**Internet Area working group meeting at IETF 79**
**Thursday, November 11, 13:00 – 15:00, Valley Ballroom C**

*Minutes by Ed Jankiewicz, edward.jankiewicz@sri.com.*

Working group items
Ipv4-id-udate
revisions since Maastricht, please review.  Presentation to follow
router-alert-consideration
proceeding with WGLC, with one open comment
shared-addressing
completed WGLC, going to IESG

Updated Specification of the IPv4 ID
draft-ietf-intarea-ipv4-id-update-01
rewrite for clarity; removed SHOULD send only atomic datagrams
added SHOULD on verify integrity
removed incremental deployment and reordering interval.
rules for safe use and non-reuse of ID; good practice
not new requirements, restated in 2119 language in this doc
comment?  Ready for WGLC?  Need a re-read of the new version and need three solid reviews
Jari – 3 is a small number; this is important.  Concern was that this went beyond existing practice, but need other reviewers to verify that this reflects current reality
Andrew Sullivan for Joe Touch – since the doc changed substantially do we want another WGLC and cross-post to DNS
Jari – definitely.  Chairs - agreed

draft-livingood-dns-whitelisting-implications-01
Jason Livingood
see deck for more details.
how does it work, rationale, implications, solutions and alternatives
you must be on the whitelist to get a AAAA response, like an ACL
why are sites considering?  Some hosts are impaired getting to a site that has AAAA; concerned that some users are harmed.  Estimates are small percentage but significant number of users on large ISP
downsides – another barrier to ready access to IPv6 content, disincentive to turning on
policies will vary by domain
implications – ISPs and content providers need support staff, troubleshooting
may encourage endpoint homogeneity
solutions/alternatives: deploy whitelisting, fix end hosts, accept 0.05-0.10% of user impairment, or help the broken users resolve the issue.
what is appropriate venue for this? And how to publish?  Please review and give feedback.

in particular, want to capture the motivations and balance of the issues
Alain Durand – comment 0.10% brokenness may be measuring noise. Some of this is due to 6to4
Jason – yes, and other transition technologies
Alain – should the IETF deprecate those technologies
Mohsen – support adoption. Everyone thinks of Google when reading this draft, applause for their experiment. If other companies followed Google, it would help. Afraid of balkanization if this is widely deployed. Go for more openness, with risk of some inconvenience.
Jason – whitelisting
erich – what part are you trying to protect? ISP or content provider?
Jason – not leaning towards this for our own content domains
Jari – important to discuss this topic, intarea could home the work. We do need to look at wider actions based on issues with transition technologies (6to4) and better detect breakage? Symapthize with issues, also with content providers – need motivation to deploy IPv6 without creating problems. Whitelist is an on/off thing, or evolving over time. First, separate IPv6 name, then one name for both v4/v6 with whitelisting, then blacklisting, finally IPv6 default. Spectrum evolving over time
Mark Townsley – no just transition technology. Carrying routes, not bad routing. Even native everywhere there are residual issues. Good that the discussion is being held among ISPs and content providers. A trust is growing between the content provider and service providers – can rely on the network, and can rely that someone will use the network we build.
? – if the resolver cached the AAAA does the whitelist still work?
Jason – should not get AAAA in the first place if not on the whitelist
? – what if the host caches?
Jason – if they use an alternate resolver, there are other effects
Kurtis Lindqvist – v6 internet is becoming better every day. Norway test for the 70 largest websites had no problem. Still a good doc to have. More generalized case is also worth documenting in a separate draft.
Christian – definitely interest, we'll talk to the ADs to see what is the right home

Traceroute and Ping Message Extension
draft-shen-traceroute-ping-ext
Naiming Shen
at the beginning of the Internet, ping and traceroute were developed, but had no security considerations. Add authentication, support UDP, TCP and ICMP; backward compatible
evolved from UDP tracerout extension draft
Format – common header with checksum and magic number; authentication and info-request TLV sections.
How to find the extension in the probe? Port is not well know.
comments from intarea resulted in this new document. Any interest in advancing?
Christian – read the draft, follow-up on mailing list

Logging Recommendations for Internet-Facing Servers
draft-durand-server-logging-recommendations

Alain Durand
small topic – due to IPv4 exhaustion, more address sharing, NATs. Logging requirements with more dynamic and shared use of addresses. Need more information to traceback to the individual user of the address. Source port number further identifies the specific user, but also need a timestamp due to reuse of address/port. Granularity of about 1 sec.
also need to know which protocol in use, multiple destination ports.
recommending this practice for internet facing servers that need to log
Wes George – support. Clarify timestamp requirements, MUST, NTP, etc.
Jari – internet finally has some privacy, now you want to fix that? Timestamp tuning may not be so important, but should be in harmony with NAT recommendations on port reuse. Is this current practice?
Alain – coauthor says yes.
Lee – support. NTP may not be necessary, but may be the right order of magnitude
Mark T. be careful how much we recommend here. Some servers may actively discard information to avoid liability, not mandatory for all. Considerations doc may get into more details. Maybe fronted by server load-balancers, which rewrites ports.
Jason – kicking in the wrong door. Important to get it correct.
Christian – wide support, but where should it be homed?
Alain – probably intarea or opsarea.
Christian – should be adopted by intarea? About 28 for, no against. Followup on mailing list.

Native IPv6 Across NAT44 CPEs (6a44)
draft-despres-softwire-6a44-01
Remi Despres
result of combining work started/presented in Maastricht. Now a complete specification to provide IPv6 behind NAT44.
IPv4-only CPEs, getting private IPv4. Some apps need incoming connections.
native IPv6 local must remain local.
other solutions have limitations compared to this problem statement.
IPv6 tunnel brokers not plug-play, non-local routing of local traffic
teredo as-is breaks with some NATs
6a44 modified hosts and 6a44 relays – stateless, to access IPv6 network, via IPv6/UDP/IPv4 with well known port and stateless address mapping
host requests parameters from the relay.
Incremental deployment, add relays as needed.
where teredo exists, it can be seen as an extension
Jari – question the motivation, who cares about QoS. Maybe more efficient. It’s a transition tool, not essential to optimize. Requires coordination. Not clear there is a compelling need for this
Brian Carpenter – need to simplify this problem. Is there something reasonably simple to do to accommodate those who don’t buy new CPE?
Jari – will those people upgrade their software,
ralph droms – they have IPv4 access, this is for someone who is moving towards IPv6, maybe those

people would be upgrading CPE.
Lee – tech plenary – how can IETF help, i.e. help less. This may be something we should not do.
Erich Nordmark – address format includes port number, which may be changing on reboot. Renumber? Yes
Alain – is there a place in IETF? No. echo what Lee said, way too many ways to embed IPv4 already. Already a technology in softwires. Go and modify every IPv6 host, not possible
Mark Townsley – Remi takes solutions and fixes them, e.g. 6rd. this is an attempt to bring teredo into the operator community. Perhaps we should look at modifying teredo to enable the ISPs to do this. If you already have teredo, it is a good thing. Adding it to other equipment that doesn't do teredo not a winner.
Fred Templin – much better service with a tiny bit of state, like a router to do this. Could have a totally native address. True full service, not a transitional tools.
Mohsen – second support – I am for native IPv6, and upgrading CPE etc. as quickly as possible. I hate 6to4, but plenty of use out there. This deserves a chance like 6rd. might put things cleaner out there.

Mobility and Privacy
draft-brim-mobility-and-privacy-00
Scott Brim
privacy is important, especially location privacy in mobility
why is privacy such a problem? Trends toward user/device correlation, and multiple uses of the device.
"privacy by design" is an opportunity to make things better
location leaking isn't just a higher level problem
avoid making data correlatable; confidential data that gets reused in surprising ways. Small leaks that can be correlated add up to loss of privacy
some designs assume no privacy
avoid persistent identifies
endpoint should retain control of when/how to reveal confidential information. Not automatically revealing location for route optimization
Fred Templin – mobility architecture can limit the resolution of location
Alain – very important topic. But users go on social networks and reveal everything. The internet doesn't know how to forget. Maybe data should decay
Scott – don't impede the privacy in internet layer
Jari – maybe logging should forget! Interesting work. Unless the system is built for privacy
Andrew – Pete McCann in Jabber – what about Name Based Sockets.
Christian – you could use emphemeral name. location privacy, no impact.
Mark – if you optimize the network to hide yourself, it is hard for the network to find you when you want it to. Privacy addressing complicates lots of other things.
Scott – within scopes. Tradeoffs – there are governments around the world defining privacy policies in various ways, and are taking actions. Outside authorities with very strong opinions
Mark – be careful what you ask for.
Jonne – is this for protocol designers or implementers?

Scott – Internet Architects
discuss on the ietf-privacy mailing list. Should merge into a more general IAB statement on privacy policy. Maybe rename the security section in RFC to "security and privacy considerations"

Renumbering Still Needs Work
RFC 5887
Brian Carpenter
what are we going to do about it? Is IPv4 a lost cause – focus on IPv6?
Jari – agree, still needs work. Promise that if there is interest on this, we will have an IETF activity on it.
If you care about this and would actually do something on it, please work with Brian
Fred – if you never have to renumber, avoid the problem. PI prefix.
Brian – some circumstances where PI still requires renumbering
Alain – renumber for privacy reasons too. Home gateway, local addresses before prefix, with limited scope this could be successful
Wes George – giving out too many PI results in route bloat
Mark T – load balancing with IPv4 LT2P, flash renumber the home, NAT hides it, but in IPv6 will be inconsistent.
Fred – scalable PI that doesn't harm route scaling.
continue on list.

IPv4 Rapid Deployment on IPv6 Infrastructures (4rd)
draft-vautrin-softwire-4rd-00
Remi Despres
reverse of 6rd – residual IPv4 via IPv6
4 ISPs intending to adopt 4rd
address sharing at optimized cost, and optimized routing.
encapsulated, stateless, via 4rd relay
ISPs committed, can IETF provide an agreed specification

Action Items: WGLC on IPv4-ID and router-alert, adoption of Alain,