms
- Wifi: attwifi
- Host security request
- Meet new people!

Assumptions:

- All traffic is encrypted
- Unencrypting traffic is out of scope

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Dinner: 24 Sept, 18:30

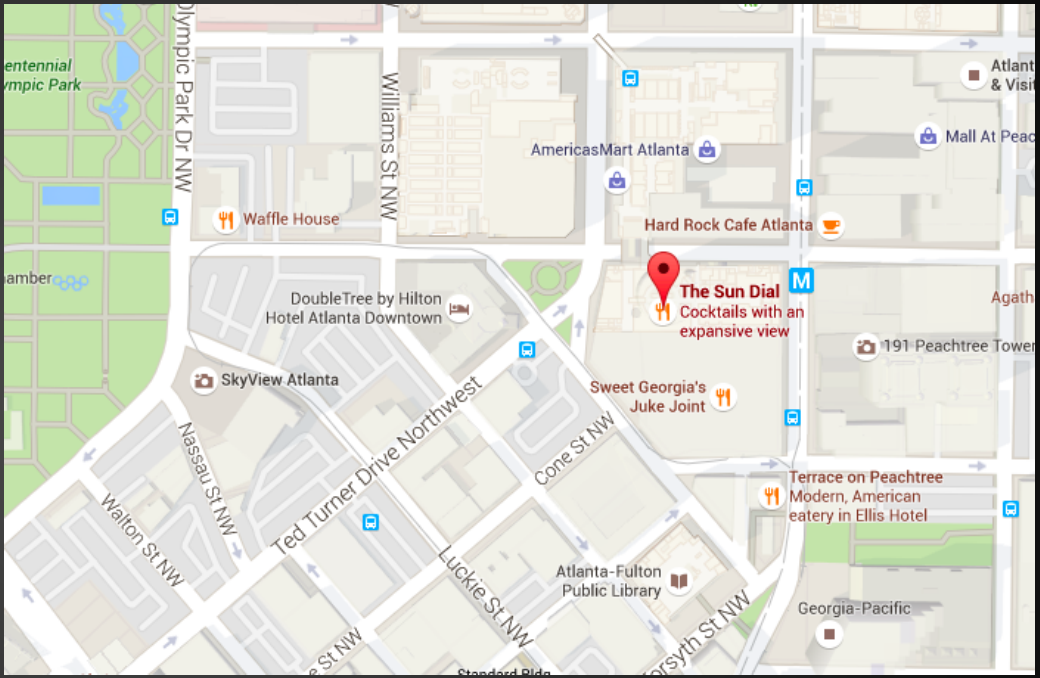
SunDial Restaurant

The Westin Peachtree Plaza, Atlanta
210 Peachtree St NW
Atlanta, GA 30303
http://www.sundialrestaurant.com/

Distance: 1.1 miles from the meeting venue, 25 minute walk, 10 minute (2 stop) MARTA trip, or 10 minute car/cab ride.

Reception/appetizers followed by dinner.

Thank-you Karen O'Donoghue and ISOC for sponsoring the dinner!



WiFi: attwifi

09:20 - 10:00
Scene Setting

Chair: Stephen Farrell
Minute Taker: Sanjay Mishra

iab.org/activities/workshops/marnew/

Session End

10:30 - 11:30
Session 1: Encryption Deployment Considerations

Chair: Kathleen Moriarty
Minute Taker: Istvan Lajtos

Speaker & Panelists

Chair: Kathleen Moriarty (IETF AD / EMC)

- *Technical Programme Committee*
- *Paper: “Respect the wishes of those encrypting”*
- *Paper: “Effect of Ubiquitous Encryption”*

Kevin Smith (Vodafone)

- *Technical Programme Committee*
- *Paper: “Network Management of Encrypted Traffic”*
- *Paper: “Encryption and government regulation: what happens now?”*

Minute Taker: Istvan Lajtos

Session End

11:30 - 12:00: Break

WiFi: attwifi

12:00 - 13:00
Session 2: Trust Models and User Choice (Privacy)

Chair: Karen O’Donoghue

Minute Taker: Ben Campbell

iab.org/activities/workshops/marnew/

Speaker & Panelists

Chair: Karen O’Donoghue (ISOC)

- *Technical Programme Committee*
- *Paper “Barriers to Deployment: Probing the Potential Differences in Developed and Developing Infrastructure”*

Wendy Seltzer (W3C)

- *Paper “Performance, Security, and Privacy Considerations for the Mobile Web”*

Patrick McManus (Mozilla)

- *Paper “User Consent and Security as a Public Good”*

Szilveszter Nadas (Ericsson)

- *Paper “Concept for Cooperative Traffic Management”*

Minute Taker: Ben Campbell

Session End

13:00 - 14:00: Lunch

WiFi: attwifi

14:00 - 15:45
Session 3: Sending Data Up for Network Management Benefits

Chair: Joe Hildebrand
Minute Taker: Diego Lopez

Speaker & Panelists

Chair: Joe Hildebrand (IAB / Cisco)

- *Technical Programme Committee*

Humberto La Roche (Cisco)

- *Paper “Use Cases for Communicating End-Points in Mobile Network Middle-Boxes”*

Andreas Terzis (Google)

- *Paper “Sharing network state with application endpoints”*

Patrick McManus (Mozilla)

- *Paper “User Consent and Security as a Public Good”*

Minute Taker: Diego Lopez

WiFi: attwifi

Session End

iab.org/activities/workshops/marnew/

15:45 - 16:15: Break

WiFi: attwifi

16:15 - 17:30
Session 4: Sending Data Down for Network Management Benefits

Chair: Dan Druta
Minute Taker: Phil Roberts

Chair & Panelists

Chair: Dan Druta (AT&T)

- *Technical Programme Committee*

Dirk Kutscher (ZTH Zurich / NEC Lab)

- *Paper “Enabling Traffic Management without DPI”*

Chunshan Xiong (Huawei)

- *Paper “The effect of encrypted traffic on the QoS mechanisms in cellular networks”*

Kevin Smith (Vodafone)

- *Technical Programme Committee*
- *Paper: “Network Management of Encrypted Traffic”*
- *Paper: “Encryption and government regulation: what happens now?”*

Minute Taker: Phil Roberts

Sending Data Down for Network Management Benefits

- Use Cases
  - Why and how end-to-end encryption is impacting
  - Can we resolve these in different ways?
  - What do we gain / what do we lose?

Session End

17:30 - 18:00
Day 1 Wrap Up

Chair: Istvan Lajtos
Minute Taker: Natasha Rooney

Session End

18:30 ~ Social Event

Social Event: 24 Sept, 18:30

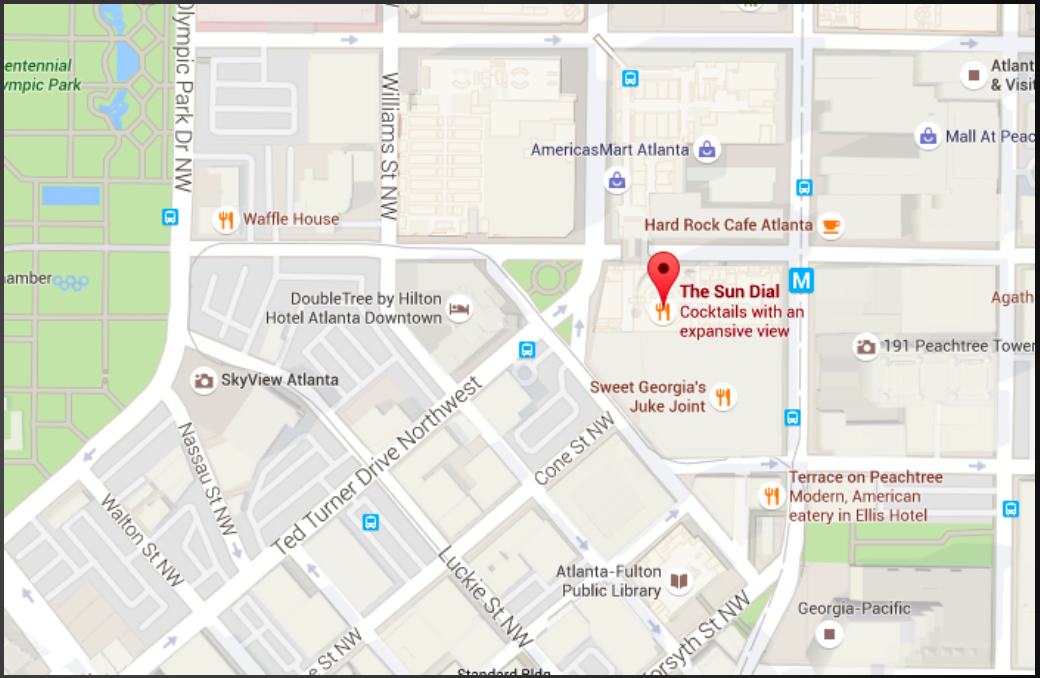
SunDial Restaurant

The Westin Peachtree Plaza, Atlanta
210 Peachtree St NW
Atlanta, GA 30303
http://www.sundialrestaurant.com/

Distance: 1.1 miles from the meeting venue, 25 minute walk, 10 minute (2 stop) MARTA trip, or 10 minute car/cab ride.

Reception/appetizers followed by dinner.

Thank-you Karen O'Donoghue and ISOC for sponsoring the dinner!



WiFi: attwifi

MaRNEW Workshop: Day 2

25 Sept 2015

iab.org/activities/workshops/marnew/

Suggested Scope

- In discussion we should assume: No broken crypto, Ciphertext increasingly common, congestion does need to be controlled as do other transport issues and Network management including efficient use of resources, in RAN and elsewhere, has to work
  - How/why is RAN different for transport; help us understand the complexities of the RAN and how hard it is to manage and why those matter
- What are the precise problems caused by more ciphertext
- Identify players, incl. Users, and resulting tensions and how ciphertext changes those
- Some solutions will be radically changed by ciphertext, it's ok to talk about that
- As good as possible Quality of experience for end user is a goal
- Our aim for the next two days is to analyse the situation and identify specific achievable tasks that could be tackled in the IETF or GSMA (or elsewhere?) and that improve the Internet given the assumptions above
- We should not delve into:
  - Ways of doing interception (legal or not), see RFC2804 for why
  - Unpredictable political actions

Agenda & Administrivia

- Thanks for the dinner!
- Parking Lot
- Chatham house rules session
- Transport
- Jabber: marnew@conference.xmpp.rg.net
- Asking questions: mic, jabber, mailing list, direct mail.

Fri 25

09:00 – 10:30	Session 5: Application Layer Optimisation, Caching and CDNs
10:30 – 11:00	Break
11:00 – 12:30	Session 6: Transport Layer: Issues, Optimisation and Solutions
12:30 – 13:30	Lunch
13:30 – 14:30	Session 7: Technical Analysis and Response to Potential Regulatory Reaction
14:30 – 15:30	Parking Lot: time to review open questions from the last two days
15:30 – 16:00	Break
16:00 – 17:00	Roundup

09:00 - 09:20: Introduction

WiFi: attwifi

Agenda

09:00 – 10:30 Session 5: Application Layer Optimisation, Caching and CDNs
Chair: Stephen Farrell, Minute Taker: Kevin Smith

11:00 – 12:30 Session 6: Transport Layer: Issues, Optimisation and Solutions
Chair: Spencer Dawkins, Minute Taker: Karen O’Donoghue

13:30 – 14:30 Session 7: Technical Analysis and Response to Potential Regulatory Reaction
Chair: Barry Leiba, Minute Taker: Istvan Lajtos

14:30 – 15:30 Parking Lot: time to review open questions from the last two days
Chair: Ted Hardie, Minute Taker:

16:00 – 17:00 Roundup
Chair: Natasha and Joe, Minute Taker:

WiFi: attwifi

09:00 - 10:30
Session 5: Application Layer Optimisation, Caching and CDNs

Chair: Stephen Farrell
Minute Taker: Kevin Smith

Speaker & Panelists

Chair: Stephen Farrell (IETF AD / Trinity College Dublin)

- Technical Programme Committee

Thomas Anderson (Cisco)

- *Paper “Bandwidth Control and Regulation in Mobile Networks via SDN/NFV-Based Platforms”*

Salvatore Loreto (Ericsson, Technical Programme Committee)

Blake Matheny (Facebook, Special Invited Guest)

Sanjay Mishra (Verizon, Technical Programme Committee)

Rich Salz (Akamai, Special Invited Guest)

Mark Watson (Netflix, Special Invited Guest)

Minute Taker: Kevin Smith

Session End

WiFi: attwifi

10:30 - 11:00: Break

iab.org/activities/workshops/marnew/

WiFi: attwifi

11:00 - 12:30
Session 6: Transport Layer: Issues, Optimisation and Solutions

Chair: Spencer Dawkins
Minute Taker: Karen O’Donoghue

iab.org/activities/workshops/marnew/

Speaker & Panelists

Chair: Spencer Dawkins (IETF AD, unaffiliated)

- Technical Programme Committee

Zubair Shafiq (The University of Iowa)

- *Paper "Tracking Mobile Video QoE in the Encrypted Internet"*

Jianjie You (Huawei)

- *Paper "Use Case Analysis and Potential Bandwidth Optimization Methods for Encrypted Traffic"*

Marcus Ihlar (Ericsson)

- *Paper "Performance Enhancing Proxies in an Encrypted World"*

Aaron Falk (Akamai, Special Invited Guest)

Jana Iyengar (Google, Special Invited Guest)

Minute Taker: Karen O'Donoghue

Session End

12:30 - 13:30: Lunch

WiFi: attwifi

13:30 - 14:30
Session 7: Technical Analysis & Response to Potential Regulatory Reaction

Chair: Barry Leiba
Minute Taker: Istvan Lajtos

Chatham House Rule

This session will be conducted under Chatham House Rule. Note Well is not in effect for this session. Please don't cause IPR issues for others.

"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

Speaker & Panelists

Chair: Barry Leiba (IETF AD / Huawei)

- Technical Programme Committee

Kevin Smith (Vodafone)

- Technical Programme Committee

Russ Housley (IAB)

Olaf Kolkman (ISOC)

- Special Invited Guest

Diego Lopez (Telefonica)

- Technical Programme Committee

Minute Taker: Istvan Lajtos

Session End

14:30 - 15:30
Parking Lot

Chair: Ted Hardie
Minute Taker:

Title

-

Session End

15:30 - 16:00: Break

16:00 - 17:00
Roundup

Chair: Joe and Natasha
Minute Taker: Joe

Roundup

- Session by session
- Successes and Next Steps
- The Ideas
- IETF Chair Summary
- Comments…
- Admin

Roundup

Thur 24

09:00 – 09:20	Introduction: welcome, introductions and announcements
09:20 – 10:00	Scene Setting: defining goals, layouts and key in and out of cope topics.
10:00 – 11:15	Session 1: Encryption Deployment Considerations
11:15 – 11:45	Coffee Break
11:45 – 13:00	Session 2: Trust Models and User Choice (Privacy)
13:00 – 14:00	Lunch
14:00 – 15:45	Session 3: Sending Data Up for Network Management Benefits
15:45 – 16:15	Break
16:15 – 17:30	Session 4: Sending Data Down for Network Management Benefits
17:30 – 18:00	Day 1 Wrap Up

Fri 25

09:00 – 10:30	Session 5: Application Layer Optimisation, Caching and CDNs
10:30 – 11:00	Break
11:00 – 12:30	Session 6: Transport Layer: Issues, Optimisation and Solutions
12:30 – 13:30	Lunch
13:30 – 14:30	Session 7: Technical Analysis and Response to Potential Regulatory Reaction
14:30 – 15:30	Parking Lot: time to review open questions from the last two days
15:30 – 16:00	Break
16:00 – 17:00	Roundup

Roundup

Scene Setting: defining goals, layouts and key in and out of cope topics.

- Increasing encryption
- Issue of qualifying trust
- Anti-spam, malware are real problems. Need use cases.
- Transport issues, radio network vs transport?

Scope

- In discussion we should assume: No broken crypto, Ciphertext increasingly common, congestion does need to be controlled as do other transport issues and Network management including efficient use of resources, in RAN and elsewhere, has to work
  - How/why is RAN different for transport; help us understand the complexities of the RAN and how hard it is to manage and why those matter
- What are the precise problems caused by more ciphertext
- Identify players, incl. Users, and resulting tensions and how ciphertext changes those
- Some solutions will be radically changed by ciphertext, it's ok to talk about that
- As good as possible Quality of experience for end user is a goal
- Our aim for the next two days is to analyse the situation and identify specific achievable tasks that could be tackled in the IETF or GSMA (or elsewhere?) and that improve the Internet given the assumptions above
- We should not delve into:
  - Ways of doing interception (legal or not), see RFC2804 for why
  - Unpredictable political actions

Roundup

Session 1: Encryption Deployment Considerations

- Gave light to issues and existing solutions
- Document: The Effect of Ubiquitous Encryption
    - increased encryption impact
    - collection of current security and network management function impact
    - Incident monitoring (becoming more difficult)
- Encryption will increase security
    - but monetary motivation behind selling boxes for preventing security attacks.
- Document: Network management of encrypted traffic
    - Mobile centric document
- Discussion
    - Radio networks are different
    - Cell handover creates not modelled in the TCP chain

Roundup

Session 2: Trust Models and User Choice (Privacy)

- 64% of users said concerns over privacy have increased
- 67% would like to do more to protect privacy
- Web (and internet) is responding
- Network operator is more like 4th party
- Good faith management strategies are indistinguishable from attacks. Bad actors will use those vectors.
- Policy controller: consent from one endpoint
- Consent may be needed from all endpoints
- Discussion
  - Difficulties finding useful APIs or maintaining policy
- Need finer granularity and more transparency about implications of choice
  - more immediate feedback on costs and benefits
  - authentication is often missing

Roundup

Session 3: Sending Data Up for Network Management Benefits

- Radio environment is complex, difficult to use with TCP
- Collaborative frameworks between content providers and mobile operators
    - Mobile Throughput Guidance
- Base station will have a key role. Can a controller adapt, and preserve E2E?
- TCP
    - Fixing TCP may not be the answer to a broken TCP
    - a different Internet: SPUD, ICN?
    - TCP is based on specific network model
    - Need abstractions for making transport protocol evolve
- Up-the-stacks solutions (blind caches)
- Whole network is important
- Avoid personal identifiers
- Content provider motivation to encrypt: avoid in-network modifications

Roundup

Session 4: Sending Data Down for Network Management Benefits

- Cooperative traffic management: meaningful capacity sharing, reacting to wireless link layer conditions, privacy friendly
- TCP feedback to senders and receivers
- Middleboxes treat data differently according to types
- Mobile network manages applications based on the resources available
- 3GPP has defined PCC-QoS mechanism, encryption breaks this:
    - if there is a lack of radio resources, you may release the wrong services
    - during handover can't well adapt services
    - middlebox services stop working
- Does it make sense for apps to send data to networks?
- Latency vs. bandwidth - preference? Needs incentive framework
- Assumption that applications need to declare the QoS they need: never worked.
    - 1 bit of information, where to do this?
- FQ-codel

Roundup

Session 5: Application Layer Optimisation, Caching and CDNs

- Trusting a fixed network CDN in a mobile context (CDN is content provider)
- CDNi work
- Content providers make assumptions that the network will adhere to standards
    - Costly if that doesn’t happen
    - Adaptive streaming just responds to network situation
- Developers develop on WiFi
- Not every company can build a cache infrastructure
- Problem Statement: Encryption is not the problem, rather a catalyst to get together to discuss network management in the broader sense.
- Actors: application provider, network, device. work together!
- Operators work with CDNs and do caching
- Optimisations: way to design the network layer or transport layer?
- Split browsers exist, and are needed now, hopefully go away

Roundup

Session 5: Application Layer Optimisation, Caching and CDNs (cont…)

- Split browsers exist, and are needed now, hopefully go away
- Keyless SSL
- Blind cache
- Testing and Metrics
  - Standards compliance helps testing
- What’s the one thing you could do if it related to the application layer?
  - metrics to allow for better resource allocation
  - metrics
  - network is calibrated to handle applications best
  - anything that makes it easier for the application to adapt
  - blind cache

Roundup

Session 6: Transport Layer: Issues, Optimisation and Solutions

- Collaboration essential
- Bufferbloat is an issue
- Congestion Control innovations
- Problem identification: resource optimisation
- 1 bit: how and where
- Need data and metrics
- Traffic classification, a solution?
- Metadata schemes can be exploited
- ECN

Roundup

Parking Lot

- Submitting meaningful data to IETF
- CROWN as a BOF in BA on co-operative resource management
- Layer of Applicability

Successes & Next Steps

Successes

- Know the people
- Understand topics, technologies and issues
- Discussed some good ideas

Next Steps

- Write Up
  - Draft Transcript / Minutes: Before end Oct
  - Report: December
- IETF94: SAAG Meeting
- Take Ideas from the meeting, discuss on mailing lists
- IETF95: bring ideas to working group or BOF
  - (if applicable!)

The Ideas

Not confirmed! Just an incomplete list of generated ideas:

- IETF gain an understanding of RAN
- Reviews and comments on 3GPP perspective
- AQM
- **Evolving TCP (or evolving transport)**
    - Congestion Control
    - SPROUT (MIT)
    - PCC (Performance & Congestion Control)
- How to do congestion controlling in RAN
    - Base Station
    - Controller that can adapt to a radio environment and provide a better experience, and preserve E2E
- Identify traffic types via 5-tuple
- Heuristics (for best effort only?)
- CDNs / caches in the network
- CDN improvements
- **Mobile Throughput Guidance**
- **One bit for latency bandwidth tradeoff**
- Small amount of data from network to user (ECN)
- API for app to query network, or vice versa
- **Blind Caching**
- Standard approach for operator to offer services to Content Providers
- **Better Collaboration**
- Sharing information hop by hop
- **Metrics and metric standards**
- Testing / Debugging
- Trust model / framework (e.g. for spud)
- Keyless SSL
- Meaningful capacity sharing; reacting correctly to wireless link layer condition
- 5G

I have comments...

Please feel free to share your comments!

marnew@iab.org

Joe: jhildebr@cisco.com

Natasha: nrooney@gsma.com

Slides

Please send slides to:

nrooney@gsma.com

Slides need to go up on the MaRNEW Website.

Thanks

- AT&T for providing the location (Dan Druta)
- ISOC for sponsoring the dinner (Karen O’Donoghue)
- GSMA for sponsoring the food and managing logistics (Istvan Lajtos)
- Cindy Morgan

Chairs, Panelists and Minute Takers

and everyone for attending!

Session End

Thank-you & Happy Travels!

WiFi: attwifi

Title

-

iab.org/activities/workshops/marnew/

Chair Summary

Main Observations

- The world does not end when there's more encryption, but some current solutions may need to change to work better with encrypted traffic
- The problem is not just about encryption, the issue is how do we optimise customer experience across a number of players?
- Identified a number of potential technical items to pursue in the short-term
- Co-operative resource management ideas gained a lot of interest in the workshop, along some other ideas
- 5G is an opportunity to do things better, together, more long-term

Technical Items to Pursue

- Develop co-operative resource management by sending data up or down (very little)
- Make CDN improvements (CDNI, blind caches, certs, keyless SSL)
- Build better testing and debugging tools

Chair Summary

Immediate Actions

- Develop ideas on what information would be useful in Kevin's data
- On-marnew-list and informal work, no need to wait for IETF meetings
- CROWN as a BOF in BA on co-operative resource management
- TBD actions for CDN improvements
- TBD actions for testing and debugging
- (In addition I know I'm personally interested in 3GPP identity privacy and NSA-proof SIM card improvements. But that's not an IETF activity.)