REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 11. No. 2, mayo-agosto, 2012, p. 85-93 ISSN 1729-3804

cRucho: un software enrutador de código abierto

Ernesto Licea Martin[1], Jose Carlos Ramos Carmenates[2]

[1]*Centro Nacional de Investigaciones Científicas (CNIC). Ingeniero en Telecomunicaciones.* ernesto.licea@cnic.edu.cu

[2] *Centro Nacional de Investigaciones Científicas (CNIC). Ingeniero en Informática.* josecarlos@cnic.edu.cu

Resumen

Los niveles de crecimiento y complejidad alcanzados por las redes de telecomunicaciones modernas ofrecen una excelente oportunidad al uso de enrutadores para la interconexión, gestión y seguridad de las mismas. El gran costo de estos equipos en el mercado ha dado lugar al surgimiento de soluciones como los enrutadores por software. En este trabajo se presenta a cRucho, un software enrutador desarrollado y soportado por el Equipo Central de la Red del Centro Nacional de Investigaciones Científicas (CNIC), en La Habana, Cuba. Este software cuenta con un conjunto de prestaciones semejantes a las presentes en los enrutadores de gama alta que lo convierten en una solución eficiente y de código abierto.

Palabras claves: cRucho, desarrollo de software, software enrutador, telecomunicaciones.

cRucho: an open source software router

ABSTRACT

The levels of growth and complexity achieved by modern telecommunications networks offer a great opportunity to the use of routers for interconnection, security and management thereof. The high cost of such equipment in the market has given rise to solutions such as software routers. This paper presents cRucho, a software router developed and supported by the Network Team of the National Center for Scientific Research (CNIC), in Havana, Cuba. This software has a feature set similar to those present in the high-end routers that make it an efficient and open source solution.

Key words: cRucho, software development, software router, telecommunications.

INTRODUCCIÓN

Un enrutador es un dispositivo hardware o software para la interconexión de redes de computadoras que opera en la capa tres, nivel de red, del modelo OSI (Open Systems Interconnection por su siglas en inglés). Este interconecta segmentos de red o redes enteras, y encamina paquetes de datos entre redes tomando como base la información de la capa de red[1].

La utilización de los enrutadores en una red brindan las siguientes ventajas:

1. Separación de los dominios de colisiones.

2. Segmentación lógica y/o física en subredes acomodando la carga, de modo que la información se transmita de una forma más clara y por lo tanto más rápidamente.

3. Seguridad mediante técnicas como el filtrado de paquetes, listas de control de acceso, IDS (Intrusion Detection System por sus siglas en inglés), etcétera.

4. Gestión y administración mediante protocolos como SNMP (Simple Network Management Protocol), registro de eventos, etcétera. Estos protocolos brindan una noción más amplia del rendimiento y permiten obtener estadísticas del funcionamiento de la red, facilitando las tareas de gestión y administración[2, 3].

Actualmente los enrutadores modernos no solo se limitan a las funciones mencionadas previamente, sino que pueden poseer un conjunto de prestaciones dependiendo del fabricante[4]. Entre estas podemos encontrar:

1. Servidor DHCP (Dynamic Host Configuration Protocol por sus siglas en inglés). Ofrece un servicio de asignación dinámica de direcciones IP que facilita la configuración de las terminales.

2. Servicio de NAT (Network Address Translation por sus siglas en inglés). La NAT se utiliza en los enrutadores conectados a Internet para traducir una única dirección pública en múltiples direcciones de la red privada. Esto significa que muchos dispositivos pueden tener una misma dirección pública y, puesto que no se puede tener acceso directamente a las direcciones privadas desde otro usuario de Internet, el resultado es una mayor seguridad[5].

3. Enrutamiento dinámico y/o estático mediante la implementación de protocolos como RIP (Routing Information Protocol por sus siglas en inglés) en sus diferentes versiones y OSPF (Open Shortest Path First por sus siglas en inglés).

4. Configuración y enrutamiento de VLANs (Virtual LANs) aumentando los niveles de seguridad y el rendimiento de la red interna.

5. Calidad de Servicio. Permite la clasificación y priorización de tráfico, dando lugar al trato diferenciado de diferentes tipos de tráficos, protocolos o aplicaciones [6.1].

6. Seguridad mediante la utilización de diferentes técnicas como filtrado de direcciones MAC, filtrado por direcciones IP, filtrado de tráfico por URL, IPS (Intrusion Prevention System por sus siglas en inglés), acceso utilizando https, implementación de autenticación de usuarios utilizando RADIUS, posibilidad de implementación de una DMZ (Demilitarized Zone por sus siglas en inglés), etcétera.

7. Servidor VPN (Virtual Private Network). Adicionalmente, diferentes modelos pueden actuar como clientes o servidores VPN posibilitando la conexión a otras redes privadas o sirviendo de pasarela para otros clientes VPN.

8. Gestión y Administración. Implementación de protocolos como SNMP, registro de eventos, alertas de incidencias, etcétera, y utilización de una interfaz gráfica de acceso web para una fácil gestión y administración.

Los enrutadores son generalmente clasificados por gamas: baja, media y alta. El aumento de la gama es directamente proporcional al número de prestaciones presentes en el equipo y al costo en el mercado del mismo.

Los software enrutadores son computadoras con un sistema operativo estándar o mejorado y programas instalados que posibilitan que esta realice las funciones de enrutamiento e interconexión de segmentos de red o redes enteras. Estos software ofrecen las siguientes ventajas sobre los enrutadores convencionales [4]:

1. Son más económicos, limitándose solamente al costo de la computadora que realizará las funciones de enrutador y al costo de los dispositivos externo añadidos a dicha computadora.

2. Son más flexibles. Se pueden añadir y/o eliminar prestaciones ya que estas son dadas por programas que funcionan sobre el sistema operativo que realiza las funciones de enrutador.

3. Configuración sencilla. Generalmente estos enrutadores poseen una interfaz web de administración muy sencilla o su configuración se limita a la edición de ficheros.

cRucho COMO SOFTWARE ENRUTADOR

cRucho es una distribución de Linux (Ubuntu 10.04) personalizada para funcionar como enrutador y cortafuegos de una red. Este software enrutador es desarrollado y soportado por el Equipo Central de la Red del Centro Nacional de Investigaciones Científicas (CNIC) como solución a las necesidades de un enrutador con ciertas características y que, a su vez, permitiese mantener la uniformidad en los Sistemas Operativos utilizados.

cRucho utiliza las herramientas presentes en el kernel de Linux para funcionar como enrutador y cortafuegos de la red. Además, cuenta con un conjunto de herramientas presentes en los repositorios de Ubuntu que enriquecen y fortalecen las potencialidades del software enrutador. La utilización en conjunto de estas herramientas permite que cRucho sea una solución sencilla y efectiva a las necesidades básicas de enrutamiento y control de tráfico de pequeñas y medianas redes.

Este proyecto fue concebido bajo principios guías entre los que se destacan los siguientes[7]:

Configuración a partir de ficheros y aplicaciones: cRucho está concebido para la configuración a partir de la edición de ficheros y la ejecución de aplicaciones para la validación y activación de las configuraciones realizadas.

Enfoque modular: La arquitectura de cRucho es totalmente modular, ofreciendo la posibilidad de usar solamente las funcionalidades deseadas mientras que las otras se mantienen inactivas. Esto brinda la posibilidad de una mayor eficiencia en la explotación de los recursos del sistema.

Escalabilidad: Existe una gran diversidad de herramientas para analizar y mejorar el funcionamiento y gestión de la red. cRucho, al estar basado en la distribución Ubuntu del Sistema Operativo Linux, permite la integración con cualquier herramienta que sea compatible con esta distribución.

Extensible a partir de aplicaciones: A partir del reconocimiento de que no existe una solución a todos los requerimientos necesarios en un enrutador, cRucho está diseñado para permitir la adición de nuevas funcionalidades a partir de extensiones en lenguajes como python, bash, perl, etcétera.

Facilidad de instalación y distribución: cRucho cuenta con una imagen ISO creada a partir de la modificación de la distribución Ubuntu del Sistema Operativo Linux en su versión 10.04. La instalación a partir de la imagen ISO elimina muchas de las acciones propias de la instalación de Ubuntu, agilizando y facilitando el proceso de instalación del software enrutador.

La arquitectura de cRucho es mostrada en la figura 1. Los administradores del enrutador pueden a través de la consola editar los ficheros de configuración y ejecutar las aplicaciones de cRucho que validan las configuraciones en los ficheros de configuración, y a su vez ejecutan las aplicaciones del sistema para modificar los parámetros necesarios en el kernel de Linux y que este realice las tareas propias del enrutador[7].

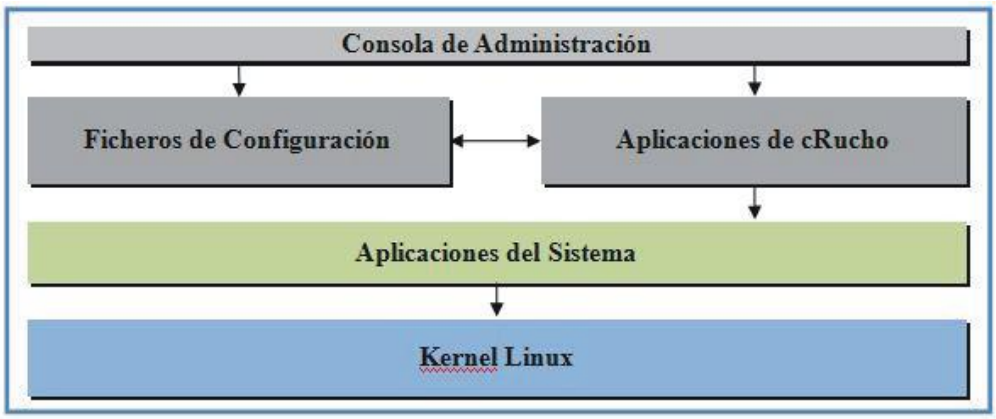

Fig 1. Arquitectura de cRucho

Entre sus principales funcionalidades se encuentran[7]:

Configuración de Interfaces: Permite la configuración individual de los dispositivos de red presentes, asignándoles una dirección IP y una máscara de red. Se crea una capa de abstracción de modo que se pueden nombrar los mismos y no llamarlos por los nombres que le asigna el Sistema Operativo. La configuración se realiza utilizando la herramienta ip del paquete iproute2, presente en el kernel de Linux a partir de la versión 2.2.

Configuración de IP Alias: Configuración de direcciones IP secundarias sobre un mismo dispositivo de red, de modo que se pueda realizar una segmentación lógica en tramos de red utilizando un mismo dispositivo de red como pasarela para todos los tramos de red creados. Esta configuración también hace uso de la herramienta ip del paquete iproute2.

Configuración de VLANs: Creación de subinterfaces virtuales con soporte para el protocolo 803.1q para la creación y enrutamiento entre LANs Virtuales. Para la creación de las mismas se hace uso de un paquete vlan presente en los repositorios de Ubuntu.

Configuración de Cortafuegos: Configuración de un cortafuegos para filtrar el tráfico entrante a cada interfaz de red. Para esto se utiliza la tabla FORWARD de la herramienta iptables del paquete Netfilter, presente en el kernel de Linux.

Enrutamiento de paquetes: El enrutamiento de paquetes se realiza modificando la tabla de rutas estáticas del sistema operativo utilizando la herramienta ip del paquete iproute2 incluido en el kernel de Linux. Las rutas estáticas son configuradas de forma convencional teniendo en cuenta la dirección IP y la máscara de la red destino y el próximo salto que debe dar el paquete enrutado.

Creación de NAT y PAT: Configuración de reglas para realizar la traducción de múltiples direcciones IP de la red interna en direcciones públicas de Internet. Además es posible la traducción de puertos. Para la configuración de NAT y PAT se utiliza la tabla NAT de la herramienta iptables.

Calidad de Servicio(QoS): Creación de jerarquía de colas HTB (Hierachical Token Bucket por sus siglas en inglés) para la priorización y tratamiento diferenciado de tráfico utilizando la herramienta TC (Traffic Control) del paquete iproute2, y la tabla MANGLE de la herramienta iptables para el marcado de tráfico. Con el uso combinado de estas herramientas es posible realizar la conformación de tráfico a la salida de las interfaces de red, de modo que se pueden colocar los paquetes en las colas creadas recibiendo un tratamiento diferenciado.

Graficado de Colas: Generación de gráficos del consumo de ancho de banda de cada una de las colas existentes a partir de las estadísticas almacenadas en Bases de Datos RRD (Round Robin Database por sus siglas en inglés). Para la creación de las Bases de Datos y la generación de los gráficos se utiliza la herramienta rrdtools presente en los repositorios de Ubuntu y el servidor web Apache para la publicación de los gráficos.

SNMP: Posee un agente SNMP capaz de recoger información de la red y del sistema y almacenarlo en las MIBs (Management Information Base por sus siglas en inglés) correspondientes, para un posterior análisis facilitando las funciones de gestión y administración de la red. Para esto, es utilizado el paquete snmp presente en los repositorios de Ubuntu.

Servidor SSH: Cuenta con un servidor SSH (Secure SHell por sus siglas en inglés) para la administración remota del enrutador.

Integración con Ntop: Ntop es una herramienta que permite monitorizar en tiempo real una red. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos en la red en un instante concreto. Posee un modo de trabajo en Web, volcando en HTML el trabajo en la red. Viene con un emisor/recolector NetFlow/sFlow, una interfaz de cliente basada en HTTP para una mejor visualización de estadísticas de la red y RRD para almacenar persistentemente estadísticas de tráfico. Permite la monitorización de protocolos como TCP, UDP, ICMP, ARP, IPX, NetBios, etcétera9. cRucho integra este monitor de red dentro del software enrutador de modo que el usuario puede apoyarse en las estadísticas recogidas por Ntop para una mejor planificación y detección de problemas en la red. La configuración de Ntop se realiza en la interfaz web que este incorpora y es independiente de las configuraciones de cRucho.

CONFIGURANDO cRucho

cRucho consta de un fichero de configuración general ubicado en el camino /etc/crucho/crucho.conf, donde se definen las configuraciones generales del sistema y los módulos del software enrutador que van a ser activados. Además, existen 8 ficheros para las configuraciones de los módulos por separado, cuyos caminos son definidos en crucho.conf. Entre las opciones que podemos encontrar en este fichero se encuentran[7]:

hostname: Nombre de la PC que funcionará como software enrutador

domain: Dominio al cual pertenece el enrutador

DNS_Servers: Servidores DNS (Domain Name Service por sus siglas en inglés)

NTP_Server: Servidores de tiempo

Authorized_SSH_Service: Direcciones IP o subredes autorizadas a la gestión remota del enrutador

Authorized_Ntop_Service: Direcciones IP o subredes autorizadas al acceso al Ntop.

Authorized_SNMP_Service: Direcciones IP o subredes autorizadas a realizar encuestas SNMP.

Community: Palabra clave usada para realizar encuestas SNMP

Authorized_HTTP_Service: Direcciones IP o subredes autorizadas a visualizar la página web donde están publicadas las gráficas de consumo de ancho de banda de las colas.

Authorized_ICMP: Direcciones IP o subredes autorizadas a realizar encuestas ICMP (Internet Control Message Protocol por sus siglas en inglés)

iface_file: Camino del fichero de configuración de las interfaces de red

vlan_file: Camino del fichero de configuración de las VLANs

alias_file: Camino del fichero de configuración de los IP Alias de las interfaces

routes_file: Camino del fichero de configuración de las rutas estáticas

firewall_file: Camino del fichero de configuración de las reglas del cortafuegos

outbound_file: Camino del fichero de configuración de las reglas NAT

portfwd_file: Camino del fichero de configuración de las reglas PAT

qos_file: Camino del fichero de configuración de Calidad de Servicio (QoS)

www_directory: Camino del directorio donde se almacenarán los gráficos de consumo de ancho de banda de las colas para su publicación web.

Las configuraciones para utilizar las potencialidades de cRucho se realizan en ficheros por separado, de modo que todas las configuraciones queden organizadas y sea sencillo realizar cambios o agregar nuevas configuraciones.

Cada modificación o nueva configuración agregada exige una activación mediante el reinicio del enrutador o la ejecución de aplicaciones que varían en dependencia de la configuración modificada. En el proceso de activación se realizan dos tareas fundamentales:

1. Validación de la configuración agregada o modificada.
2. Activación de los parámetros del sistema.

Si durante la validación de la configuración se encuentran errores, estos son almacenados en los logs de cRucho e informados al administrador y se omite el paso 2. De esta manera se evita que errores en las configuraciones provoquen un mal funcionamiento del enrutador.

No todas las configuraciones exigen el reinicio del enrutador para su activación, sino que algunas pueden activarse mediante la ejecución de aplicaciones, como puede observarse en la figura 2. Las configuraciones en el cortafuegos, tabla de rutas estáticas, NATs y/o PATs, IP Alias y Calidad de Servicio tienen sus propias aplicaciones capaces de activar una modificación o nueva configuración, mientras que los cambios en las configuraciones generales del enrutador, VLANs e Interfaces si necesitan el reinicio del enrutador[7].

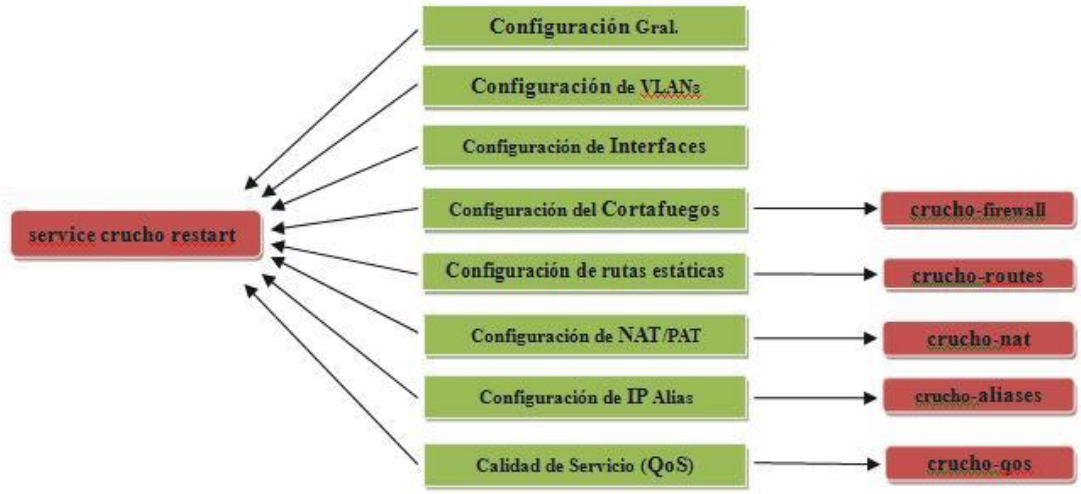

Fig 2. Proceso de activación de configuraciones de cRucho

CONCLUSIONES

El uso de enrutadores en pequeñas y medianas redes reporta múltiples beneficios en cuestiones de seguridad, gestión y rendimiento de una red. Los enrutadores por hardware pueden ser muy costosos en la actualidad, dependiendo de las características requeridas. El uso de enrutadores por software de código abierto constituye una solución alternativa. cRucho se destaca gracias a los siguientes elementos:

Es de fácil gestión y administración

Cuenta con muchas de las prestaciones presentes en los enrutadores por hardware de gama alta.

Es flexible y relativamente fácil de extender, posibilitando la adaptación a las necesidades específicas de una red.

REFERENCIAS

COMER, DUGLAS E.: "Redes Globales de Información con Internet y TCP/IP. Principios básicos, protocolos y arquitectura". 3a. Ed. Prentice-Hall Hispanoamericana, S.A. pp 54-55, 1996 .

RFC 1157: "A Simple Network Management Protocol (SNMP)", disponible en: http://tools.ietf.org/html/rfc1157.

BARRIOS DUEÑAS, JOEL: "Como configurar SNMP", disponible en: http://www.alcancelibre.org/staticpages/index.php/como-linux-snmp.

MICROSOFT TECHNET: "Diseño de enrutadores y conmutadores", disponible en: http://www.microsoft.com/spain/technet/recursos/articulos/secmod40.mspx.

RFC 3022: "Traditional IP Network Address Translator", disponible en: http://tools.ietf.org/html/rfc3022.

Recomendación UIT-T E.800: "EDefiniciones de términos relativos a la calidad de servicio", disponible en: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809-I!!PDF-S&type=items.

LICEA MARTIN, ERNESTO: "cRucho:Manual de Usuario". Centro Nacional de Investigaciones Científicas, 2012.

BERT, HUBERT: "Enrutamiento Avanzado y Control de Tráfico en Linux", disponible en: http://www.lartc.org/lartc.pdf.

PRAS, AIKO: "NTOP Network TOP An Overview", disponible en: http://www.ntop.org/wp-content/uploads/2011/09/ntop-overview.pdf.