Responsabilidad Corporativa y Sostenibilidad

Cuaderno Red de Cátedras Telefónica

Universidad Carlos III de Madrid

La Arquitectura SAVI Para Validación de Dirección de Origen en Internet

Cátedra Telefónica de Internet del Futuro de la Universidad Carlos III de Madrid

La arquitectura SAVI (Source Address Validation Implementation) que está siendo estandarizada por el Internet Engineering Task Force (IETF) proporciona los medios para validar las direcciones de origen mediante la observación del tráfico de los mecanismos de configuración de direcciones IP.

Marcelo Bagnulo, Alberto García-Martínez.

Febrero 2013

www.catedras.telefonica.es
www.rcysostenibilidad.telefonica.com

Telefónica

Biografía

Marcelo Bagnulo

Marcelo es Profesor Titular del Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid. Es el Director de la Catedra Telefónica de Internet del Futuro para la productividad de la Universidad Carlos III de Madrid.

Alberto García- Martínez

Alberto es Profesor Titular del Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid.

Índice

1. INTRODUCCION

El paradigma no orientado a conexión sobre el cual fue construida la capa de red de Internet ha hecho posible la suplantación de direcciones origen de forma natural, esto es, el uso de una dirección origen por un nodo en el cual no se ha configurado de forma legítima dicha dirección. Los atacantes pueden emplear direcciones falsas para prevenir ser detectados y para evitar filtrado basado en dirección origen mientras realizan ataques de denegación de servicio basado en inundación, ataques de envenenamiento o cuando propagan gusanos o malware [1].

La preocupación sobre los riesgos inducidos por la suplantación de la dirección origen ha dado lugar a la recomendación de la implantación del ingress filtering (o filtrado de entrada) [2]. Esta técnica consiste en el filtrado de cualquier paquete con una dirección origen que no pertenece al conjunto de prefijos que están asignados a la parte de la topología desde la que proviene el paquete. El filtrado de entrada se lleva a cabo habitualmente cerca del lugar en el cual se originan los paquetes, ya sea en el router de salida del sitio o bien en el router de entrada del proveedor inmediato. Esta estrategia de implementación no solo implica una protección más eficaz, sino una manera más sencilla de determinar los prefijos correspondientes al sitio, ya sea por configuración explicita o por la inferencia de éstas en las tablas de enrutamiento.

Nótese que la efectividad de esta técnica también depende de realizar un amplio despliegue de la misma, ya que desde cualquier sitio en el que no se aplique filtrado de entrada permite que un conjunto de máquinas puedan generar paquetes con direcciones falsificadas.

Aunque el filtrado de entrada fuese desplegado universalmente, todavía nos enfrentaríamos a vulnerabilidades residuales. En particular, como el filtrado de entrada trabaja a nivel de prefijo (o conjunto de prefijos) un atacante podría falsificar cualquiera de las direcciones del conjunto de prefijos asignados a la parte de la topología desde la cual se conecta. El Grupo de Trabajo sobre SAVI (Source Address Validation Implementation) del Internet Engineering Task Force (IETF) está trabajando en la estandarización de mecanismos que complementen el filtrado de entrada y proporcionen mejor protección. El enfoque propuesto trabaja en una granularidad más fina y sitúa los filtros de dirección origen más cerca de los nodos, preferiblemente en los conmutadores de capa 2 que conectan dichos nodos en un enlace IP. En este enfoque, un conmutador está

configurado con un mapeo entre la dirección IP de un nodo y una propiedad específica en la capa 2 de dicho nodo (llamada binding anchor), la cual debería ser difícil de falsificar, permitiendo al puente filtrar los paquetes que no correspondan a un mapeo existente. El puerto físico al que está conectado el nodo es un ejemplo de este binding anchor.

Debido a que el proceso de filtrado se ha acercado a los nodos finales, la dificultad en determinar qué dirección de origen debería ser o no filtrada se incrementa. Cuando el filtrado de entrada es realizado por un sitio, el conjunto de direcciones de origen que pueden ser utilizadas legítimamente es el resultado del proceso de asignación de direcciones a nivel de prefijo, y la configuración del filtro es bastante sencilla y estática. Sin embargo, si el filtrado se va a realizar con granularidad por cada dirección IP, los costes de gestión de los mapeos van a aumentar. La configuración estática de los mapeos es complicada e impide la movilidad del host en la capa 2, esto es, impide que los hosts se sigan comunicando una vez que cambia el punto al que están conectados en la infraestructura a nivel 2. Un segundo enfoque, como el seguido por 802.1X [12] es la definición de nuevos protocolos que permitan demostrar a los nodos la propiedad de su dirección, pero esto implica cambiar los nodos finales y ciertamente limita el despliegue de dicha solución. Una tercera alternativa es monitorizar el tráfico intercambiado por los nodos e inferir del mismo la posesión de direcciones. Por ejemplo, los conmutadores podrían inspeccionar los mensajes DHCP para saber qué direcciones son asignadas a qué nodos y así prevenir que los nodos utilicen otros binding anchors que no les corresponden (por ejemplo, nodos conectados a otros puertos) utilizando las direcciones de forma ilegítima. Tenga en cuenta que el grado en el que se puede inferir con éxito la propiedad de la dirección depende mucho del método utilizado para configurar las direcciones en los nodos. En particular, si no hay una autoridad central para la asignación de direcciones, como ocurre en las direcciones auto configuradas de IPv6, no es obvio conocer a cuál de los nodos que intentan utilizar la misma dirección se le debe de conceder la comunicación.

El Grupo de Trabajo sobre SAVI ha adoptado el enfoque de control del tráfico para demostrar la propiedad de la dirección. Se han desarrollado tres soluciones para el filtrado de direcciones en el nivel de enlace (conocidas como soluciones SAVI), cada una adaptada a un mecanismo específico de configuración de direcciones. La primera solución, DHCP SAVI [9] inspecciona los mensajes DHCP y DCHPv6 para deducir a qué nodos se le asignan qué direcciones. La segunda solución, FCFS SAVI [10], está dirigida a los nodos de que configuran localmente las direcciones IPv6, utilizando por ejemplo el mecanismo de Configuración Automática de Direcciones sin Estado [3]. La última solución, SEND SAVI [savi-send], se beneficia de la capacidad de los nodos que ya están implementando SEND (Secure Neighbor Discovery Protocol, [6]) para demostrar la propiedad de la dirección por medio de direcciones criptográficas y certificados de los routers.

El resto del artículo está organizado como sigue: la sección 2 presenta la arquitectura general que se aplica a todas las soluciones SAVI, incluyendo el concepto de la aplicación del perímetro. Estas consideraciones de diseño se encuentran más detalladas en [5]. A continuación se describen las soluciones para los diferentes mecanismos de configuración de direcciones, es decir, DHCP (sección 3), nodos que configuran las direcciones IPv6 a nivel local (sección 4) y SEND (sección 5). Finalmente se presentan algunas conclusiones.

2. LA ARQUITECTURA SAVI

Las soluciones SAVI previenen la suplantación de la dirección IP de origen mediante el filtrado de paquetes para los que no existe un mapeo SAVI. Un mapeo SAVI es una asociación entre una dirección IP y un binding anchor, propiedad de la conexión del host a la red, como por ejemplo el puerto de la conexión física de la máquina. El binding anchor debe ser verificable y difícil de falsificar. Para dicho fin son adecuados, por ejemplo, mecanismos específicos sobre la MAC para asegurar las tramas de datos, tales como IEEE 802.1AE, o cualquier otra asociación de seguridad. Cuando el puerto de conexión es utilizado como binding anchor, la protección que se ofrece es que los paquetes con una determinada dirección IP de origen son reenviados sólo cuando llegan desde dicho puerto físico.

En un enlace dado se suelen conectar tanto hosts como routers. Tanto unos como los otros generan paquetes con sus propias direcciones como dirección de origen. Los routers, además, también reenvían paquetes que proceden de otros enlaces. Los mapeos SAVI se crean para validar las direcciones de origen locales al enlace y también para evitar que los hosts generen paquetes con direcciones que no pertenecen al enlace al que están conectados.

Los mapeos SAVI son creados de forma dinámica como resultado del proceso de inspección de tráfico, en función del mecanismo de configuración de direcciones usado. Cada solución SAVI define sus propias reglas para la creación y actualización de los mapeos.

La validación de direcciones de origen definida en SAVI puede ser llevada a cabo en cualquier dispositivo que reenvíe paquetes conectado al mismo enlace que el host, por ejemplo, en el router de salida. Sin embargo, la protección proporcionada es más efectiva si el filtrado SAVI se realiza cerca de los nodos, los cuales se supone que son menos fiables, por lo que todo el tráfico intercambiado entre los nodos se valida. Además, cuando el puerto se utiliza como binding anchor se puede conseguir una protección óptima al tener

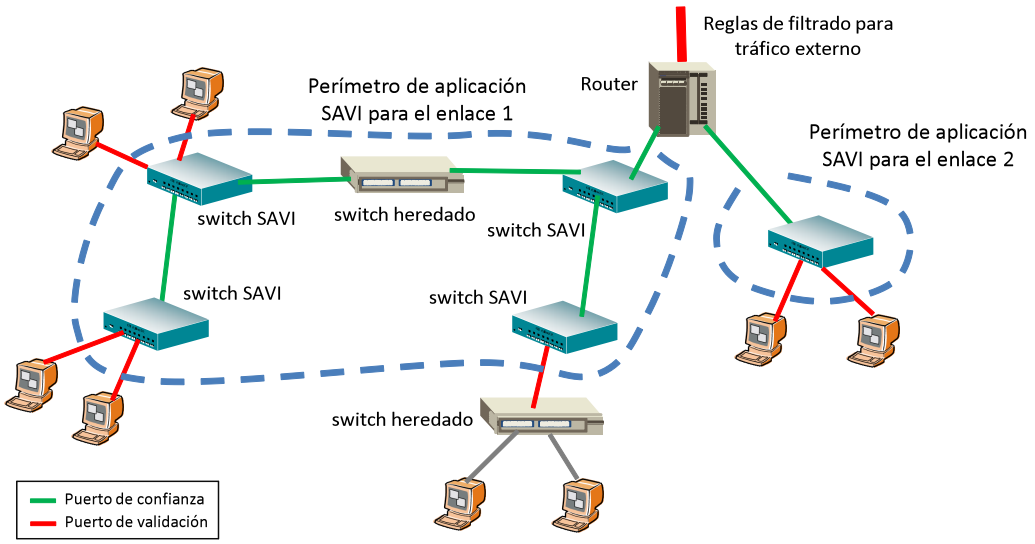

Figura 1: Ejemplo de perímetro de protección para SAVI

sólo un nodo conectado a un puerto del dispositivo que está realizando el filtrado SAVI (a partir de aquí dispositivo SAVI). Por lo tanto, se recomienda implementar la funcionalidad SAVI en los conmutadores de la capa de enlace que conectan los nodos de la capa de red.

Es habitual conectar muchos conmutadores de capa 2 para crear enlaces con un gran número de nodos. Esto impone potencialmente la necesidad de una gran cantidad de memoria en los dispositivos SAVI para almacenar la información de los mapeos. Si además se intercambian grandes cantidades de tráfico entre los nodos, las consideraciones de rendimiento son críticas. Con el fin de reducir el número de paquetes que debe validar cada dispositivo SAVI y el estado requerido por esta operación, la arquitectura SAVI se basa en el concepto de protección perimetral. El perímetro de protección está formado por un conjunto de dispositivos SAVI interconectados, y divide el enlace en una zona de confianza y una zona de no confianza. Los puertos de los dispositivos SAVI que están conectados a la zona de confianza son configurados como puertos de confianza, es decir, puertos en los que la validación no se realiza, ya que se conectan a dispositivos en los que se confía, tales como otros conmutadores o routers SAVI. Los puertos conectados a la zona de no confianza son configurados como puertos de validación, lo que significa que las direcciones de origen de los paquetes provenientes de estos puertos son verificadas frente a un enlace existente antes de que sean reenviados. Los puertos conectados a los hosts también se configuran como puertos de validación. Los conmutadores que no implementan SAVI se pueden colocar dentro del perímetro, siempre y cuando sólo se

utilicen para interconectar la infraestructura de confianza, de lo contrario tienen que colocarse fuera del perímetro. Cuando el perímetro de protección se configura, cada dispositivo SAVI sólo almacena los enlaces de los nodos conectados a través de los puertos de validación, y sólo comprueba la validez de las direcciones de origen procedentes de estos puertos. Un ejemplo de la implementación del perímetro de protección SAVI se muestra en la figura 1.

3. DCHP SAVI

DHCP (tanto para IPv4 [7] como en DHCPv6 [8]) define un mecanismo para configurar direcciones en los hosts. El funcionamiento habitual de DHCP en IPv4 ocurre de la siguiente manera: un nodo sin una dirección configurada manualmente difunde un mensaje de tipo DHCPDISCOVER (con la dirección IP de origen no especificada, 0.0.0.0) para solicitar una dirección a los servidores DHCP. Uno o más servidores responderán con un mensaje tipo DHCPOFFER, el cual incluye la posible dirección a utilizar. El nodo selecciona una de dichas direcciones ofrecidas y difunde un mensaje de tipo DHCPREQUEST, el cual es confirmado por el servidor correspondiente con un mensaje tipo DHCPACK.

La asignación de direcciones por DHCPv6 se lleva a cabo con las siguientes variaciones: tras la autoconfiguración de una dirección de enlace local, el nodo emite un mensaje de solicitud al router para descubrir los routers en el enlace y recibir las posibles prefijos. Si se supone que el enlace debe usar DHCP para la configuración de la dirección, el router contestará con un mensaje de anuncio del router en el que el flag M [4] estará activo (Managed address configuration, o configuración de dirección gestionada), indicando que el nodo debería utilizar DHCPv6 en el proceso de configuración de su dirección. Utilizando la dirección de enlace local como dirección origen, y la dirección de multidifusión All_DHCP_Relay_Agents_and_Servers como destino, el nodo envía un mensaje de tipo DHCPv6 SOLICIT para descubrir los servidores disponibles, el cual es contestado con un mensaje de tipo ADVERTISE en el que se incluye(n) la(s) dirección(es) a ser configurada(s). El nodo selecciona uno de dichos servidores y envía un mensaje tipo REQUEST con los parámetros seleccionados para la configuración, los cuales son confirmados por el servidor con un mensaje tipo REPLY. Se puede incluir la opción Rapid Commit en el mensaje DHCPv6 SOLICIT con el fin de pedir al servidor un mensaje REPLY, reduciendo así el intercambio de entre dos y cuatro mensajes.

DHCP SAVI [9] se basa en la autoridad proporcionada por el servidor DHCP y la habilidad de los dispositivos SAVI para inspeccionar el intercambio de mensajes DHCP y determinar los mapeos entre las direcciones IPv6 asignadas por el servidor y el binding anchor utilizado por el nodo para realizar la petición. En particular, los dispositivos DHCP SAVI

espían los mensajes tipo REQUEST para identificar el binding anchor del nodo de origen y obtener la dirección IP asociada de la inspección del mensaje DHCPACK/REPLY. El tiempo de concesión incluido en la respuesta del servidor se utiliza para configurar el tiempo de caducidad asociado al estado del dispositivo SAVI. Los mensajes DHCP también son monitorizados para actualizar o eliminar los mapeos existentes.

Para permitir el despliegue de la protección del perímetro, el binding anchor de los servidores o repetidores DHCP deben ser configurados de forma que los mensajes de asignación de direcciones sólo puedan ser enviados por entidades de confianza.

Tenga en cuenta que para DHCPv6, la validación de dirección de origen para la dirección de enlace local utilizada por el mecanismo DHCP (entre otros posibles usos) debe ser realizada de otra forma, como por ejemplo mediante FCFS SAVI, comentado a continuación.

4. FCFS SAVI PARA NODOS IPV6 SLAAC

State-Less Address Auto-Configuration (abreviando, SLAAC) [3] define un mecanismo por el cual un nodo puede generar direcciones tanto de enlace local como globales y comprobar la unicidad de dichas direcciones por medio del mecanismo de detección de direcciones duplicadas del protocolo de descubrimiento de vecinos. Para la obtención de las direcciones de enlace local y global, los identificadores supuestamente únicos de la interfaz se derivan de la configuración permanente de la capa de enlace de la interfaz. La parte del prefijo de una dirección global se obtiene de los mensajes de anuncio del router generados por los routers locales. Para comprobar que no existe algún otro nodo con la misma dirección al generar una dirección de enlace local o global, se ejecuta el procedimiento de detección de direcciones duplicadas (DAD) como sigue: Un nodo en el proceso de configurar una dirección envía un mensaje de solicitud de vecino (a partir de ahora DAD_NSOL) con una dirección de destino multicast a la que cualquier otro nodo que posea dicha dirección debe estar asociado. Si existe un nodo con la misma dirección, responderá al mensaje DAD_NSOL con un mensaje de tipo anuncio de vecino (DAD_NADV), y el nodo que inició el procedimiento DAD no configurará la dirección. En caso de no haber respuesta durante un corto periodo de tiempo, se considerará que la dirección está disponible y el nodo la utilizará. Mientras no finalice el proceso, se dice que la dirección se encuentra en estado de tentativa.

Al contrario que en el caso de DHCP, SLAAC no se basa en un sistema de autorización externa, y su modelo de propiedad es de por sí más débil que el de DHCP. SLAAC se utiliza por nodos en los que el cambio de dirección cada vez que se conectan a la red no es un problema (por ejemplo, hosts ejecutando aplicaciones cliente). Para esos nodos, no es tan relevante mantener su dirección/identidad durante un largo periodo de tiempo, sino para evitar la coincidencia temporal de dos nodos utilizando la misma dirección/identidad al mismo tiempo. Es en ese caso FCFS SAVI es suficiente- FCFS SAVI permite aseurar que una vez que un nodo A esté utilizando una dirección, otro nodo no puede utilizarla. Si el nodo A libera la dirección y deja de utilizarla durante algún tiempo, es aceptable permitir que otro nodo B la utilice. Si A intenta configurar de nuevo la dirección, el mecanismo DAD le indicará que el nodo B la está utilizando, y A debería configurar una dirección diferente (de las 2^64 direcciones posibles para el enlace) para recuperar la conectividad. En resumen, FCFS SAVI protege las direcciones siguendo un enfoque “Primero que llega, primero en ser atendido” (FCFS pro su sigla en inglés).

La regla de propiedad de dirección FCFS es impuesta por SAVI de la siguiente manera: Cuando un nodo está configurando una dirección D, debe validar si otro nodo ya tiene configurada la misma dirección mediante la generación de un mensaje DAD_NSOL [3]. Un dispositivo SAVI S que recibe el mensaje DAD_NSOL a través de un puerto de validación, comprueba si existe un mapeo para la dirección solicitada ya sea en el mismo dispositivo o en otro de la red. Para hacer esto, S reenvía el mensaje DAD_NSOL a otros conmutadores, y a los puertos de validación asociados a una mapeo existente para la dirección D en S, en caso de que dicho mapeo exista. Otros conmutadores que reciban este mensaje procederán de la misma forma: reenviar el mensaje a otros puentes y a cualquier puerto de validación para el que exista una mapeo con la dirección D. Si un host tiene la dirección D configurada, y su puente SAVI más cercano tiene un mapeo para D, contesta al mensaje DAD_NSOL recibido con un mensaje DAD_NADV. Nótese que sólo los nodos para los que existía previamente un mapeo con D reciben el mensaje DAD_NSOL, previniendo que los nodos maliciosos interfieran en el proceso. Cuando el puente S recibe el DAD_NADV, se da cuenta de que ya existía un mapeo para D y no se crea el mapeo local. S reenvía el mensaje DAD_NADV al puerto de validación por el que se recibió el DAD_NSOL de forma que el host que intenta configurar la dirección sea notificado sobre la colisión de direcciones y trate de configurar una dirección distinta.

FCFS SAVI soporta la movilidad de host a nivel de capa 2 sin modificaciones adicionales. En caso de que un nodo cambie su punto de conexión del puerto P al puerto Q, se emitirá un mensaje DAD_NSOL desde el puerto Q para comenzar de nuevo con el proceso DAD, tal y como es requerido por [3]. El mensaje será reenviado al puerto P, pero ningún host contestará la petición, con lo que el nodo configurará la dirección, el mapeo en Q será configurado y el mapeo en P será eliminado.

Por último, destacar que este mecanismo no es adecuado para el uso en IPv4, ya que para dicho protocolo se emplea DHCP para habilitar el uso de direcciones efímeras de forma eficiente, considerando la escasez del espacio de direcciones IPv4.

5. SEND SAVI

SEND (SEcure Neighbor Discovery, o descubrimiento seguro de vecinos) [6] define una serie de extensiones de seguridad para el descubrimiento de vecinos en IPv6 que permiten a los nodos probar integridad, autenticación y autorización para el intercambio de mensajes ND al adjuntar una firma RSA. La autorización de los routers se basa en cadenas de certificados. Además, SEND permite probar la propiedad de las direcciones para los hosts que configuran automáticamente sus direcciones locales. Para hacer esto, se necesita que los hosts creen un par de claves pública y privada, para generar un tipo especial de dirección IPv6 utilizando la clave pública. Este tipo de direcciones, denominadas CGA (Cryptographically Generated Address, o direcciones generadas criptográficamente) se crean utilizando un hash de la clave pública en los 64 bits inferiores de la dirección. Una vez creada, los hosts pueden utilizar la clave privada asociada a la CGA para firmar los mensajes ND. La clave pública asociada a la CGA también se incluye en el mensaje ND. Un nodo que reciba un mensaje ND asegurado, primero comprueba la validez de la clave pública asociada a la CGA, y entonces comprueba que la firma se hizo con la clave privada asociada a la CGA. De esta forma, la capacidad de firmar mensajes ND está ligada a una dirección IPv6 particular, con lo que la validación de un mensaje ND también permite probar la propiedad de la CGA para el nodo que la generó. Un atacante que quiera suplantar a un nodo legítimo mediante SEND necesita generar un par de claves pública y privada con un hash de la clave pública que coincida con la CGA del destino, lo cual es computacionalmente inviable.

SEND SAVI se basa de la habilidad de los nodos SEND para probar la propiedad de las direcciones. Un dispositivo SEND SAVI inspecciona y valida los mensajes DAD_NSOL y DAD_NADV para determinar si los nodos involucrado en el intercambio de mensajes están autorizados para utilizar y configurar la dirección. Para actualizar el mapeo y determinar si un nodo que envía paquetes de datos posee una dirección, los mensajes NSOL generados por el dispositivo SEND SAVI son enviados al puerto de validación al cual está conectado el nodo que utiliza la dirección. Conforme a la especificación de inalcanzabilidad de vecinos [4], los hosts deben contestar con un mensaje NADV, que será protegido por SEND.

Los mensajes de anuncio de router protegidos se utilizan por los dispositivos SEND SAVI para determinar los prefijos del enlace y los routers habilitados para inyectar tráfico off-link.

La protección contra posibles ataques basándose en los mensajes válidos SEND que son retransmitidos desde diferentes puertos es similar a FCFS SAVI: los mensajes relevantes para la configuración de enlaces SEND SAVI son únicamente reenviados a los puertos en los que ya existía un mapeo para la dirección.

6. CONCLUSIONES

Se ha presentado el marco SAVI para prevenir la falsificación de direcciones de origen en un enlace. Hasta ahora, tres soluciones están estandarizadas en el IETF, cada una de ellas derivando la autorización de la dirección de origen de los mensajes intercambiados por los diferentes mecanismos de configuración de direcciones. DHCP SAVI puede ser utilizado tanto para el protocolo IPv4 como para IPv6, mientras que FCFS y SEND están específicamente orientados a las redes IPv6.

El funcionamiento de SAVI es preferible implementarlo en los conmutadores de capa 2, y está diseñado para operar de manera eficiente en redes grandes. En todos los casos, los nodos no necesitan ser modificados para beneficiarse de la protección adicional. Para mantener el diseño tan simple como sea posible, no se han definido nuevos mensajes, pero los mensajes existentes definidos por otros protocolos (manteniendo la semántica actual) se utilizan en los dispositivos SAVI para preguntar y señalizar el estado de los enlaces entre ellos. La única configuración requerida por SAVI con el fin de asegurar un funcionamiento eficiente es la definición del perímetro de protección mediante la definición de los puertos de confianza y los puertos para los que se debe realizar una validación SAVI.

7. REFERENCIAS

[1] D. McPherson, F. Baker, J. Halpern. “SAVI Threat Scope”. Draft-ietf-savi-threat-scope-03. September 2010.
[2] P. Ferguson, D. Senie. “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”. RFC 2827. May 2000.
[3] S. Thomson, T. Narten, T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.
[4] T. Narten, E. Nordmark, W. Simpson, H. Soliman. “Neighbor Discovery for IP version 6 (IPv6)”. RFC 4861. September 2007.
[5] J. Wu et al. “Source Address Validation Improvement Framework”. draft-ietf-savi-framework-04. March 2011.
[6] J. Arkko, J. Kempf, B. Zill, P. Nikander. “SEcure Neighbor Discovery (SEND)”. RFC 3971. March 2005.
[7] R. Droms. “Dynamic Host Configuration Protocol”. RFC 2131. March 1997.
[8] R. Droms et al. “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”. RFC 3315. July 2003.
[9] J. Bi, J. Wu, G. Yao, F. Baker. “SAVI Solution for DHCP”. draft-ietf-savi-dhcp-09.txt. April 2011
[10] E. Nordmark, M. Bagnulo, E. Levy-Abegnoli. “FCFS SAVI: First-Come First-Serve Source-Address Validation for Locally Assigned IPv6 Addresses”, RFC6620. April 2011.
[11] M. Bagnulo, A. Garcia-Martinez. SEND-based Source-Address Validation Implementation. draft-ietf-savi-send-05. April 2011.
[12] IEEE. “IEEE 802.1X-2010 Port-Based Network Access Control”. Feb 2010.