Celebrando 10 Años 2005–2015

VOLUMEN 11, NÚMERO 2 • NOVIEMBRE 2015

# IETF® Journal

Informe sobre el IETF 93 realizado en Praga (República Checa) en julio de 2015. Publicado por la Internet Society en cooperación con el Grupo de Trabajo en Ingeniería de Internet.*

## EN ESTE NÚMERO

Palabras del Editor ..... 1
ACME: Mejor seguridad mediante la automatización... 1
Mensaje del Presidente del IETF ..... 2
Palabras del Presidente del IAB ..... 3
Se anticipa que las redes vehiculares salvarán vidas, aunque conllevan riesgos para la privacidad ..... 6
CrypTech en el IETF 93..... 9
Encuentro de Snowden con el Grupo de Trabajo en Ingeniería de Internet ..... 11
YANG y NETCONF/ RESTCONF ganan terreno en la industria ..... 12
Marcando tendencia: Resumen del IETF Hackathon..... 14
BoF IETF 93: EDUNEXT ..... 16
Nueva versión del sitio web del IETF: Primer vistazo en el IETF 93..... 17
Taller MaRNEW explora los desafíos del cifrado ..... 18
Informe del IRTF..... 19
Demostraciones en la sesión Bits-N-Bites: Demoras ultrabajas para todos..... 20
Anuncian los ganadores del premio ANRP..... 22
Modelado de redes basado en Internet ..... 23
Ornitología en el IETF: Avistamientos recientes..... 24
Síntesis del IETF 93 ..... 26
Calendario ..... 27

Internet Society™

# PALABRAS DEL EDITOR

*Por Mat Ford*

EL GRUPO DE TRABAJO EN INGENIERÍA DE INTERNET (IETF) REGRESÓ A LA imponente ciudad de Praga para nuestra 93.ª reunión, que fue organizada por Brocade y el registro de dominios de la República Checa, CZ.NIC. En este número del IETF Journal compartimos los aspectos más destacados de la reunión e intentamos transmitir el espíritu de las múltiples personas y discusiones que componen una reunión del IETF.

Nuestro artículo de portada presenta un informe sobre el nuevo y emocionante trabajo para simplificar el despliegue de tecnologías de seguridad en Internet. También incluimos un artículo sobre el IETF Hackathon (página 14), una gran introducción al creciente mundo de NETCONF y YANG (página 12), y un informe sobre la sesión de preguntas y respuestas en vivo con Edward Snowden que tuvo lugar a través de video antes de la reunión (página 11).

Puede averiguar qué ideas propuso la comunidad para mejorar los programas educativos y de mentores del IETF en nuestra lectura del BoF de EDUNEXT (página 16) y aprender acerca de una de las demostraciones de tecnología presentadas durante la sesión Bits-N-Bites (página 20).

El número se completa con nuestras columnas habituales de los presidentes del IETF, el IAB y el IRTF, además de la cobertura de temas de actualidad tratados durante las sesiones plenarias. Si desea leer más detalles sobre el Área de Internet del IETF, hay un informe resumido del Grupo de Trabajo disponible en https://wiki.tools.ietf.org/area/int/trac/wiki/IETF93.

Estamos enormemente agradecidos a todos nuestros colaboradores. Por favor envíe sus comentarios y sugerencias para el IETF Journal a ietfjournal@isoc.org. Para recibir la edición en papel o la versión por correo electrónico, escríbanos a https://www.internetsociety.org/publications/ietf-journal/ietf-journal-subscription.

# ACME: MEJOR SEGURIDAD MEDIANTE LA AUTOMATIZACIÓN

*Por Richard Barnes*

ES CADA VEZ MÁS IMPORTANTE ASEGURAR QUE TODAS LAS APLICACIONES DE INTERNET reciban ciertas garantías mínimas de seguridad [RFC 7202]. Desde hace muchos años, el IETF ha requerido que los protocolos que publica incorporen mecanismos de seguridad [RFC 3552]. Sin embargo, para que los usuarios se beneficien de ellos, estos mecanismos deben ser desplegados por quienes operan las aplicaciones de Internet.

*Continúa en la página 4.*

# MENSAJE DEL PRESIDENTE DEL IETF

*Por Jari Arkko*

Jari Arkko, Presidente del IETF

EL IETF 93 REALIZADO EN PRAGA BATIÓ RÉCORDS EN TÉRMINOS DE ASISTENCIA: 1384 personas de 65 países se hicieron presentes, mientras que muchos más participaron de forma remota. Aunque nuestras reuniones en Europa son siempre muy populares, este tipo de atención es un testimonio tanto de nuestro crecimiento como de la variedad de proyectos interesantes que están en marcha.

Otro aspecto llamativo de esta reunión fue la cantidad de código producido. El IETF Hackathon se realizó el fin de semana antes de la reunión (página 14); tantas personas se presentaron que apenas pudimos acomodarlas en una habitación. También tuvimos un ETSI Plugtest para probar implementaciones del protocolo 6TISCH, el Code Sprint para trabajar en herramientas para el IETF, y la reunión CrypTech para hackear diseños de hardware de código abierto (página 9). Estimo que más de 150 personas participaron en total. De ellas, muchas participaban de un IETF por primera vez, mientras que otras representaban a importantes proyectos de código abierto, como por ejemplo OpenDaylight, OPNFV y RIOT. Esperamos contar con más actividades de programación en las próximas reuniones. Cuando reserve sus pasajes para viajar a Yokohama, asegúrese de incluir tiempo para la programación durante el fin de semana anterior a la reunión: 31 de octubre - 1.º de noviembre.

**LA REUNIÓN IETF 93 celebrada en Praga fue un evento record... Aunque nuestras reuniones en Europa son siempre muy populares, este tipo de atención es un testimonio tanto de nuestro crecimiento como de la variedad de proyectos interesantes que están en marcha.**

La plenaria técnica del IAB trató las redes vehiculares (página 3). Christoph Sommer y William Whyte explicaron cómo se están desarrollando las redes vehiculares y los desafíos que generan en materia de seguridad. Este tema me resultó interesante, ya que recientemente he estado trabajando en algunos prototipos relacionados. Será fascinante ver cómo se desarrolla esta área en el futuro. Puedo ver tanto aplicaciones locales que se ejecutan entre vehículos como aplicaciones basadas en Internet que las utilizan para comunicarse con servidores basados en Internet o conectar vehículos.

Esta fue la primera reunión del Grupo de Trabajo NETVC. Este grupo trabaja en el desarrollo de códecs de video para aplicaciones de Internet, siendo los códecs la base para que navegadores y otras aplicaciones puedan intercambiar flujos de video de forma eficiente e interoperable. El trabajo sobre seguridad y privacidad continuó, tocando básicamente a todos los grupos de trabajo en cierta medida.

Esta vez el evento de Bits-N-Bites estuvo muy activo. Dediqué algún tiempo a tratar de comprender cómo podía instalar y probar uno de los proyectos de código abierto que participaron en el encuentro. Este es el tipo de cosa que hace que Bits-n-Bites sea excepcional: podemos hablar directamente con los líderes de las iniciativas y sus programadores y así obtener información de primera mano.

También pudimos observar cómo una reunión del IETF difiere intencionalmente de una conferencia tradicional de la industria. Aunque en algunas ferias todavía son habituales las promotoras, en esta ocasión no fueron recibidas como una adición constructiva a la sesión técnica de Bits-n-Bites. El IETF no fue lo suficientemente claro en cuanto a que esto no era apropiado. He pedido al Comité de Supervisión Administrativa del IETF que desarrolle políticas y prácticas

*Continúa en la página 5.*

La misión del Grupo de Trabajo en Ingeniería de Internet es hacer que Internet funcione mejor mediante la producción de documentos técnicos relevantes y de alta calidad que afecten la manera en al que la gente diseña, utiliza y gestiona Internet. Ver http://www.ietf.org.

**Acciones recientes de protocolo y de documento del IESG**

Puede consultar una lista completa de las últimas acciones de documento y de protocolo del IESG en https://datatracker.ietf.org/iesg/ann/new/

# PALABRAS DEL PRESIDENTE DEL IAB

*Por Andrew Sullivan*

Andrew Sullivan, Presidente del IAB

SIEMPRE ME SORPRENDE EL POCO TIEMPO QUE PARECE HABER ENTRE REUNIONES DEL IETF, al menos cuando ya la reunión se nos viene encima. El IETF 93 de Praga no fue la excepción. Aún así, el Consejo de Arquitectura de Internet (IAB) tuvo mucho para informar a la comunidad.

### Sesiones plenarias y vinculación del IAB con la comunidad

Hemos oído decir que las sesiones plenarias son demasiado largas e incluyen demasiados informes. No obstante, la plenaria, los informes que presentamos y nuestras sesiones de micrófono abierto son nuestros mecanismos básicos de rendición de cuentas. En Praga, los plenarios se realizaron por la mañana. Acortamos el plenario técnico en 30 minutos para permitir más "tiempo de pasillo", aunque la sesión resultó algo apretada. No obstante, en Yokohama vamos a intentarlo nuevamente, en un plenario combinado con el Grupo Directivo de Ingeniería de Internet (IESG). Si bien no esperamos hacerlo siempre, creemos que vale la pena probar estos diferentes enfoques para ver si nos podemos concentrar en el trabajo sobre los protocolos, mantener la semana de la reunión lo más corta posible y aún así vincularnos con la comunidad del IETF.

Uno de los trabajos del IAB consiste en ser la interfaz entre el IETF y los demás organismos de normalización. Fue un gusto para nosotros dar la bienvenida a Houlin Zhao, Secretario General de la Unión Internacional de Telecomunicaciones (UIT). No esperamos que otros organismos de normalización asistan al plenario técnico, por lo que nos alegró la presencia de Zhao y esperamos en el futuro una exitosa colaboración con la UIT.

**[C]reemos que vale la pena probar estos diferentes enfoques para ver si nos podemos concentrar en el trabajo sobre los protocolos, mantener la semana de la reunión lo más corta posible y aún así vincularnos con la comunidad del IETF.**

### Apelación

El IAB se ocupa de las apelaciones cuando una de las partes no está de acuerdo con una decisión del IESG con respecto de alguna apelación. El IAB se toma en serio este trabajo, parte del cual consiste en asegurarse de que los participantes trabajen dentro de los procesos del IETF. En este caso, el IAB concluyó que el apelante debía trabajar dentro de esos otros procesos. El texto completo de la decisión está disponible en https://www.iab.org/appeals/2015-2/response-draft-ietf-ianaplan-icg-response/.

### Cuando ustedes hablan, nosotros escuchamos

Dado que el IAB supervisa al Editor de Solicitudes de Comentarios (RFC) (a través del Programa de Editores de RFC y el Comité de Supervisión de la Serie de RFC), también publicamos los documentos relevantes para la serie de RFC. Un cambio reciente a la serie de RFC fue la adición de identificadores de objetos digitales (DOI). El IAB solicitó comentarios de forma temprana, pero los DOI se implementaron antes que el IAB procediera a publicar el draft-iab-doi-04. A muchos les pareció que el IAB simplemente estaba solicitando comentarios sobre un hecho consumado. Este no era el objetivo, a pesar de lo cual podríamos haber hecho mejor las cosas y estamos agradecidos por los comentarios. Este es el nuevo proceso que utilizaremos para desarrollar estas RFC:

1. La propuesta de cambio relevante será un Borrador de Internet (I-D) que describa el plan y así sucesivamente. A este lo procesaremos como cualquier otro documento del flujo del IAB, con el período de comentarios correspondiente. El borrador destacará las áreas que podrían variar debido a la implementación. Una vez finalizado el período de comentarios, procederemos a la publicación de la manera habitual (suponiendo que se justifique).

*Continúa en la página 5.*

El Consejo de Arquitectura de Internet se creó como un comité del IETF y como un cuerpo asesor de la Internet Society. Sus responsabilidades incluyen la supervisión de la arquitectura de las actividades del IETF, la supervisión y apelación del proceso de estándares de Internet y el nombramiento del Editor de las RFC. Ver http://www.iab.org.

*ACME: Mejor seguridad mediante la automatización, continúa de la página 1*

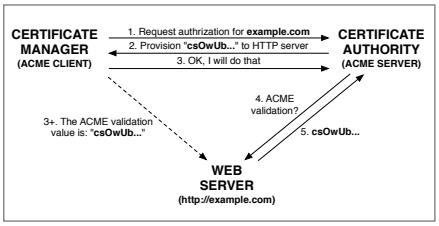
El despliegue de tecnologías de seguridad presenta diferentes desafíos importantes para los operadores. El requisito de autenticación del servidor en las aplicaciones de Internet es especialmente difícil para los operadores de servidores. La mayor parte de la autenticación del servidor se basa en la noción de un certificado digital [RFC 5280], una declaración firmada que asocia un nombre de dominio con la clave pública de un par clave pública / privada. Esta credencial es una declaración por parte de una autoridad de certificación (también llamada CA) que indica que el titular de la clave privada correspondiente puede representar legítimamente a dicha identidad.

Antes de hacer tal declaración, la autoridad de certificación debe comprobar que el titular de la clave privada sea también el titular de la identidad declarada; este proceso representa gran parte del costo y el riesgo asociados con la configuración de una aplicación segura de Internet.

Hoy en día este proceso se realiza de forma mayormente manual: Las pruebas informales de usabilidad realizadas por los autores indican que completar estos pasos le llevará a un administrador experto entre una y tres horas. Claramente, esto no se puede escalar para contextos que implican numerosos dominios o numerosos certificados para el mismo dominio.

Para lograr una seguridad más universal, el proceso de gestión de certificados debe ser automatizado. Necesitamos un único protocolo que se pueda integrar en los servidores de aplicaciones que requieren certificados, de modo que estos servidores se puedan autoconfigurar para un funcionamiento seguro.

Algunas autoridades de certificación sí exponen APIs para emisión automatizada que son adecuadas para algunos escenarios de emisión, como el servicio UniversalSSL de CloudFlare. Pero, hasta la fecha, estas API se han mantenido específicas para cada CA, lo que impide el desarrollo de herramientas que funcionen con múltiples CA. El Grupo de Trabajo ACME del IETF está trabajando en un protocolo común para la gestión de certificados, conocido como Entorno de Gestión Automatizada de Certificados (Automated Certificate Management Environment, ACME).




Resumen de cómo ACME valida la titularidad de un dominio

ACME es un sencillo protocolo cliente-servidor basado en HTTP. El cliente representa el solicitante de un certificado (por ejemplo, el operador de un servidor web); el servidor representa la autoridad de certificación. El objetivo de ACME es permitir que la CA verifique que el solicitante posee algunos dominios y luego habilitar al solicitante a pedir certificados para dichos dominios.

ACME utiliza un conjunto extensible de los así llamados desafíos para permitir que la CA verifique que un solicitante es el titular de un nombre de dominio. Cuando un solicitante pide autorización para un dominio, la CA lo desafía a hacer algo que solo el titular del dominio debería poder hacer:

- Suministrar un archivo a un directorio de un servidor web controlado por el administrador
- Suministrar un certificado para un host virtual HTTPS
- Suministrar un registro DNS

Una vez que el solicitante ha escogido un desafío y notificado a la CA, la CA verifica que el desafío se haya cumplido, por ejemplo, realizando una consulta HTTP o DNS para obtener el registro que se debería haber suministrado según el desafío escogido. Si se suministró el archivo o registro con el valor esperado, la CA sabe que el titular del dominio ha autorizado a este solicitante para que actúe en su nombre.

Tenga en cuenta que este proceso de desafío solo verifica que el solicitante tiene control práctico sobre un dominio, lo que no siempre es lo mismo que ser su titular. Por ejemplo, un proveedor de DNS o de alojamiento web podría utilizar estas técnicas para obtener certificados para el dominio de un cliente.

Además, dado que las consultas de validación de la CA se realizan a través de canales no seguros, la CA es vulnerable a cosas como los ataques de envenenamiento de DNS. Para bien o para mal, esto refleja el estado del arte actual de la infraestructura de clave pública (independientemente de ACME), por lo que al menos no es peor. Además, la estandarización que ofrece ACME podría facilitar la validación desde múltiples perspectivas, reduciendo así la posibilidad de que un atacante pueda demostrar falsamente su control de un dominio.

Una vez que el solicitante ha demostrado que tiene el control de un conjunto de dominios, la emisión de certificados es simple. El solicitante crea una solicitud de firma de certificado [RFC 2986] que expresa la clave pública y un conjunto de dominios que el certificado debe contener y luego la CA responde con el certificado.

La separación entre la autorización y la emisión de certificados significa que para un solicitante que tiene múltiples dominios es fácil combinar y mezclar nombres en diferentes certificados. Por ejemplo, un proveedor de alojamiento web que reúne veinte dominios en un servidor podría realizar una transacción de autorización para cada dominio y luego asignar dichos dominios a certificados de servidor en cualquier forma que tenga sentido para su entorno.

Todo este trabajo de automatización se realiza en una etapa temprana. ACME está siendo desplegado por *Let's Encript* (https://letsencrypt.org/), una autoridad de certificación recientemente incorporada al mercado, aunque probablemente necesitará algo de adaptación a través del proceso del IETF antes de poder ser adoptado por otras CA. Todavía hay muchas oportunidades para que las autoridades de certificación y quienes operan servidores contribuyan al grupo de trabajo para dar forma al protocolo ACME de manera que satisfaga sus necesidades.

*Mensaje del Presidente del IETF, continúa de la página 2*

para asegurar que para futuras reuniones existan directrices claras que comuniquen nuestras expectativas a los patrocinadores y expositores.

También nos visitó el Secretario General de la UIT, quien estivo presente en la sesión plenaria técnica. Houlin Zhao se puso la camiseta del IETF de su visita anterior; nosotros le regalamos una camiseta del Hackathon realizado en el marco de esta reunión. Me entusiasma tanto el foco que la UIT ha puesto en la programación como el espíritu de colaboración que Zhou claramente representa.

En paralelo al IETF 93 se proyectó la película *Citizenfour*, a la cual siguió una sesión de preguntas y respuestas con con Edward Snowden. Este fue un evento organizado por particulares fuera del programa del IETF.

CZ.NIC, nuestro patrocinador local, nos dio una cálida bienvenida checa en nuestro evento social realizado en el Palacio Žofín. ¡El evento terminó con fuegos artificiales!

Por último, quisiera dar las gracias a todos los participantes, a nuestros anfitriones CZ.NIC, a Brocade y a todos los demás patrocinadores por su ayuda para que el IETF 93 funcionara tan bien. Esta fue una de nuestras mejores reuniones. Como siempre, todavía queda mucho por hacer. La mayor parte del trabajo del IETF se lleva a cabo en las listas y a través de reuniones virtuales, por lo que es hora de volver a casa. Nuestra próxima reunión presencial será en Yokohama. Curiosamente, OpenStack y W3C también se van a reunir en la misma ciudad por la misma época, de modo que estoy buscando incluso más posibilidades de trabajo conjunto.

Fuegos artificiales durante el cierre del evento social realizado en el Palacio Žofín

*Palabras del Presidente del IAB, continúa de la página 3*

2. La implementación seguirá la RFC resultante, pero cualquier variación atribuible a la implementación será informada a la comunidad a través de las listas del IETF que corresponda.
3. Cuando todo esté listo, se preparará un nuevo I-D para dejar obsoleta la RFC anterior y documentar lo ocurrido. Para este se solicitarán comentarios de la comunidad para asegurarse de que coincida con lo que la gente piensa que se ha implementado.

Habrá más cambios a medida que la serie de RFC evolucione. Estamos prestando especial atención para garantizar la correcta gestión de este proceso.

### Otros hechos a destacar desde el IETF 92

El IAB hizo una declaración sobre el comercio en las tecnologías de seguridad y envió comentarios a la Oficina de Industria y Seguridad de Estados Unidos. El IAB también envió comentarios a la Oficina del Director de Tecnología de la Información de Estados Unidos y al Grupo de Trabajo Intercomunitario sobre Mejora de la Responsabilidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Realizamos este tipo de comunicaciones como parte de nuestro trabajo de interacción con organismos externos. Puede ver todas nuestras comunicaciones en https://www.iab.org/documents/correspondence-reports-documents/.

**A la larga, la respuesta a los ataque en Internet debe crecer tan vigorosamente como las capacidades de los atacantes.**

Junto con la Internet Society y en colaboración con FIRST 2015, el IAB patrocinó el taller sobre Coordinación de respuestas a ataques a escala de Internet (CARIS). El IAB participa en este tipo de talleres como parte de sus responsabilidades como enlace externo y porque se supone que debemos ofrecer orientación sobre la arquitectura de Internet. La respuesta a los ataques en Internet es una parte crítica del entorno operacional. El taller tuvo como objetivo fortalecer los vínculos entre las diferentes organizaciones que forman parte de la comunidad de respuestas a los ataques. A la larga, la respuesta a los ataque en Internet debe crecer tan vigorosamente como las capacidades de los atacantes. Kathleen Moriarty, uno de los Directores del Área de Seguridad y directora de programa del taller, presentó un informe rápido sobre el taller durante el plenario técnico del IETF 93. Puede buscar el Borrador de Internet correspondiente en cualquier repositorio de I-D.

El IAB también anunció el taller sobre Gestión de redes de radio en un mundo cifrado (MaRNEW) (ver página 18), que se llevó a cabo los días 24 y 25 de septiembre. El IAB seguirá compartiendo en el IETF 94.

### Referencias

[1] https://www.iab.org/documents/correspondence-reports-documents/2015-2/iab-statement-on-the-trade-in-security-technologies/.

# SE ANTICIPA QUE LAS REDES VEHICULARES SALVARÁN VIDAS, AUNQUE CONLLEVAN RIESGOS DE PRIVACIDAD

*Por Carolyn Duffy Marsan*

LOS SISTEMAS DE COMUNICACIÓN VEHICULAR PROMETEN EVITAR CHOQUES y salvar vidas. Estos sistemas estarán listos para su despliegue masivo en la próxima década. Durante la sesión plenaria técnica del IETF 93 se abordaron las tecnologías de red y los protocolos subyacentes que requieren las comunicaciones vehiculares, así como los desafíos de seguridad y privacidad relacionados.

Cristoph Sommer, profesor adjunto en la Universidad de Paderborn, abrió el debate presentando un breve panorama del estado actual de los sistemas de comunicación vehicular, incluidos los estándares que se han desarrollado para apoyar a estos sistemas y las pruebas de campo que se han realizado hasta la fecha.

Comunicaciones vehiculares se refiere a una serie de vehículos conectados en red que hablan entre sí y con nodos ubicados al borde de la carretera para proveer advertencias de seguridad e información sobre el tráfico. Por ejemplo, cuando un vehículo frena de repente, automáticamente se alertaría a los automóviles que viajan detrás para que se detengan y así evitar choques.

Sommer observó que la idea de los sistemas de comunicación vehiculares se remonta a la década de 1970, pero no fue hasta la popularización de las redes móviles en la década de 1990 que los sistemas como OnStar de General Motors y BMW Assist se volvieron viables.

“Después del año 2000, el importante aumento de la potencia de cálculo ha permitido desplegar sistemas *ad hoc* totalmente distribuidos y altamente reactivos que permiten que los automóviles se comuniquen directamente entre sí mientras están en la carretera”, dijo Sommer. “Esto generó una serie de actividades, incluso muchos programas de investigación coordinados... entre los más grandes fabricantes de Estados Unidos, Europa o Japón. El resultado fueron numerosas pruebas de campo a gran escala que concluyeron que esta tecnología es muy beneficiosa.”

**La Administración Nacional de Seguridad en el Tráfico Carretero (NHTSA) de Estados Unidos concluyó que dos aplicaciones sencillas... podrían evitar 500 000 choques y salvar 1000 vidas al año.**

La Administración Nacional de Seguridad en el Tráfico Carretero (NHTSA) de Estados Unidos concluyó que dos aplicaciones sencillas (movimiento en las intersecciones y asistencia en el giro a la izquierda) podrían evitar 500 000 choques y salvar 1000 vidas al año. En agosto de 2014, la NHTSA dijo que propondrá normas para que en 2020 todos los vehículos nuevos estén equipados con redes vehiculares. De hecho, algunos fabricantes de automóviles estadounidenses dicen que van a ofrecer esta tecnología tan pronto como en 2017.

Mientras tanto, innovadores como Google están desarrollando sistemas de conducción autónoma que permitirían que los automóviles se conduzcan a sí mismos o formen 'trenes de carretera' (*platoons*), es decir, un vehículo conducido por una persona seguido de cerca por varios automóviles conducidos de forma autónoma que aceleran o desaceleran en función de las acciones del automóvil 'líder'.

“Las redes de vehículos representan la tercera evolución en las redes”, comentó Sommer. “La primera fueron las redes cableadas tradicionales con configuraciones estáticas. La segunda fueron las redes móviles *ad hoc*, basadas en la tecnología móvil inalámbrica y la configuración dinámica. La tercera son las redes vehiculares *ad hoc*, que representan un campo de implementación totalmente nuevo”.

Ya se ha desarrollado el protocolo de red de nivel inferior para las comunicaciones vehiculares, el protocolo DSRC (Dedicated Short Range Communication), que es el “cable” sobre el que se sustentan estas aplicaciones. Este protocolo comprende extensiones para los estándares IEEE 802.11 para comunicación inalámbrica. Utiliza: 802.11e para calidad de servicio; 802.11j-2004 para operaciones a media velocidad, una forma de comunicación más robusta; y 802.11p para operación en la banda de 5.9 GHz y un nuevo modo llamado OCB (*Outside the Context of a Basic Service Set*).

“El modo OCB permite que en todo momento los dispositivos transmitan tramas dirigidas a un servicio genérico (*wildcard*) y que siempre reciban paquetes de servicios genéricos”, explicó Sommer.

Sommer agregó que la banda de 5.9 GHz está reservada para las comunicaciones vehiculares y que Estados Unidos dedica siete canales para estas comunicaciones y Europa cinco. Mientras que estos canales tienen no tienen costos de licenciamiento, sí tienen estrictas reglas de uso para garantizar que solo las redes vehiculares operen en estas frecuencias.

Sommer indicó que las comunicaciones basadas en IP solo son adecuadas en un pequeño espacio del paradigma de las redes vehiculares, ya que para la mayoría de las aplicaciones el enrutamiento es excesivamente costoso en términos de red. Según dijo, solo las aplicaciones de entretenimiento podrían soportar la transmisión de datos a los autos.

“Hay que ensamblar una nueva pila de protocolos que debe superar muchos retos de larga data —el multicast, la baja carga y la baja demora—, además de otros que son nuevos, como por ejemplo una topología altamente dinámica, la seguridad, el particionado y una movilidad compleja”, agregó Sommer.

Para superar los desafíos de las redes vehiculares se han desarrollado tres estándares:

- **El estándar IEEE 1609 WAVE (*Wireless Access in Vehicular Environments* o Acceso inalámbrico en entornos vehiculares), que está siendo adoptado en Estados Unidos.** La pila WAVE incluye: una capa física; una capa MAC (Media Access Control) con coordinación de canales, una capa LLC (Logical Link Control) y finalmente el WSMP (Wave Short Message Protocol). Sommer comentó que es posible que IPv6 y TCP/UDP puedan transportarse sobre la capa LLC, pero para que esto ocurra se necesita más trabajo. WAVE soporta dispositivos con una radio o con múltiples radios. Los dispositivos de una radio sintonizan periódicamente el canal de control (CCH) para garantizar la recepción de los mensajes importantes.
- **El estándar ETSI ITS G5 (*Intelligent Transportation Systems* o Sistemas de transporte inteligentes), que está siendo adoptado en Europa.** Este estándar se enfoca más en los escenarios multirradio en los que una radio siempre está sintonizada en el CCH. Esta pila incluye *Cooperative Awareness Messages*, es decir, mensajes periódicos que informan sobre la velocidad y la ubicación de los vehículos circundantes. La pila ITS G5 consiste en capas física y MAC basadas en la norma IEEE 802.11p, con control de congestión descentralizado (DCC) que se encarga de las tareas de gestión de tráfico para la capa de acceso, la capa de red y de transporte, y la capa de servicios (*facilities layer)*. Este estándar también incluye GeoNetworking, que permite la difusión de información a un área determinada por una latitud y longitud particulares.
- **El estándar ARIB T109 (Sistemas de transporte inteligentes en la banda de 700 MHz), diseñado en Japón.** Sommer no dio demasiados detalles sobre este estándar.

"Las perspectivas indican que en el futuro habrá múltiples aplicaciones para redes vehiculares, pero cada una estará diseñada a medida para un caso de uso específico y utilizará una parte muy diferente de la red", dijo Sommer.

Entre las aplicaciones para redes vehiculares que Sommer citó junto con los estándares correspondientes podemos mencionar: pagos electrónicos usando IEEE 1609.11; temporización de señales de tráfico usando SAE SPAT; transmisión periódica de mensajes de seguridad usando ETSI CAM e IEEE/SAE BSM; y transmisión geolocalizada de advertencias usando ETSI DENM.

"Aparte de todas estas aplicaciones, las redes vehiculares abren un montón de oportunidades, siendo una de las más importantes la fusión de la comunicación en el vehículo y la comunicación de vehículo a vehículo", dijo Sommer. "Esta será la primera vez que podamos fusionar los datos de los sensores locales de un vehículo con los datos de sensores de otros vehículos. Así, si otro automóvil me avisa que hay un obstáculo en el camino, yo podría intentar verificar esta información usando mi sistema de visión por computadora."

Después que Sommer concluyó su charla, William Whyte, Director Científico de Innovación en Seguridad, discutió los aspectos de seguridad y privacidad de las redes vehiculares.

Whyte observó que las redes vehiculares enfrentan los típicos problemas de seguridad que enfrentan todas las redes, como por ejemplo la confidencialidad, la integridad, la autenticidad, la autorización y el no repudio, así como requisitos de cifrado. Sin embargo, las redes vehiculares incorporan otras preocupaciones sobre la privacidad, como por ejemplo no querer habilitar el seguimiento o el análisis del tráfico.

Los participantes escuchan con atención durante una Sesión Plenaria Técnica del IAB a sala llena.

"La persona que tiene esta radio en su auto —se espera que en Estados Unidos los autos estarán obligados a contar con estas radios en 2020 o 2022— no quiere que la radio le ponga multas automáticas por exceso de velocidad. La gente no quiere que sea posible el seguimiento a gran escala", explicó Whyte.

Además, las redes vehiculares implican dispositivos con limitaciones en términos de tamaño, potencia, almacenamiento y conectividad, y esto limita las capacidades de seguridad basadas en hardware. Las comunicaciones están limitadas debido a que hay un número limitado de canales de 10 MHz.

"Si hay 200 o 300 vehículos en una zona y todos tienen que comunicarse a la vez, hay que asegurarse de que la sobrecarga producto de estas comunicaciones no sea excesiva", dijo Whyte.

Whyte identificó dentro del IETF varios esfuerzos relacionados con la seguridad que podrían superponerse con las redes vehiculares por el uso de certificados similares, la emisión automática y la gestión de certificados.

"Algo que espero que hagamos en los próximos años es trabajar más estrechamente con las tecnologías y los grupos de tecnología existentes para asegurarnos de no reinventar la rueda", agregó Whyte.

En cuanto al modelo de confianza de las redes vehiculares, el plan consiste en utilizar certificados IEEE 1609.2 y ETSI TS 103 097. Las unidades de datos de protocolo (también llamadas PDU) son autorizadas por certificados, con permisos de servicio específicos dentro de las aplicaciones. La autoridad de certificación verifica que el emisor tenga derecho a tales permisos. El receptor verifica que la PDU sea coherente con los permisos.

Por ejemplo, los vehículos de emergencia tendrían permisos especiales que les permitirían enviar mensajes a otros vehículos diciendo básicamente "déjame pasar", explicó Whyte.

*Continúa en la página siguiente*

*Se anticipa que las redes vehiculares salvarán vidas, aunque conllevan riesgos de privacidad, cont.*

En cuanto a su desempeño en materia de seguridad, los estándares de redes vehiculares utilizan el algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm) con curvas de 256 bits para el cifrado. Dado el elevado grado de seguridad de las firmas digitales, el IEEE permite certificados implícitos sin firmas explícitas para mejorar el desempeño, mientras que el ETSI solo utiliza certificados explícitos.

Otra preocupación relacionada con el desempeño es que el sistema puede manejar 600 mensajes entrantes por segundo. Mientras que la Unión Europea utiliza aceleración por hardware para mejorar el desempeño, Estados Unidos está filtrando los mensajes y utilizando claves efímeras, que son solicitudes por única vez para que la autoridad de certificación genere cierto número de certificados distintos.

Según dijo Whyte, para evitar el seguimiento de los vehículos se requerirá una nueva legislación. Una forma técnica que permitiría minimizar el seguimiento es que un vehículo reciba múltiples certificados para una aplicación de modo que se pueda rastrear *aquí* y *allá*, pero no en todos los puntos intermedios. Otra amenaza para la privacidad es que una persona con acceso a información privilegiada en la autoridad de certificación (CA) podría rastrear un vehículo, o bien que la CA podría ser vulnerada por un atacante.

Una precaución es que las redes vehiculares no revelarán información sobre los movimientos anteriores de un vehículo. “Si un auto es robado en junio, se lo podrá seguir de ahí en adelante, pero no se podrán conocer sus movimientos previos”, aclaró Whyte.

El modelo ETSI requiere que todos los paquetes enviados por geonetworking se firmen en la capa de geonetworking; esto indica que el emisor tiene los permisos necesarios para solicitar el reenvío de un paquete. Además, los paquetes se verifican antes de su reenvío. El hecho de evitar solicitudes de reenvío no autorizadas reduce la congestión.

En palabras de Whyte, “esta es una optimización más ya que, si de todos modos se está firmando en la capa de red, no será necesario que firme en la capa de aplicación”.

Las redes vehiculares transportan publicidad de diferentes servicios como un remolque de alta velocidad o la carga de vehículos eléctricos, pero los protocolos de red asumen una estrategia de tipo “el comprador deberá tener cuidado” (*buyer beware*). Además, si casi nadie utiliza un servicio, la privacidad del comprador podría estar en riesgo.

“Una de las áreas relacionadas con la privacidad que requieren mayor estudio es ... si una persona tiene múltiples aplicaciones tales que su combinación sea una huella digital para su dispositivo”, dijo Whyte. “El dispositivo debería soportar algún tipo de separación tal como un dispositivo virtual independiente para cada aplicación. Todavía está por verse si es que esto funciona.”

Según dijo Whyte, los desafíos clave para los sistemas de seguridad a la hora de preparar las redes vehiculares para su despliegue en la próxima década consisten en trabajar dentro de las limitaciones que imponen la capacidad del canal y el procesamiento, a la vez soportando diferentes niveles de confianza y protegiendo la privacidad contra probables ataques. Pero el futuro implica la integración de las redes vehiculares al marco de seguridad general de la Internet de las Cosas.

“Las redes vehiculares serán un subconjunto de sistemas de máquina a máquina; en general, pasaremos a sus marcos en los próximos años para asegurarnos de podemos crecer a la escala necesaria”, sostuvo Whyte. “Tenemos que gestionar la congestión en escenarios de confrontación, ya que los ataques de denegación de servicio podrían tener impactos reales en el futuro. Y debemos armonizar la política para definir cuáles aplicaciones pueden usar cuáles canales.”

Luego de las presentaciones formales, Russ Housley, miembro del IAB, moderó una sesión de preguntas y respuestas.

Allistair Woodman preguntó si la información recogida cuando un vehículo cruza un puente, atraviesa un túnel o paga un peaje puede ser citada y utilizada en contra del conductor.

“Los gobiernos son conscientes de que lo están exigiendo y observan con recelo las preocupaciones sobre la privacidad”, dijo Whyte. “En definitiva, el objetivo es salvar vidas. Si el uno por ciento de las personas lo apagan para evitar ser rastreados, habrá una caída del dos por ciento en la eficacia. Todo el mundo toma muy en serio la idea de que la información no será utilizada por la policía y no será exigible judicialmente.”

Christian Huitema preguntó si hay planes para llevar la tecnología desarrollada para las redes vehiculares a otros ámbitos como el IETF.

“Toda la tecnología es pública; ninguna está sujeta a patentes”, respondió Whyte. “Estamos construyendo una PKI que tenga capacidad de emitir 1000 certificados por año para cada vehículo circulando. Esta enorme escala debería poder soportar otros usos. Sería muy interesante explorar otros usos.”

Por último, Charlie Perkins preguntó si hay alguna diferencia en los protocolos de red para vehículos con o sin conductor.

“En la capa de aplicación habrá grandes diferencias según para quién sea la información, un vehículo autónomo o de un ser human”, dijo Sommer. “Pero en la capa física y la capa MAC esto no importa.”

### El Secretario General de la UIT comparte su visión

Al término de la sesión plenaria del IAB, Houlin Zhao, Secretario General de la UIT, se dirigió al público presente e hizo hincapié en la importancia de una fuerte relación entre la UIT y el IETF.

“Me gustaría fortalecer la cooperación entre la UIT y la Internet Society, el IETF, el IAB e ICANN para beneficio de nuestras familias globales”, dijo Zhao, y agregó que su foco está en ayudar a la gran cantidad de personas que todavía no son usuarios de Internet. “Los animo no solo a hablar de nuevas tecnologías para los que ya están conectados, sino también a encontrar innovaciones para quienes no están conectados con tecnologías físicas y sostenibles.”

# CRYPTECH EN EL IETF 93

*Por Karen O'Donoghue*

CUANDO SE PIENSA EN EL IETF, LA MAYORÍA DE LAS PERSONAS PIENSA EN software y protocolos; sin embargo, en el IETF 93 un taller CrypTech ofreció a los participantes la oportunidad de trabajar juntos en hardware de código abierto: motores criptográficos desarrollados por un equipo multinacional diseñado para restablecer la confianza del público en la criptografía.

**¿Qué es el Proyecto CrypTech?**

El proyecto CrypTech surgió en respuesta a la pérdida de confianza en los algoritmos criptográficos y los productos resultantes que se produjo a partir de las revelaciones sobre vigilancia omnipresente y algoritmos y productos potencialmente comprometidos. Se desarrolló a partir de los debates en la comunidad del IETF y el Consejo de Arquitectura de Internet (IAB).

CrypTech se fundó como un esfuerzo de desarrollo internacional independiente para crear diseños y prototipos de confianza para un motor de cifrado por hardware de código abierto y bajo costo. El primer producto de CrypTech será un diseño de referencia de confianza de un módulo de seguridad por hardware (HSM, un dispositivo especializado que se utiliza para almacenar de forma segura los pares de claves pública/privada que se usan con los certificados digitales más utilizados en SSL/TLS (capa de conexión segura/seguridad de la capa de transporte). El HSM de CrypTech se puede utilizar como base para el desarrollo de futuros productos comerciales; CrypTech apoya a la comunidad de Internet ofreciendo una alternativa abierta y auditable a los dispositivos criptográficos existentes. El primer caso de uso de CrypTech es para los HSM. Sin embargo, hay otras aplicaciones para este tipo de tecnología. El modelo de desarrollo de CrypTech se basa en un sistema modular que permite que el diseñador seleccione los componentes mínimos indispensables, reduciendo así todavía más el riesgo y la superficie de ataque de un dispositivo basado en CrypTech.

> **CrypTech apoya a la comunidad de Internet, ofreciendo una alternativa abierta y auditable a los dispositivos criptográficos existentes.**

CrypTech está empezando de abajo hacia arriba, implementando una amplia variedad de algoritmos criptográficos para cargar en una FPGA (Field Programmable Gate Array) especializada, diseñando el hardware necesario para un TRNG o generador de números aleatorios, desarrollando herramientas de auditoría y gestión de alta seguridad para las operaciones con clave y criptográficas, y produciendo el software de apoyo necesario para vincular el HSM de CrypTech a las aplicaciones de infraestructura de clave pública (PKI) existentes tales como DNSSEC y RPKI.

Al trasladar la investigación y el desarrollo (I+D) asociados con el hardware de PKI a la comunidad de Internet, CrypTech puede reducir drásticamente los costos. Esto le da a las empresas la oportunidad de hacer un uso mucho mayor del hardware criptográfico, lo que aumenta la seguridad general en comparación con la gestión de claves basada en software.

**¿Por qué hardware?**

El objetivo de CrypTech de diseñar un dispositivo criptográfico de hardware es mucho más complejo que el simple desarrollo de software de código abierto. Como el proyecto debe integrar componentes tanto de hardware como de software, también hay costos de materiales que no incurren los proyectos de código abierto. Por ejemplo, CrypTech tiene que construir un sistema inviolable, de modo que si el hardware cae en las manos equivocadas o sufre un ataque físico el dispositivo no libere el material criptográfico y de claves que contiene.

CrypTech también está construyendo un generador de números aleatorios verdaderos que para ser una fuente de "aleatoriedad" requiere algunos componentes de hardware especializados. Los expertos en criptografía siempre han sido críticos de los métodos algorítmicos de generación de números aleatorios; algunos algoritmos generadores de números aleatorios mal desarrollados han sido factores críticos en diferentes fallos de seguridad. Un generador de números aleatorios verdaderos es un elemento importante para una infraestructura de criptografía segura. El TRNG inicial de CrypTech ya ha sido probado por varias fuentes respetadas y los informes son increíblemente positivos.

El componente de hardware más


Stephen Farrell (centro), investigador en CONNECT, con otros participantes durante CrypTech en el IETF 93.

*Continúa en la página siguiente*

## ¿QUÉ ES UN HSM O MÓDULO DE SEGURIDAD DE HARDWARE?

Un módulo de seguridad de hardware (HSM) es un dispositivo especializado diseñado para almacenar de forma segura los pares de claves públicas/privadas que se utilizan con los certificados digitales. Un HSM proporciona agrega seguridad para la PKI y las autoridades de certificación (CAs) porque elimina la necesidad de almacenar claves en discos o en memoria y los riesgos que esto implica.

Cuando un HSM protege una clave privada, también debe ser poder realizar operaciones criptográficas con dichas claves. Por ejemplo, cuando una autoridad de certificación tiene que firmar un certificado digital, envía la información al HSM y solicita que el HSM cree la firma digital. El HSM firma el certificado y devuelve el resultado.

Almacenar las claves fuera del alcance de cualquier aplicación asegura que nunca estén expuestas fuera del HSM y que no puedan ser robadas, ya que no se pueden recuperar del HSM.

El HSM implementa una combinación de funciones de almacenamiento, cifrado y auditoría, entre ellas:

- Almacenamiento, respaldo y gestión de claves, incluida la resistencia a la manipulación del hardware.
- Procesamiento criptográfico acelerado, incluidos los algoritmos comunes de hash y de cifrado.
- Un generador de verdaderos números aleatorios.
- Gestión e integridad del sistema, incluida la generación de registros, su autenticación y auditoría.

*CrypTech en IETF 93, cont.*

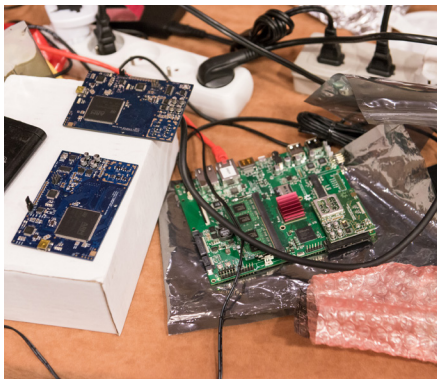
significativo del proyecto CrypTech es el uso de un FPGA para funciones criptográficas críticas. Cuando un algoritmo de cifrado o de hash se codifica en software y se integra en una unidad de procesamiento central (CPU) de propósito general, o se carga en una computadora de propósito general como por ejemplo un sistema Windows o Linux, dicho algoritmo sigue siendo muy vulnerable a los ataques. El software se puede modificar, a veces muy sutilmente. El contenido de la memoria puede ser leído durante las operaciones. Incluso se puede medir el tiempo que demoran las operaciones y así revelar información. Sin embargo, cuando el cifrado se realiza en un dispositivo de hardware dedicado y totalmente inaccesible para el sistema operativo normal, estas debilidades se reducen significativamente.

### CrypTech Workshop en el IETF 93

Desde sus inicios, el lema del IETF ha sido siempre “consenso aproximado y código que funciona”. El fin de semana anterior al IETF 93 se realizaron múltiples actividades que pusieron de relieve el desarrollo de software de código abierto funcional, entre ellas el Code Sprint, el Hackathon (página 14) y por último el taller CrypTech (www.cryptech.is). Todas estas actividades giraron en torno al software de código abierto, pero CrypTech también incluyó hardware de seguridad de código abierto.

Quienes participaron en el taller pudieron configurar su propio prototipo de hardware basado en diseños y software CrypTech. Los participantes pudieron inicializar los servicios criptográficos en el prototipo de hardware, configurarlo para utilizar PKCS11 para las comunicaciones a un servidor, configurar OpenDNSSEC para obtener sus claves del prototipo CrypTech y por último utilizar el sistema para firmar la zona DNSSEC.

En las sesiones del Grupo Asesor del Área de Seguridad del IETF (SAAG) y el Grupo de Investigación del *Crypto Forum* (CFRG) del IRFF se presentó un informe general sobre el proyecto CrypTech, incluidos los resultados del taller. Las detalladas



Hardware en uso durante el taller CrypTech en el IETF 93.

preguntas sobre el estado de implementación, entre ellas sobre su compatibilidad con ciertos algoritmos específicos, ilustraron el interés y la relevancia de la iniciativa.

Además, George Michaelson resumió su experiencia en el taller y compartió fotos en una detallada publicación en el blog de APNIC https://blog.apnic.net/2015/07/21/its-alive-blinkenlights-in-cryptech-ietf93/.

### La comunidad muestra su apoyo a CrypTech

El código abierto es una de las grandes historias de éxito de Internet —cualquier hardware o software producido hoy en día incluye software de código abierto—. Lo mismo ocurre con el proyecto CrypTech: al traer una filosofía de código abierto al software y hardware criptográfico, la idea es aumentar la confianza y la transparencia, ofrecer alternativas a los productos comerciales y reducir los costos. Para aprender más sobre CrypTech y cómo puede apoyar este importante esfuerzo, visite https://cryptech.is.

**Quienes participaron en el taller pudieron configurar su propio prototipo de hardware basado en diseños y software CrypTech.**

# ENCUENTRO DE SNOWDEN CON EL GRUPO DE TRABAJO EN INGENIERÍA DE INTERNET

*Por Mark Nottingham*

*En base a un artículo publicado el 20 de julio de 2015 en https://www.mnot.net/blog/2015/07/20/snowden_meets_the_ietf.*

DURANTE EL IETF 93, APROXIMADAMENTE 170 PARTICIPANTES ASISTIERON a la proyección de *Citizenfour,* la película sobre las revelaciones de Edward Snowden y la información que llevó al IETF a declarar esta vigilancia omnipresente como un ataque a la propia Internet. El público presente —las propias personas que diseñan y mantienen a la Internet— mantuvo sus ojos pegados a la pantalla; nadie abrió su computadora.

También tuvimos una visita sorpresa: Edward Snowden por video chat. Después de ser ovacionado de pie, Snowden compartió su perspectiva sobre la misma tecnología que estamos definiendo, desde DNSSEC y DANE hasta privacidad y WiFi. Respondió las preguntas del público y nos permitió un vistaso tanto a sus motivaciones como a las capacidades técnicas y modos de pensar de quienes realizan la vigilancia omnipresente.

Los miembros del público dijeron estar impresionados por la profundidad de su pensamiento. Varias veces advirtió en contra de una Internet "anti-NSA" (Administración de Seguridad Nacional de Estados Unidos); en cambio, dijo que nuestra atención debe centrarse en hacer del usuario nuestro principal interesado. Su declaración resonó especialmente en mí, ya que la semana pasada, cuando estábamos discutiendo el hallazgo de Unsanctioned Web Tracking (Seguimiento no autorizado en la web) en el TAG (Grupo de Arquitectura Técnica del W3C), Tim Berners-Lee nos exhortó a diseñar para la web que queremos, no solo paa la web que tenemos hoy.

### Cómo fue que ocurrió

Esto no fue un evento oficial del IETF, sino que fue un esfuerzo de muchas personas que, respetando las reglas, solicitaron un salón durante la reunión. Cuando empezamos a hablar de la idea, algunas personas no mostraron interés; pensaban que todos los que querían ver la película ya la habían visto. De hecho, recibimos donaciones suficientes para cubrir la proyección y hacer una donación de 670 euros a la Courage Foundation (https://courage-found.org/), un resultado fantástico.

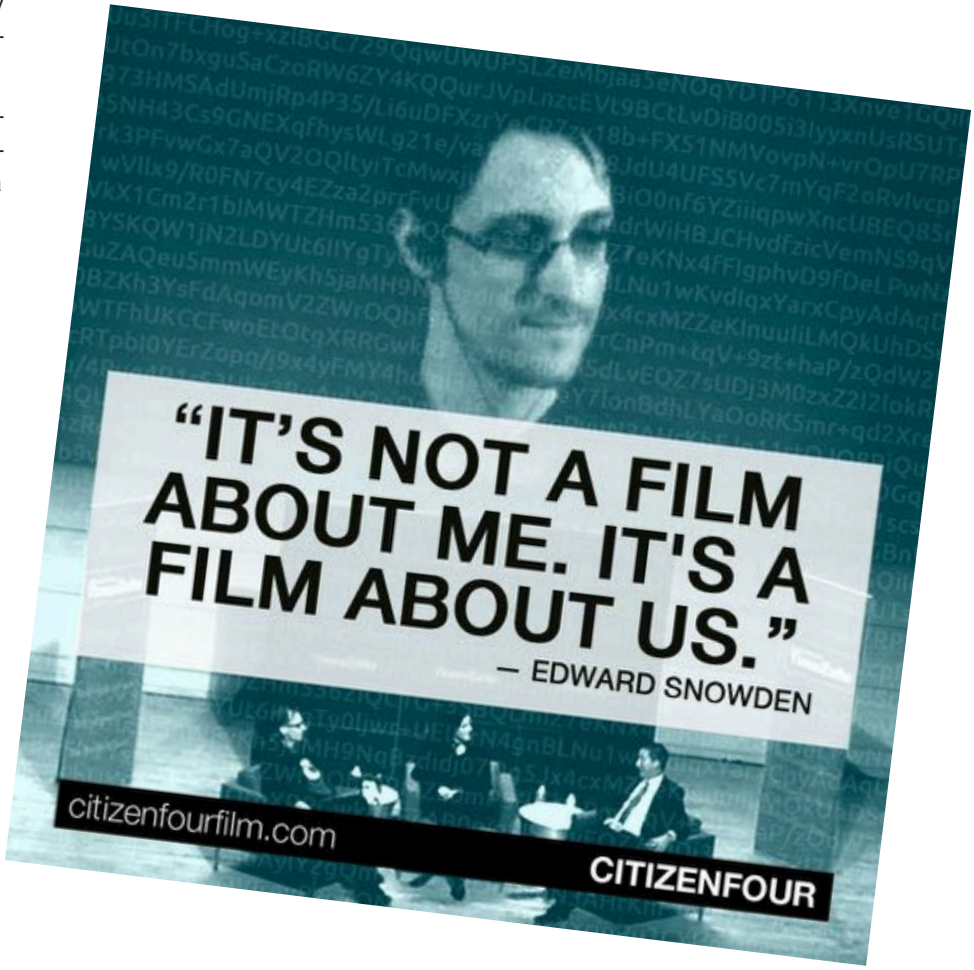
**Snowden compartió su perspectiva sobre la misma tecnología que estamos definiendo, desde DNSSEC y DANE hasta privacidad y WiFi.**

Muchas gracias a Daniel Kahn Gillmor por organizar la sesión de preguntas y respuestas y a Jake Applebaum y Laura Poitras por ayudarnos con la proyección.

### Enlaces

Video: https://www.youtube.com/watch?-v=0NvsUXBCeVA&feature=youtu.be

Transcripción: https://gist.github.com/mnot/382aca0b23b6bf082116a transcript



# YANG Y NETCONF/RESTCONF GANAN TERRENO EN LA INDUSTRIA

*Por Mahesh Jethanandani y Benoît Claise*

EN 2003, LA SOLICITUD DE COMENTARIOS (RFC) 3535, "OVERVIEW OF THE 2002 IAB Network Management Workshop"[1] documentó los resultados del diálogo que se dio entre operadores de redes y desarrolladores de protocolos sobre cuál debía ser el foco del trabajo futuro del IETF sobre gestión de redes. El taller identificó catorce requisitos de los operadores e identificó la 'facilidad de uso' como un requisito clave para cualquier nuevo sistema de gestión de redes. Esta facilidad de uso incluye la capacidad de gestionar una red (no solo un dispositivo en la misma) y afirma que debe haber una clara distinción entre la información de configuración y funcionamiento y la información estadística del dispositivo. Los requisitos también incluyen la posibilidad de montar una configuración, validarla antes de confirmarla, y revertir a la configuración anterior en caso de fallo.

Estos catorce requisitos de los operadores dieron lugar a la creación del Grupo de Trabajo NETCONF ese mismo año, el Grupo de Trabajo NETMOD en 2008 y el desarrollo de modelos de datos básicos para gestión de redes. El resultado del trabajo fueron las RFC 6241, 6242, 6243 y 6244 sobre el protocolo NETCONF (Network Configuration Protocol) basado en HTML en 2011 (revisadas respectivamente a partir de las 4741, 4742, 4743 y 4744), y las RFC 6020 y 6021 el lenguaje de modelado de datos asociado, YANG, en 2010.

En estos últimos años, NETCONF y YANG han ganado fuerza en la industria de las redes. Han pasado de la fase de definición a la fase de implementación. En el IETF, la cantidad de modelos YANG en fase de desarrollo ha crecido de forma increíble. Se están desarrollando nuevos modelos YANG en el área de Operaciones y Gestión (OPS), así como en las áreas de Enrutamiento (RTG), Internet (INT), Transporte (TSV) y Seguridad (SEC). Pero la adopción más notable de los modelos YANG llega desde el proyecto de código abierto OpenDaylight, donde a través de la versión Lithium se han publicado más de 480 modelos YANG[2].

Otros organismos de estandarización también han puesto en marcha proyectos de desarrollo de modelos YANG. Por ejemplo, el Metro Ethernet Forum fue un pionero al desarrollar modelos YANG para operación y mantenimiento de servicios (*Service OAM* o SOAM), gestión de fallas (*Fault Management* o FM) y gestión de performance (*Performance Management* o PM); actualmente este foro está trabajando en modelos YANG a nivel de servicio[3] (figura 1). Además, el Instituto de Ingeniería Eléctrica y Electrónica (IEEE) ha aprobado un proyecto para modelos 802.1x y 802.1q, con interés en desarrollar un modelo para 802.3. De manera similar, el Sector de Estandarización de la Unión Internacional de Telecomunicaciones (ITU-T) está detectando interés en el desarrollo de un modelo G.8032. En GitHub (https://github.com/YangModels/yang) se puede acceder a modelos de todos los organismos de estandarización.

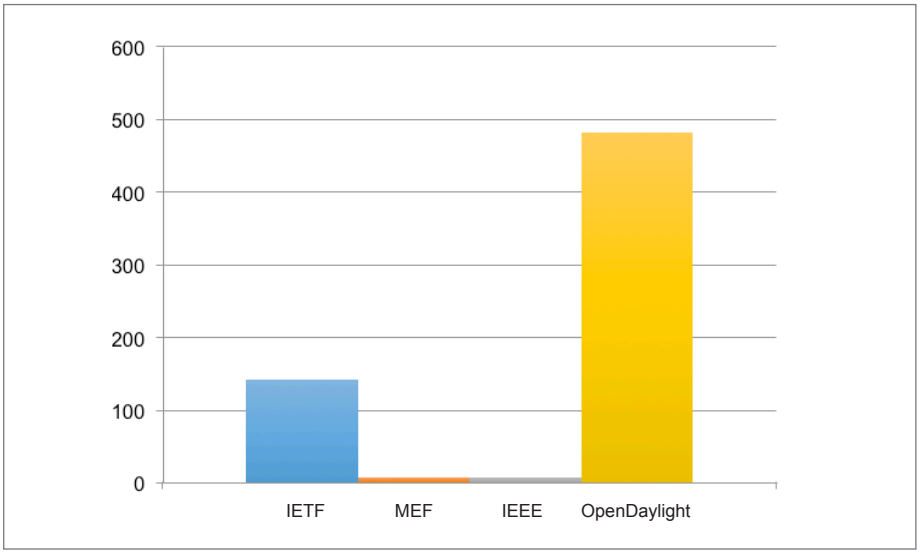



Figura 1. Modelos YANG en la industria

El rápido crecimiento de la cantidad de modelos YANG no está exento de desafíos, entre ellos su coordinación. Si bien todos los modelos hacen un gran trabajo al definir cómo se pueden configurar o supervisar determinadas características particulares, también deben interactuar con los modelos que se están desarrollando tanto en el IETF como en otros organismos de estandarización. La primera coordinación práctica la está realizado el Foro de Coordinación de YANG[4] en el área de enrutamiento. La coordinación del trabajo de desarrollo de YANG en el IETF y otros organismos de estandarización cae bajo el paraguas del director del Área de Operaciones y Gestión (OPS), Benoît Claise, con ayuda del Equipo de Coordinación de Modelos YANG[5].

Hay varios grupos de trabajo del IETF que abarcan diferentes aspectos del desarrollo de YANG:

- LIME (modelos YANG para OAM)
- L3SM (modelo YANG para servicios L3VPN)
- SUPA (modelos YANG para políticas coherentes)
- I2NSF (modelos YANG relacionados con la seguridad)

Para ayudar con el desarrollo de modelos YANG, los doctores[6] YANG se pueden contactar tanto a través del correo electrónico como durante la semana de las reuniones del IETF en las sesiones de asesoramiento/edición de YANG. Además, hay varias herramientas disponibles para desarrollar y compilar modelos YANG (ver una lista completa en http://trac.tools.ietf.org/area/

ops/trac/wiki/YangModelCoordGroup).

Probablemente la herramienta más importante sea pyang, una herramienta de compilación YANG basada en python que realiza una comprobación sintáctica y permite generar formatos de salida tales como UML, un modelo basado en árbol, YIN y así sucesivamente. Estas herramientas se deben ejecutar configurando la opción IETF para comprobar si cumplen con las directrices sobre YANG especificadas en la RFC 6087. Muchos modelos YANG todavía no compilan correctamente (ver http://www.claise.be/IETFYANGPageCompilation.html). En http://yangvalidator.com hay un equivalente gráfico de la herramienta pyang; toma un archivo YANG o un borrador o RFC del IETF, extrae el modelo y luego lo valida.

**El rápido crecimiento de los modelos YANG no está exento de desafíos, entre ellos su coordinación.**

Gracias a la extensión de la experiencia en el desarrollo y la implementación de algunos modelos YANG, el Grupo de Trabajo NETMOD ha estado recibiendo comentarios sobre YANG 1.0. Sobre la base de esta información, actualmente se está finalizando una versión YANG 1.1. Se trata de una versión de mantenimiento del lenguaje YANG que resuelve ambigüedades y defectos de la especificación original.

Con NETCONF y YANG especificados, los operadores pueden empezar a usarlos para la configuración y monitoreo. Sin embargo, algunos operadores ya han comenzado a utilizar las API REST propietarias que ofrecen diferentes proveedores para gestionar sus redes. RESTCONF es un protocolo tipo REST que corre sobre HTTP para acceder a los datos definidos en YANG. La API tipo REST no pretende reemplazar a NETCONF, sino que ofrece una interfaz simplificada que satisface una necesidad de quienes desarrollan aplicaciones. Por esta razón, el Grupo de Trabajo NETCONF decidió incorporar en su charter el apoyo al protocolo RESTCONF. RESTCONF soporta dos formatos de codificación: XML y JSON.

Aunque muchas veces esta capacidad se pasa por alto, los dispositivos también pueden enviar notificaciones definidas en el modelo YANG. NETCONF recientemente adoptó un charter que incluye una actualización de las notificaciones de eventos NETCONF[7] y el desarrollo de un mecanismo tipo *subscription-and-push* que permite que las aplicaciones cliente soliciten notificaciones sobre cambios en el repositorio de datos. Estas capacidades abrirán NETCONF al mundo de telemetría: empuje (pushing) de datos hacia las aplicaciones del sistema de gestión de redes (NMS).

Una de las consecuencias de la popularidad de YANG es que ahora los operadores que desean desarrollar su propio protocolo para gestión utilizan YANG como lenguaje de modelado de datos. Esto incluye CoMI, que define una interfaz de gestión para dispositivos limitados. Incluso entre los protocolos existentes NETCONF y RESTCONF hay diferentes codificaciones para modelos YANG (por ejemplo, XML y JSON).

En definitiva, lo que cuenta son los modelos de datos. La industria tiene una clara necesidad de contar con modelos de datos estándares para facilitar la gestión y más precisamente la capacidad de ser programadas de las redes de múltiples proveedores. YANG claramente se ha posicionado como *el* lenguaje de modelado de datos para estos modelos estándares. Si queremos que funcionen juntos sin problemas, coordinar todos los modelos YANG está en manos del IETF.

### Referencias


1 http://tools.ietf.org/html/rfc3535.

2 http://www.claise.be/YANGPageMain.html.

3 https://wiki.mef.net/ (requires login).

4 http://trac.tools.ietf.org/area/rtg/trac/wiki/RtgYangCoord.

5 http://www.ietf.org/iesg/directorate/yang-model-coordination-group.html.

6 http://www.ietf.org/iesg/directorate/yang-doctors.html.

7 http://datatracker.ietf.org/doc/rfc5277/.

# MARCANDO TENDENCIAS: RESUMEN DEL IETF HACKATHON

*Por Charles Eckel*

*Publicado originalmente en https://communities.cisco.com/community/developer/opensource/blog/2015/08/03/going-mainstream--recap-of-ietf-93-hackathon.*

EL IETF 93 DE PRAGA ARRANCÓ CON UN HACKATHON EL FIN DE SEMANA DEL 18 AL 19 DE julio. Tras el éxito del primer Hackathon IETF que se llevó a cabo en el IETF 92, Cisco DevNet y el IETF se unieron una vez más para organizar este evento.

Más de 135 participantes se reunieron en 18 equipos y trabajaron en 15 tecnologías diferentes. Entre los participantes vimos muchas personas que participaban de una reunión del IETF por primera vez y de diferentes universidades y comunidades de código abierto. Esto nos alegró sobremanera, ya que los objetivos declarados de la Hackathon son traer el "running code" o código en funcionamiento de regreso al IETF, cerrar la brecha entre el código abierto y los estándares abiertos, y atraer a más desarrolladores y personas jóvenes al IETF. Por estas y por otras razones, el Hackathon fue un enorme éxito y quedó establecido como una valiosa adición para la comunidad del IETF de cara al futuro.

El Hackathon incluyó tecnología relevante a muchos grupos de trabajo del IETF (por ejemplo, 6TISCH, ACE, BIER, DANE, HOMENET, HTTPBIS, MPTCP, NETVC, NETCONF, SFC y SIDR) y los correspondientes proyecto de código abierto (por ejemplo, Dalla, Kea, OpenDaylight, OpenDNSSEC, OPNFV, Quagga, RIOT y SPUDlib).

### ¿Cómo funciona?

El evento comenzó a las 9:00, cuando los promotores de cada tecnología procedieron a presentarlas y propusieron proyectos a modo de ejemplo. A continuación, promotores y participantes se organizaron en equipos, algunos de los cuales incluyeron a participantes de múltiples grupos de trabajo del IETF y comunidades de código abierto. Esta mezcla de personas, ideas y culturas dio lugar a algunos de los proyectos más interesantes y destacó la posibilidad de lograr beneficios a largo plazo que se extiendan mucho más allá de lo que se logró ese fin de semana.


Entre los premios en juego para quienes participaron había una serie de Raspberry Pi.

La energía en la sala era contagiosa. Motivados por aspiraciones altruistas, los participantes trabajaron cooperativa y diligentemente para desarrollar los estándares que constituyen los cimientos de Internet, así como las implementaciones de código abierto que validan estos estándares y hacen que sean más fáciles de usar.

Quienes no tenían otras actividades en el IETF se quedaron a cenar y muchos trabajaron hasta altas horas de la noche, mucho más allá del horario de cierre previsto para las 21:00. Pero, claro, esto no quiere decir que el día no tuvo diversión.

El día siguiente no se había perdido el entusiasmo: muchos llegaron antes de la hora de inicio señalada para las 9:00. También se hicieron presentes algunas caras nuevas, que fueron muy bien recibidas y se incorporaron a equipos existentes o nuevos.

### Las presentaciones

A media tarde del domingo, los equipos presentaron sus logros a los jueces: Jari Arkko, presidente del IETF; Ray Pelletier, director administrativo del IETF; Rick Tywoniak, director de Cisco DevNet; y Martin Thomson, autor de borradores e incansable colaborador del IETF. Los jueces debieron enfrentar una tarea poco envidiable dada la gran variedad de proyectos, entre ellos pruebas, experimentos, implementaciones de protocolos y nuevos servicios. En juego estaban el orgullo de los participantes y la posibilidad de ser los primeros en llevarse los últimos *gadgets* como Raspberry Pi, Arduinos y accesorios para la Internet de las Cosas, además de invitaciones donadas por Brocade para asistir al evento social de la IETF.

Entre los ganadores hubo tres proyectos a los cuales el jurado reconoció como los mejores:

- ACE – Premio a la tecnología clave
- DNSSEC – Premio a la mayor cobertura
- HOMENET – Premio a la mejor característica para enrutador WiFi y Premio "Cool Kids"

**Los resultados y perspectivas de los proyectos sirvieron como insumos para las sesiones de los grupos de trabajo que se llevaron a cabo durante toda la semana.**

Los participantes del Hackathon trabajaron en forma colaborativa y en equipos.


Participantes del segundo Hackathon del IETF presentando su trabajo.

**Por estas y por otras razones, el Hackathon fue un enorme éxito y quedó establecido como una valiosa adición para la comunidad del IETF de cara al futuro.**

### Bits-N-Bites

La ceremonia de premiación dio fin al Hackathon, pero la recompensa por todo el trabajo realizado aún estaba por llegar. Los proyectos del Hackathon se compartieron de manera más amplia con la comunidad del IETF en una sesión muy concurrida de Bits-N-Bites.

Los resultados y perspectivas derivadas de los proyectos sirvieron como insumos para las sesiones de los grupos de trabajo que se llevaron a cabo durante toda la semana. Uno de los mejores ejemplos fue la reunión del Grupo de Trabajo NETVC. De acuerdo con Nathan Egge de Mozilla, "En el transcurso de dos días un equipo de 11 participantes (tanto presenciales como remotos) hackearon las bases de código Thor y Daala, dos códecs de vídeo de código abierto aportados por Cisco y Mozilla, respectivamente, al Trabajo Grupo NETVC. Los resultados del Hackathon incluyeron la adición de soporte para Thor al entorno de pruebas AreWeCompressedYet.com, la realización de cuatro experimentos utilizando la compensación de movimiento de Thor dentro de Daala, y la reparación de un problema de larga data en Daala mediante el agregado del filtro de postprocesamiento CLP de Thor. Cisco confirmó cambios al código de Daala y Mozilla al de Thor, lo que demuestra el espíritu de colaboración del IETF. Organizar un Hackathon es una excelente manera de probar nuevas ideas en código funcional, por lo que NETVC volverá para el Hackathon del IETF 94 que se realizará en Yokohama."

Junto con fotografías y un resumen del evento en video, todas las tecnologías y proyectos están disponibles en el evento Wiki en https://www.ietf.org/registration/MeetingWiki/wiki/93hackathon.

Desde la página principal del Hackathon (https://www.ietf.org/hackathon/) es fácil navegar hasta la información sobre todos los Hackathons del IETF. Alentamos a las comunidades del IETF y el código abierto a consultar estos sitios, que podrán encontrar de utilidad para sus trabajos en curso.

### ¿Y ahora qué?

El IETF ya ha anunciado un Hackathon para el IETF 94 a realizarse en Yokohama y Cisco DevNet ya ha confirmado nuevamente su patrocinio. Además, el Hackathon es ahora parte habitual de las reuniones del IETF. Hay oportunidades de patrocinio disponibles para quienes deseen mostrar su apoyo a este importante esfuerzo. Para obtener más información, comuníquese con Ray Pelletier.

### Manténgase al tanto

Para mantenerse al tanto de las Hackathons pasadas y futuras del IETF, suscríbase a hackathon@ietf.org.

Algunos participantes creían no están a la altura de las circunstancias, pero su trabajo demostró que estaban equivocados.

# BOF IETF 93: EDUNEXT

*Por Mirjam Kuehne*

EN EL *IETF JOURNAL,* VOLUMEN 10, NUMERO 1, ESCRIBÍ SOBRE LAS ACTIVIDades del Equipo de Educación del IETF (http://ietf.org/edu/). Desde entonces, además de organizar los tutoriales del domingo y las sesiones para los *chairs* de los grupos de trabajo, hemos revisado nuestra oferta, nuestros métodos de capacitación, el público al que llegamos y los temas que hemos abarcado. Esto planteó una serie de preguntas: ¿Debemos mantener los tutoriales del día domingo? ¿Deberíamos ofrecer más capacitación en línea en forma de videos temáticos cortos? ¿Son los webinars la mejor opción a futuro? ¿Cómo podemos llegar a otros públicos, por ejemplo a la comunidad de código abierto? ¿Debemos revisar nuestro *charter* o ya cubre tanto las actividades que desarrollamos actualmente como posibles cambios y ajustes futuros? Por último y más importante todavía, algunos miembros del Equipo de Educación se retirarán pronto. ¿Cómo haremos para encontrar nuevos miembros?

**Además de organizar los tutoriales del domingo y las sesiones para los *chairs* de los grupos de trabajo, hemos revisado nuestra oferta, nuestros métodos de capacitación, el público al que hemos llegado y los temas que hemos abarcado.**

Además, hemos comenzado a colaborar más con el programa de mentores del IETF y a buscar diferentes formas de colaborar más eficazmente y compartir recursos. ¿Tendría sentido fusionar el Equipo de Educación y el programa de mentores?

Nuestras discusiones culminaron tanto en la organización de la sesión *Birds-of-a-Feather* (BoF) EDUNEXT que se llevó a cabo en el IETF 93 y que presidimos junto con Dan Romascanu, y un Borrador de Internet que escribimos junto con Nalini Elkins en preparación para el BoF.

El principal objetivo del BoF sobre EDUNEXT era recoger los aportes de la comunidad sobre las preguntas mencionadas, tanto para el Equipo de Educación como para el programa de mentores. El BoF tuvo una muy buena concurrencia y comenzó con una descripción de las actividades del Equipo de Educación y el programa de mentores (una iniciativa mucho más reciente). El resto del tiempo, las discusiones fueron activas, por momentos intensas y hasta caóticas. Fue muy bueno ver la pasión de los participantes por el IETF, el intercambio de conocimientos y la integración de los recién llegados al proceso. Varios recién llegados también compartieron sus experiencias; todos alguna vez estuvimos en su lugar y seguramente recordamos lo que se siente al asistir por primera vez a una reunión del IETF. ¡Yo lo recuerdo muy bien!

La mayor parte de la sesión se dedicó al programa de tutoría, una iniciativa reciente que todavía está definiendo su misión y objetivos. Pero, el Equipo de Educación también tuvo bastante atención. Por ejemplo, surgieron ideas interesantes sobre tutorías regionales y centros de formación a distancia. Al finalizar la sesión tuvimos respuestas a la mayoría de las preguntas que habíamos planteado al comienzo del BoF.

- Mantener los tutoriales del domingo, pero considerar la posibilidad de ofrecer sesiones de capacitación más cortas (menos de dos horas de duración).
- El *charter* del Equipo de Educación es bueno. Permite tanto tutoriales orientados a procesos como tutoriales técnicos, por lo que no fue necesario modificarlo.
- Continuar ofreciendo tutoriales técnicos (no solo orientados a los procesos).
- No apuntar solamente a los recién llegados; apuntar también a los participantes existentes, a quienes presiden los grupos de trabajo y a los directores de área.
- Considerar la posibilidad de ofrecer contenido que se adapte mejor a la modalidad de aprendizaje a distancia, como por ejemplo videos y webinars.
- Recoger más comentarios después de cada tutorial.
- Realizar un seguimiento de los recién llegados después de sus primeras reuniones del IETF para averiguar qué funcionó para ellos y qué no.

Hubo la fuerte sensación de que en este momento el Equipo de Educación no debe fusionarse con el programa de mentores. En primer lugar, el programa de mentores debe definir mejor sus objetivos y necesita tanto un *charter* como una lista de correo. Además, los participantes sintieron que

Mirjam Kuehne, presidente del BoF EDUNEXT, presenta el afiche del BoF.

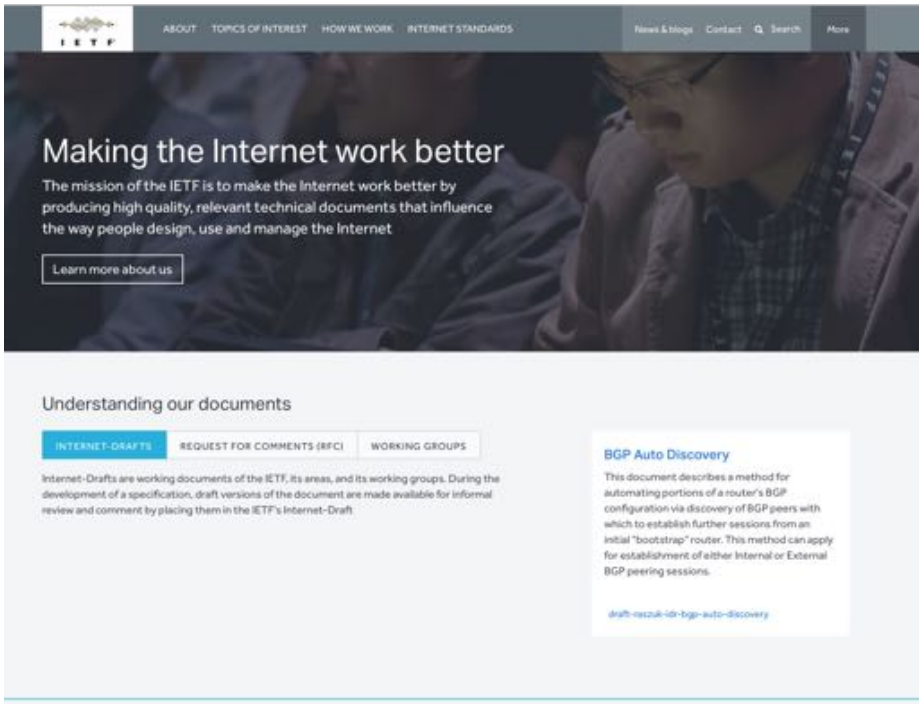
**Varios recién llegados también compartieron sus experiencias; todos alguna vez estuvimos en su lugar y seguramente recordamos lo que se siente al asistir por primera vez a una reunión del IETF. ¡Yo lo recuerdo muy bien!**

no estaba claro qué necesitan quienes se acercan al IETF por primera vez. Hay más de un tipo de nuevo participante —cada persona llega al IETF con diferentes antecedentes y objetivos. Jari Arkko, presidente del IETF y director del área que supervisa las actividades del Equipo de Educación y el programa de mentores, trabajará con el equipo de mentores para definir mejor sus actividades.

Durante todo el proceso, Arkko se mostró muy comprensivo y dispuesto a colaborar. Es bueno ver que nuestras actividades son consideradas valiosas y útiles y que son cada vez más visibles en la estructura general del IETF.

Me alegra mucho haber encontrado a dos nuevos miembros: Karen O'Donoghue y Dan Romascanu. Nalini Elkins se quedará en el equipo de Educación para asegurar que continúe la colaboración entre el programa de mentores y el Equipo. Y Greg Wood aceptó formar parte del Equipo de Educación durante el proceso de reestructuración del sitio web dek IETF (y esperemos que por más tiempo también). Puede consultar una lista de los miembros del Equipo de Educación en http://ietf.org/edu/team-members.html.

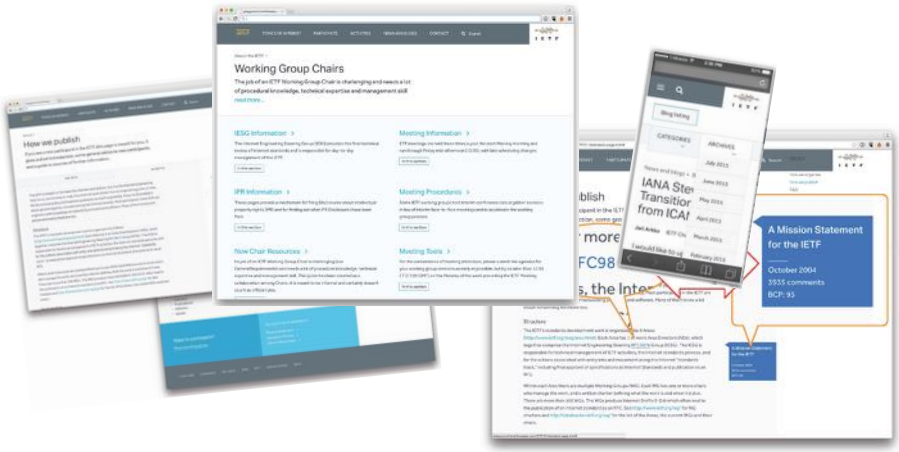
Gracias a todos quienes participaron en los preparativos y en la sesión BoF. Gracias también por las excelentes sugerencias. Por favor, no duden en comunicarse con nosotros escribiendo a edu-team@ietf.org para hacernos llegar sus preguntas, comentarios, preocupaciones, críticas o sugerencias. También se puede acceder a una lista de correo en edu-discuss@ietf.org.




# NUEVA VERSIÓN DEL SITIO WEB DEL IETF: PRIMER VISTAZO EN EL IETF 93

DURANTE EL PLENARIO ADMINISTRATIVO DEL IETF 93, LOS MIEMBROS DE LA COMUNIDAD pudieron echar un primer vistazo al nuevo sitio web del IETF (https://www.ietf.org). El diseño se desarrolló en base a datos sobre la utilización de la actual página web del IETF, el aporte del público objetivo y consultas con el Comité de Revisión de la Comunidad del IETF. El nuevo diseño busca ser ampliamente utilizable, accesible a través de dispositivos móviles y compatible con conexiones de red de bajo ancho de banda / alta latencia.

Torchbox, el proveedor con sede en el Reino Unido seleccionado para el proyecto, estuvo presente en el IETF 93 para responder las preguntas de quienes asistieron a la reunión. El proyecto sigue el calendario previsto y se espera desplegar el sitio final después del IETF 94. Mientras tanto, se está trabajando para continuar probando el diseño y su accesibilidad y para migrar el contenido a la nueva plataforma. De acuerdo con el cronograma actual, la nueva página web estará funcionando a principios de 2016.



# EL TALLER MARNEW EXPLORA LOS DESAFÍOS DEL CIFRADO

*Por Karen O'Donoghue*

HACE TIEMPO QUE EL IETF Y EL IAB SE DEDICAN A ACTIVIDADES TENDIENTES a reconstruir la confianza de los usuarios y a fortalecer Internet en vista del monitoreo omnipresente y la existencia de productos con potenciales vulnerabilidades. El taller MaRNEW (*Managing Radio Networks in an Encrypted World*, Gestión de redes de radio en un mundo cifrado) (https://www.iab.org/activities/workshops/marnew/) fue la última de una serie de actividades colaborativas.

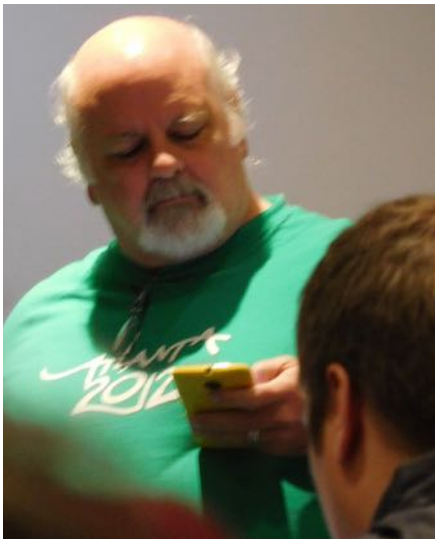
En noviembre de 2014, el Consejo de Arquitectura de Internet (IAB, www.iab.org) hizo pública una Declaración sobre Confidencialidad de Internet (https://www.iab.org/2014/11/14/iab-state-ment-on-internet-confidentiality/). Esta declaración alentaba el uso generalizado del cifrado para garantizar la confidencialidad y mejorar la seguridad global de Internet. Una preocupación que surgió en relación con esta declaración era la posible dificultad de desplegar el cifrado de forma generalizada. La mayoría de estas preocupaciones parecían exageradas. La cantidad de cifrado desplegado parece estar creciendo de manera constante en la mayoría de los escenarios de implementación. Sin embargo, en los entornos móviles la preocupación persiste. El taller MaRNEW reunió a las comunidades del IETF y el Groupe Speciale Mobile Asociación (GSMA) para discutir estos desafíos y explorar posibles soluciones a corto plazo y largo plazo.

Jianjie You, panelista del taller de MaRNEW, comparte sus observaciones con los participantes.

Celebrada en Atlanta, Georgia, el 24 y 25 de septiembre de 2015, el taller fue patrocinado conjuntamente por el IAB, la Internet Society (www.internetsociety.org), AT&T (www.att.com) y la GSMA (www.gsma.com). Aproximadamente 50 expertos de todo el mundo, representantes de una variedad de grupos, entre ellos proveedores de navegadores, proveedores de contenido, redes de distribución de contenido, proveedores de equipos y operadores de telefonía móvil, se reunieron para comprender mejor los desafíos únicos que presenta el entorno móvil y explorar diferentes maneras de abordarlos.

**[E]l problema no es el cifrado en sí, sino que las técnicas actuales de gestión y optimización no funcionan bien (o no funcionan en absoluto) en presencia de cifrado. Se necesitan nuevas formas de optimizar la experiencia del cliente.**

El taller comenzó con algunas discusiones introductorias: un panorama general y antecedentes del proceso de las comunidades tanto del IETF como de la GSMA, seguidos por una sesión dedicada a consideraciones sobre el despliegue desde los puntos de vista del IETF y la GSMA. A continuación se llevó a cabo una sesión sobre modelos de confianza y elección de los usuarios que exploró algunas perspectivas



Spencer Dawkins, Director de Área del IETF, consulta sus notas mientras modera un panel en el taller MaRNEW.

y posibles compromisos. Las dos sesiones siguientes exploraron el envío de datos en todas direcciones en beneficio de la gestión de redes. Estas fueron seguidas por sesiones sobre modelos de aplicación, cuestiones de transporte, y políticas y regulación. Las primeras sesiones presentaron múltiples desafíos y todos los caminos parecían conducir a cuestiones relacionadas con el transporte. Sin embargo, hacia el final del segundo día surgieron varios temas clave.

### Temas clave

Una observación importante fue que el problema no es el cifrado en sí, sino que las técnicas actuales de gestión y optimización no funcionan bien (o no funcionan en absoluto) en presencia de cifrado. Se necesitan nuevas formas de optimizar la experiencia del cliente. Como soluciones clave se identificaron temas como la gestión cooperativa de recursos y la mejora de las redes de distribución de contenido (CDN). Como trabajo a corto plazo se identificó un posible nuevo protocolo para SSL sin clave que facilite el despliegue de redes de distribución de contenido distribuidas.

También se destacó el hecho de que el problema no se comprende completamente y que sería útil contar con otras mediciones y datos que caractericen cómo funcionan los diferentes enfoques de optimización. Se discutió un marco para la

*Fotos MaRNEW: Olaf Kolkman*

recopilación y el intercambio de datos operativos. La línea de base contra la cual se medirían las nuevas soluciones son los algoritmos de gestión de recursos utilizados en un mundo sin cifrado. Hay una fuerte necesidad de mejorar las herramientas de prueba y análisis.

### Próximos pasos

Las actas del taller estarán disponibles a principios de noviembre en el sitio web del taller MaRNEW (https://www.iab.org/activities/workshops/marnew/). Está prevista la publicación de un informe borrador a fin de año. Este informe también estará disponible en el sitio web de MaRNEW. En la reunión del Grupo Asesor del Área de Seguridad (SAAG) que se realizará durante la próxima reunión del IETF (IETF 94, Yokohama) se discutirá un informe preliminar del taller.

Mientras se aguarda la publicación de estos informes y análisis más completos, ya se han difundido un par de resúmenes preliminares. Natasha Rooney, *co-chair* del taller, preparó un resumen para el blog del IETF disponible en http://www.ietf.org/blog/2015/09/impressions-from-the-marnew-workshop/. También Dirk Kutscher —activo participante en el taller— publicó su perspectiva sobre el taller en ttp://dirk-kutscher.info/publications/managing-radio-networks-in-an-encrypted-world-2/.

Las siguientes referencias presentan las perspectivas de la GSMA y W3C:

- "Network Management of Encrypted Traffic," GSMA, febrero de 2015, http://www.gsma.com/newsroom/wp-content/uploads/WWG-04-v1-0.pdf.
- W3C Tag Finding, “Securing the Web”, enero de 2015, https://w3ctag.github.io/web-https/.

Con todo, fueron dos días de intensas discusiones al final de los cuales hubo consenso general sobre algunos elementos de trabajo a corto plazo y la necesidad de continuar la discusión y el análisis.

# INFORME DEL IRTF

*Por Lars Eggert*

OCHO DE LOS NUEVE GRUPOS DE INVESTIGACIÓN ya creados en el Grupo de Trabajo para Investigación sobre Internet (IRTF) se reunieron durante el IETF realizado en Praga:

- Crypto Forum (CFRG)
- Acceso global a Internet para todos (GAIA)
- Control de la congestión en Internet (ICCRG)
- Redes centradas en la información (ICNRG)
- Virtualización de funciones de red (NFVRG)
- Gestión de redes (NMRG)
- Codificación de redes (NWCRG)
- Redes definidas por software (SDNRG)

Además de las reuniones de los grupos de investigación que ya recibieron su charter, también se reunieron tres grupos de investigación propuestos. El grupo de investigación propuesto sobre consideraciones sobre los Derechos Humanos en los protocolos (HRPC) tuvo su segunda reunión pública. El grupo de investigación propuesto llamado “Thing-to-Thing” (T2TRG) y relacionado con las redes para la Internet de las Cosas mantuvo una segunda reunión, más larga, el fin de semana anterior al IETF, además de una reunión más corta durante la semana. Por último, en su primer reunión presencial, el tercer grupo de investigación propuesto, ¿Qué tan osificada está la pila de protocolos? (HOPSRG), discutió sobre mediciones.

Haya Shulman y João Luís Sobrinho, ganadores del premio ANRP 2015.

En la Reunión Abierta del IRTF, dos de los cinco ganadores del Premio IRTF 2015 a la investigación aplicada en redes (ANRP) presentó su investigación: Haya Shulman analizó las deficiencias de los enfoques de privacidad del Sistema de nombres de dominio (DNS); João Luís Sobrinho diseñó una técnica de agregación de rutas que permite filtrar respetando las políticas de enrutamiento. En la página 22 encontrará más información sobre los ganadores del premio ANRP.

El período de nominaciones para los Premios ANRP 2016 ya está cerrado. El premio ANRP a la investigación aplicada en redes se otorga a resultados recientes relevantes para llevar al mercado productos de Internet y esfuerzos de estandarización relacionados. Le animamos a nominar artículos científicos relevantes que haya escrito o leído recientemente para su consideración. Consulte los detalles en https://irtf.org/anrp.

**Manténgase al tanto de estos y otros acontecimientos sumándose a la lista de discusión del IRTF en www.irtf.org/mailman/listinfo/irtf-discuss.**

# DEMOSTRACIONES EN LA SESIÓN DE BITS-N-BITES: DEMORAS ULTRABAJAS PARA TODOS

*Por Bob Briscoe*

EN LA SESIÓN DE BITS-N-BITES REALIZADA EN PRAGA DURANTE EL IETF 93 se demostró algo bastante notable: la transmisión de un partido de fútbol que se podía desplazar, acercar y alejar sobre una pantalla táctil con gestos de los dedos —y obtener HD (alta definición) incluso con el máximo acercamiento—. La aplicación en sí estaba muy buena, pero lo más notable era su capacidad de respuesta: parecía pegarse al dedo a medida que el usuario acercaba o desplazaba la imagen. Como era de esperar, los asistentes tuvieron buenas preguntas para los responsables: Reducir la Latencia del Transporte de Internet (RLTI o RITE), un equipo de investigadores europeos cuyo objetivo es eliminar las causas raíz de la latencia innecesaria en Internet. La iniciativa es financiada por la Comisión Europea en el marco del programa FP7-ICT.


Figura 1. Vistas solicitadas y presentadas

**¿Se almacenaba en caché localmente?**

No. Cada cliente enviaba los movimientos de los dedos a un proxy remoto, que generaba la escena HD sobre la marcha para ese usuario desde un video panorámico de todo el estadio.

**¿Se trataba solamente de un cable corto?**

No. A principios de la semana ya se había demostrado la misma tecnología en el Grupo de Trabajo sobre gestión activa de colas (AQM) usando un acceso remoto al banco de pruebas de banda ancha de Bell Labs. Allí estaban transmitiendo desde un proxy en un centro de datos a una red domiciliaria a través de un núcleo real, transporte (*backhaul*) y el equipamiento de la linea digital del abonado (DSL) con una demora total de ida y vuelta de 7 ms, el tipo de demora base que debería tener hasta su red de entrega de contenido (CDN) local. Para Bits-N-Bites, estaban utilizando NetEm emular la misma demora.

**¿Era calidad de servicio (QoS) basada en servicios diferenciados (Diffserv)?**

No. Eso era lo más notable. Diffserv solo entrega QoS a algunos a expensas de otros. Esto era para todo el tráfico, incluso en alta carga. Un panel de control permitía hacer clic y agregar hasta 100 flujos web paralelos por segundo; además, era posible iniciar decenas de descargas para agregar así aún más carga. No solo las funciones de desplazamiento y acercamiento mantenían su capacidad de respuesta, sino que una gráfica en el panel de control indicaba que los demás flujos veían el mismo retardo de encolamiento ultrabajo. Media el retardo de encolamiento de cada paquete, no solo del video sino de todos los flujos y descargas web. El peor retardo era tan bajo que casi no se podía ver su gráfica: apenas un par de píxeles.

**Un panel de control permitía hacer clic y agregar hasta 100 flujos web paralelos por segundo; además, era posible iniciar decenas de descargas para agregar así aún más carga.**

**¿Se habían configurado buffers muy pequeños?**

No. El panel de control mostraba que se utilizaba todo el enlace.

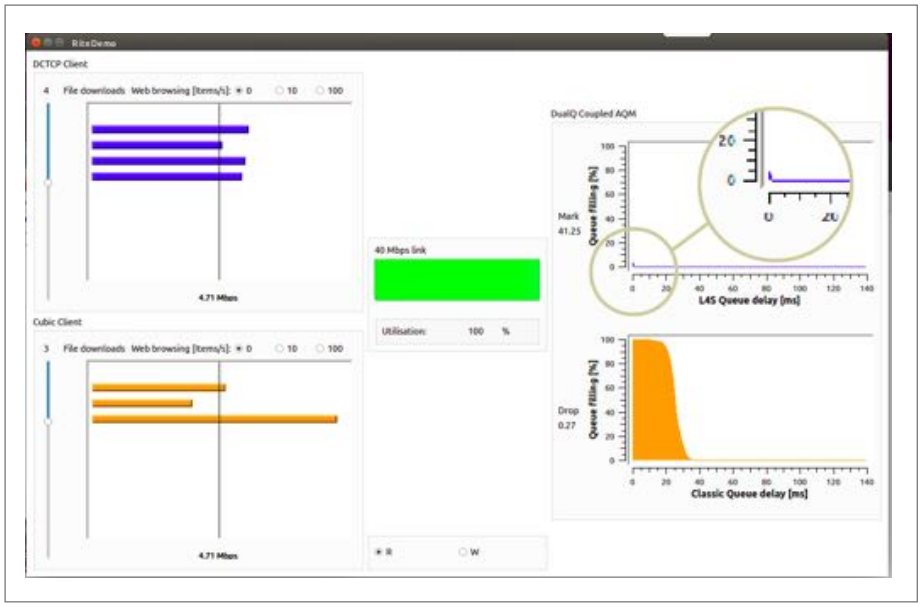



Figura 2. Vista del panel de control

**Entonces, ¿cuál era era el secreto?**

En pocas palabras, lo que hacían era no utilizar el protocolo de control de transmisión (TCP) habitual (ni New Reno, ni Cubic). En vez de ello, habían cambiado las pilas en los dos extremos por lo que llamaron un TCP escalable, sin necesidad de cambiar las aplicaciones. Dijeron que cualquier TCP escalable funcionaría, siempre que también utilizara notificación explícita de congestión (ECN). Como TCP escalable estaban utilizando Data Centre TCP (DCTCP) no modificado, que Microsoft desplegó a partir de Windows Server 8 y del cual también existe una versión para Linux.

Luego habían configurado la cola del cuello de botella para que marcara con ECN los paquetes por encima de un umbral de ocupación bajo. Típicamente, la capacidad del enlace de acceso es el cuello de botella en DSL, cable y celular. Así, para el caso del DSL de bajada solo necesitaban este marcado en la puerta de enlace de banda ancha (BNG, también conocida como, BRAS o MSE). Lo mismo hace falta en la puerta de enlace hogareña para resolver también el caso de la subida.

**¿Despliegue incremental?**

¿Sería posible tener esta maravilla en la Internet pública? Seguramente cualquier flujo TCP "clásico" de los equipos más antiguos introduciría un retardo de encolamiento que arruinaría la experiencia de los demás. Además, los TCP "escalables" son mucho más agresivos que los TCP clásicos. Por lo tanto, cuando ambos compitieran, sería de esperar que los TCP clásicos apenas obtendrían pequeña parte de la capacidad.

Aquí fue donde la demostración se puso muy interesante. Usando el panel de control también se podían agregar flujos clásicos. Pero esto no afectó en absoluto el retardo de encolamiento ultrabajo de los paquetes escalables. Y tampoco se comprometió el retardo de encolamiento de los flujos clásicos: este retardo no era peor de lo que hubiera sido si toda la carga hubiera sido clásica.

Más impresionante todavía, todos los flujos aún se repartían la capacidad en forma más o menos equitativa, como si todos

**¿Sería posible tener esta maravilla en la Internet pública? Seguramente cualquier flujo TCP clásico de los equipos más antiguos introduciría un retardo de encolamiento que arruinaría la experiencia de los demás.**

fueran del mismo tipo de TCP. Pero no había ninguna programación por flujo; de hecho, no estaban inspeccionando nada por encima de la capa del protocolo de Internet (IP).

**¿Cómo lo hicieron?**

Clasificaron el tráfico clásico en una cola separada para evitar que retrasara el tráfico escalable. Luego, acoplaron el descarte y el marcado con ECN de los paquetes entre las dos colas, marcando los flujos escalables de forma más agresiva para contrarrestar exactamente su respuesta más agresiva a las marcas. Esto requería una relación cuadrática que codificaron de manera muy astuta: simplemente compararon el tiempo en cola contra un número aleatorio para el marcado y contra dos para descarte. Para esto tienen un buena ayuda memoria: "Hay que pensarlo dos veces antes de descartar un paquete"

**¿Ocaso del protocolo TCP?**

Cuando el IETF inició sus esfuerzos en el área de las comunicaciones en tiempo real en los navegadores web (RTCWEB) allá por 2012, ya se sabía que el retardo de encolamiento y su variación (*jitter*) solían degradar las RTCWEB. Un taller del Consejo de Arquitectura de Internet (IAB) dio lugar a la creación de los grupos de trabajo sobre técnicas para evitar la congestión en RTP (RMCAT) y gestión activa de colas (AQM). Las RMCAT evitarían que el tráfico en tiempo real empeorara el problema, mientras que la AQM al menos eliminaría las colas innecesariamente largas ocupándose de lo que se conoce como *buffer-bloat* (exceso de buffers). Pero el verdadero problema era el protocolo TCP. El encolamiento por flujo se incluyó en el charter del Grupo de Trabajo sobre AQM como una forma de aislar los flujos sensibles al retardo y separarlos de los flujos TCP, pero resultó estar plagado de problemas, dado que la red tendría que identificar los flujos de la capa de transporte y decidir sobre sus tasas relativas de uso conjunto, por no hablar del costo adicional —mil y pico de colas adicionales para un típico acceso residencial—.

La tecnología mostrada en Praga nos ofrece un nuevo componente, usando solo dos colas; una especie de membrana semipermeable que particiona el retardo perjudicial del TCP clásico sin prejuzgar dónde particionar el ancho de banda.

La demostración mostró que Internet podría ser mucho mejor sin el TCP clásico. Mostró que ya existe una clase escalable superior de algoritmos TCP. Y mostró el camino para llegar desde aquí hasta allí. Fue una muestra del IETF en su mejor momento.

Para obtener más información sobre RITE puede dirigirse a http://riteproject.eu.

**La tecnología mostrada en Praga nos ofrece un nuevo componente, usando solo dos colas; una especie de membrana semipermeable que particiona el retardo perjudicial del TCP clásico sin prejuzgar dónde particionar el ancho de banda.**

João Luís Sobrinho, ganador del premio ANRP 2015

Haya Shulman, ganadora del premio ANRP 2015

# ANUNCIAN LOS GANADORES DEL PREMIO ANRP A LA INVESTIGACIÓN APLICADA EN REDES

*Por Mat Ford*

EL PREMIO ANRP A LA INVESTIGACIÓN APLICADA EN REDES SE OTORGA A resultados recientes relevantes para llevar al mercado productos de Internet y esfuerzos de estandarización relacionados. Durante el IETF 93 dos personas recibieron este premio:

- **Haya Shulman.** Por su análisis de los enfoques sobre privacidad en el DNS en el trabajo titulado “Pretty Bad Privacy: Pitfalls of DNS Encryption”.

  El trabajo completo está disponible en https://www.ietf.org/mail-archive/web/dns-privacy/current/pdfWqAIUmEl47.pdf.

- **João Luís Sobrinho.** Por diseñar una técnica de agregación de rutas que permite el filtrado respetando las políticas de enrutamiento en el trabajo “Distributed Route Aggregation on the Global Network”.

  El trabajo completo está disponible en http://www.cs.princeton.edu/~jrex/papers/dragon14.pdf.

Shulman y Sobrinho presentaron sus conclusiones en la reunión abierta del Grupo de Trabajo para Investigación sobre Internet durante el IETF 93.

Las presentaciones están disponibles en https://www.ietf.org/proceedings/93/slides/slides-93-irtfopen-1.pdf y https://www.ietf.org/proceedings/93/slides/slides-93-irtfopen-0.pdf.

Gracias a Meetecho, el audio y el video de las presentaciones están disponibles en http://recordings.conf.meetecho.com/Playout/watch.jsp?recording=IETF93_IRTFOPEN&chapter=chapter_1 (a partir de00:17:45).

**El período de nominaciones para los Premios ANRP 2016 ya está cerrado.** Los ganadores del premio ANRP 2016 se anunciarán antes de cada una de las tres reuniones del IETF programadas para el año próximo. Suscríbase a la lista de correo irtf-announce@irtf.org para recibir todas las notificaciones relacionadas con este premio.

# MODELADO DE REDES BASADO EN INTERNET

*Por Bert Wijnen, Tianran Zhou, Susan Hares y Pedro A. Aranda Gutiérrez*

LOS PROPONENTES DEL MODELADO DE REDES BASADO EN INTERNET (IBNEMO) ORGANIZARON DOS REUNIONES *bar-BoF* en Praga durante el IETF 93. Muchas personas tienen interés en estandarizar un lenguaje mínimo capaz de expresar intención en la configuración de redes y están trabajando en este tema a través de diferentes proyectos usando la plataforma OpenDayLight. Nuestro objetivo es definir un conjunto mínimo de comandos que pueda cubrir el 80 por ciento de las expresiones de intención que se necesitan en las configuraciones de red (figura 1).

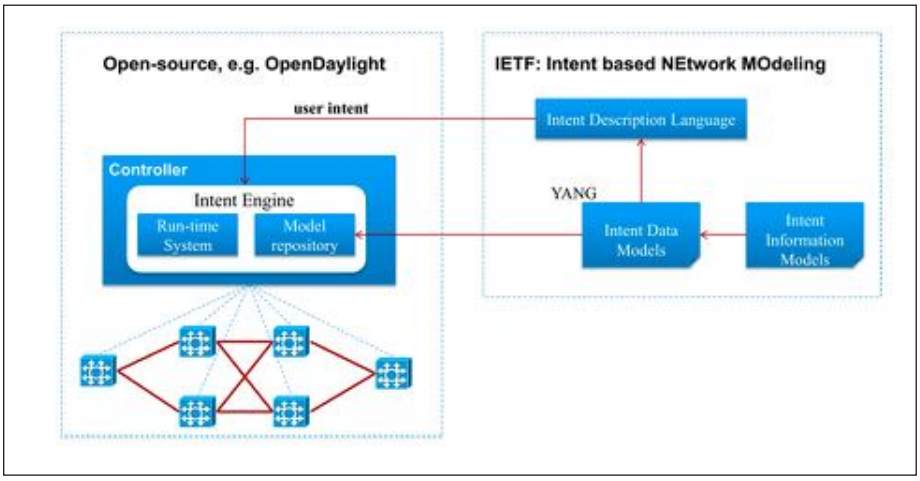



Figura 1. El conjunto mínimo de comandos que puede cubrir el 80 por ciento de las expresiones de intención que se necesitan en las configuraciones de red

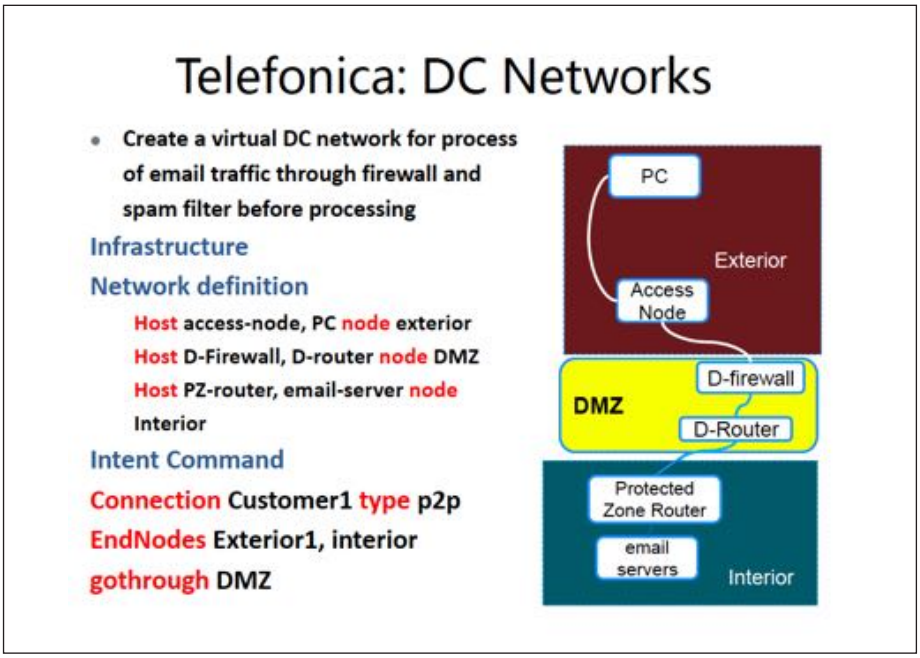



Figura 2. Ejemplo de IBNEMO operativo en el contexto de NetIDE, un proyecto de investigación colaborativo financiado por la Unión Europea

**Muchas personas tienen interés en estandarizar un lenguaje mínimo capaz de expresar intención en la configuración de redes y están trabajando en este tema.**

En https://tools.ietf.org/html/draft-hares-ibnemo-overview-00 el lector encontrará un Borrador de Internet que incluye una descripción general de IBNEMO y un planteo del problema.

Entre 15 y 20 personas participaron en cada una de las dos sesiones. Sue Hares presentó el tema, explicó los objetivos de IBNEMO y presentó su Borrador de Internet. El Dr. Pedro A. Aranda Gutiérrez de I+D de Telefónica compartió un ejemplo de IBNEMO operativo en el contexto de NetIDE, un proyecto de investigación colaborativo financiado por la Unión Europea (figura 2). Además, Tianran Zhou de Huawei demostró una implementación temprana de IBNEMO.

Se plantearon una serie de preguntas interesantes que a su vez nos animaron a ayudar a los recién llegados a comprender mejor esta tecnología. También concluimos que es necesario generar mayor conciencia e interés en la tecnología antes de intentar establecer un grupo de trabajo dentro del IETF.

Si le interesa la tecnología IBNEMO, puede unirse a nuestra lista de correo disponible en https://www.ietf.org/mailman/listinfo/ibnemo. En https://mailarchive.ietf.org/arch/msg/ibnemo/69t80ww_gkWuEuxetugQxkgMSlg el lector encontrará un informe completo del *bar-BoF*.

Planeamos organizar presentaciones o reuniones BoF en las reuniones de RIPE y NANOG para correr la voz sobre este trabaj novedoso e interesante.

**El Proyecto NetIDE es cofinanciado por DG CONNECT en el FP7 de la Comisión Europea bajo el acuerdo de subvención 619543.*

# ORNITOLOGÍA EN EL IETF: AVISTAMIENTOS RECIENTES

*Compilado por Mat Ford*

Para lograr que comience un nuevo trabajo en el IETF por lo general se requiere una reunión BoF (Birds-of-a-Feather) para discutir las metas del trabajo, la idoneidad del IETF como lugar para desarrollarlo, además del nivel de interés y apoyo con que se cuenta. En este artículo se revisan los BoF que tuvieron lugar durante el IETF 93 y se presentan sus objetivos y resultados. Si desea organizar una reunión BoF, por favor lea la RFC 5434, Consideraciones para organizar una reunión BoF exitosa.

### Interacción con portales cautivos (capport)

**Descripción:** Muchos lugares como hoteles, cafeterías, etc. utilizan portales cautivos para controlar el acceso inalámbrico a Internet. La actual tendencia hacia una Internet más segura significa que las técnicas de intercepción empleadas por estos portales se vuelven cada vez más problemáticas. La experiencia del usuario también deja mucho que desear. En esta reunión BoF se intentó determinar si hay energía suficiente para trabajar en el problema y diseñar un protocolo de interacción con los portales cautivos.

**Actas:** https://www.ietf.org/proceedings/93/minutes/minutes-93-capport

**Resultados:** La reunión atrajo a una cantidad de técnicos y expertos que trabajan en el desarrollo de código para portales cautivos o sistemas operativos que deben tratar con portales cautivos. Se requiere un mayor esfuerzo tanto para reducir el alcance del problema como para obtener más datos sobre los tipos de portales cautivos y la extensión de su despliegue. Un documento con una taxonomía podría ser un buen primer paso.

### Educación y mentores, siguiente generación (edunext)

**Descripción:** El objetivo de esta reunión fue recabar opiniones sobre la futura dirección de las actividades educativas (http://www.ietf.org/edu/) y los mentores (https://www.ietf.org/resources/mentoring-program.html) del IETF.

**Actas:** https://www.ietf.org/proceedings/93/minutes/minutes-93-edunext

**Resultados:** Se propusieron y discutieron muchas buenas ideas para mejorar los programas tanto de educación como de mentores. En el artículo de la página 16 encontrará más detalles sobre el tema.

### Redes determinísticas (detnet)

**Descripción:** El Grupo de Trabajo 802 del Instituto de Ingeniería Eléctrica y Electrónica (IEEE) ha definido *Audio Video Bridging* como “la provisión de sincronización temporal y programación (*scheduling*) de precisión para lograr cero pérdidas por congestión y latencia finita en flujos de capa 2 reservados”. Ahora la necesidad de contar con características de calidad de servicio (QoS) también aparece en las redes que, además o en lugar de pasarelas (*bridges*), incluyen routers (por ejemplo, aplicaciones industriales, vehiculares y de infraestructura pública). Los objetivos de esta reunión fueron analizar la posibilidad de formar un grupo de trabajo junto con el Grupo de Trabajo IEEE802.1TSN y especificar tanto cómo introducir estas características de QoS en los routers como la forma en que se podrían usar protocolos de control nuevos y/o existentes para controlar estos flujos.

**Actas:** https://www.ietf.org/proceedings/93/minutes/minutes-93-detnet

**Resultados:** Una reunión muy concurrida que apoyó firmemente la necesidad de contar con estándares abiertos en este espacio. Se identificó y discutió un gran número de casos de uso, que llevaron a plantear algunas preocupaciones acerca de la necesidad de limitar el alcance de los elementos de trabajo propuestos para hacerlos más manejables. Los participantes mostraron su apoyo a que el IETF trabaje sobre el problema en un Grupo de Trabajo sobre DETNET. (El charter del DETNET WG se aprobó

*European Goldfinch (Carduelis carduelis)*

Eurasian Kestrel
(Falco tinnunculus)

el 5 de octubre de 2015, http://datatracker.ietf.org/wg/detnet/charter/.)

### Uso simplificado de politicas abstractas (supa)

**Descripción:** El Grupo de Trabajo sobre SUPA define un modelo de datos a utilizar para representar políticas de alto nivel y posiblemente aquellas aplicables a toda la red que, a su vez, se puedan usar como entrada para una función de gestión de red (dentro de un controlador, un orquestador o un elemento de red). El procesamiento de esta entrada probablemente requerirá cambios en la configuración de las redes. Sin embargo, SUPA no se ocupa de definir cambios de configuración específicos, sino que se ocupa de cómo se aplican los cambios de configuración (por ejemplo, quién está autorizado a establecer políticas y cuándo y cómo se activan, cambian o desactivan las políticas).

En la práctica, SUPA define modelos YANG de base para codificar políticas que a su vez referenciarán modelos YANG específicos de dispositivos, tecnologías y servicios desarrollados en otros grupos de trabajo. El grupo de trabajo se enfoca en un único dominio de gestión y está diseñado para trabajar con modelos de dispositivos, protocolos, redes y servicios.

**Actas:** https://www.ietf.org/proceedings/93/minutes/minutes-93-supa

**Resultados:** Una reunión bastante concurrida que identificó trabajo para el IETF y demostró que las personas adecuadas para realizar el trabajo están disponibles. Antes de formar un grupo de trabajo sobre este tema se requiere más discusión para acotar su alcance y aclarar las expectativas. (El charter del SUPA WG se aprobó el 2 de octubre de 2015, http://datatracker.ietf.org/wg/supa/charter/.)

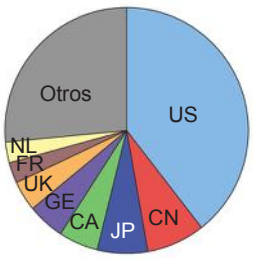
### Interfaz con las funciones de seguridad de red (i2nsf)

**Descripción:** El objetivo principal de I2NSF es definir un modelo de información, un conjunto de interfaces de software y modelos de datos para control y seguimiento de diferentes aspectos de las funciones de seguridad de redes (NSF) físicas y virtuales. Otros aspectos de las funciones de seguridad de redes (por ejemplo, el aprovisionamiento y la configuración de dispositivos y redes) exceden el alcance del grupo. El control y seguimiento de as funciones de seguridad de redes deben incluir la posibilidad de especificar, consultar, supervisar y controlar estas funciones por parte de una o más entidades de gestión. Dado que diferentes proveedores de seguridad admiten diferentes características y funciones en sus dispositivos, I2NSF se centrará en las NSF basadas en el flujo que ofrecen tratamiento para paquetes/flujos, tales como IPS/IDS, filtrado web, filtrado de flujos, inspección profunda de paquetes, o coincidencia y remediación de patrones.

**Actas:** https://www.ietf.org/proceedings/93/minutes/minutes-93-i2nsf

**Resultados:** Ahora el charter de este grupo de trabajo propuesto está mejor definido que cuando se propuso originalmente durante en IETF 91. Los participantes apoyaron fuertemente la formación de un grupo de trabajo y varios indicaron su interés en implementar o desplegar una solución I2NSF. (El charter del I2NSF WG se aprobó el 18 de septiembre de 2015, http://datatracker.ietf.org/wg/i2nsf/charter/.)

# SÍNTESIS DEL IETF 93




Participantes: 1384

Participantes por primera vez: 204

Número de países: 65

**Actividad del IETF desde el IETF 92 (22 de marzo al 19 de julio de 2015)**

Nuevos grupos de trabajo: 12

Grupos de trabajo cerrados: 8

Grupos de trabajo con charter: 143

Borradores de Internet nuevos y revisados: 1739

RFC publicadas: 116

- 76 en el proceso de estandarización, 5 mejores prácticas actuales, 6 experimentales, 27 informativas

**Reestructuración del IESG**

Reestructuración finalizada

- Siete áreas: ART, GEN, INT, OPS, RTG, SEC, TSV
- El IESG está trabajando en experimentos para trasladar más trabajo de los Directores de Área a los Grupos de Trabajo y la comunidad

**Actividad de la IANA desde el IETF 92 (marzo-junio de 2015)**

Se procesaron 1458+ solicitudes relacionadas con el IETF

- Se revisaron 97 R-Ds en período de último llamado y 118 R-Ds en evaluación
- Se revisaron 110 R-Ds antes de convertirlas en RFCs, 57 de las 110 contenían acciones para la IANA

Desde el IETF 92 (marzo-junio de 2015) se agregaron 12 nuevos registros

- gmpls-wson, precis-parameters, precis-tables-6.3.0, rdap-asn, rdap-dns, rdap-ipv4, rdap-ipv6, gmpls-wson, precis-parameters, precis-tables-6.3.0, babel, ppspp, security-label-format-selection, battery-technologies, scim

Desempeño SLA (enero-junio de 2015)

- Procesamiento meta promedio para las solicitudes relacionadas con el IETF: 99%

IANA y DNSSEC

- Al 15 de julio de 2015, 834 TLD tenían una cadena de confianza completa desde la raíz del DNS. http://stats.research.icann.org/dns/tld_report/

**Actividad del Editor de RFC desde el IETF 92 (marzo – 15 de julio de 2015)**

RFC publicadas: 135

- 108 IETF (12 IETF no correspondientes a ninguno de los grupos de trabajo), 2 IAB, 4 IRTF, 9 independientes

# CALENDARIO DE REUNIONES DEL IETF

Para obtener más información sobre las reuniones del IETF pasadas o futuras, diríjase a

**www.ietf.org/**.

**IETF 95**
**Fecha:** 3 al 8 de abril de 2016
**Anfitrión:** TBD
**Lugar:** Buenos Aires, Argentina

**IETF 96**
**Fecha:** 17 al 22 de julio de 2016
**Anfitrión:** Juniper Networks
**Lugar:** Berlín, Alemania

**IETF 97**
**Fecha** :13 al 18 de noviembre de 2016
**Anfitrión:** TBD
**Lugar:** Seúl, Corea del Sur

**IETF 98**
**Fecha:** 26 al 31 de marzo de 2017
**Anfitrión:** TBD
**Lugar:** Montreal, Canadá

**Un agradecimiento especial por recibir al IETF 93**

BROCADE

cz.nic | CZ DOMAIN REGISTRY

**La beca o *fellowship* de la Internet Society para participar en las reuniones del IETF forma parte de su programa Líderes de la Próxima Generación y es auspiciada por**

Afilias Google Microsoft

**Esta publicación fue posible gracias al apoyo de los siguientes auspiciantes que participan en el Programa Platino de la Internet Society**

Afilias cisco comcast ERICSSON Google

ICANN JUNIPER NETWORKS NBCUniversal RIPE NCC

Publicado tres veces al año
por la Internet Society.
Galerie Jean-Malbuisson 15
1204 Ginebra, Suiza

**Editor**
Mat Ford

**Editores Asociados**
Megan Kruse • Michelle Speckler

**Escritora Colaboradora**
Carolyn Marsan

**Editorial y diseño**
Speckler Creative

**Consejo Editorial**
Jari Arkko
Mat Ford
Olaf Kolkman
Megan Kruse
Andrew Sullivan
Greg Wood

**Email:**
ietfjournal@isoc.org

**Encuéntrenos en la Web**
www.internetsociety.org/ietfjournal

**Nota del Editor**
*La versión en inglés del IETF Journal* se adhiere al *Oxford English Dictionary*, segunda edición



*pub-IETFJv11.2-20151022-en*




# IETF Journal

Internet Society
Galerie Jean-Malbuisson 15
1204 Ginebra, Suiza