

Laboratorio virtual de networking como infraestructura tecnológica estratégica para realización de prácticas de redes de computadoras y seguridad informática. Use of a Virtual Networking Laboratory as strategic technological infrastructure to perform practices for computer networking and security IT

Cabañas Victoria, V.V.¹, Vázquez Castillo, J.², Blanqueto Estrada, M.³, Dávalos Castilla, L.Y.⁴

^{1,2,3,4} Dpto. de Ingeniería, División de Ciencias e Ingeniería

A/ Boulevard Bahía, s/n. 77019 Chetumal, Quintana Roo. México.

¹vdrakul@uqroo.edu.mx, ²jvazquez@uqroo.edu.mx, ³melissa@uqroo.edu.mx, ⁴laurad@uqroo.edu.mx

Fecha de recepción: 04 de junio de 2019

Fecha de aceptación: 30 de agosto de 2019

Resumen. El presente trabajo propone una infraestructura de redes virtualizada como opción viable y factible para las Instituciones de Educación Superior que desean el reconocimiento por la buena calidad de sus programas educativos en el área de las tecnologías de información y comunicación. Un elemento importante de la evaluación es la infraestructura. Sin embargo, no todas las IES poseen una infraestructura física de redes (instalaciones, equipos de telecomunicaciones activos, bastidores, UPS, etc.) y requieren que los estudiantes accedan a estos recursos tecnológicos para realizar prácticas con equipos de cómputo, de conmutación, ruteo y uso de dispositivos de seguridad perimetral. La infraestructura virtualizada que se propone en este artículo tiene como principales características la escalabilidad y reconfigurabilidad para diversos escenarios de infraestructuras de red.

Palabras Clave: Acreditación, Virtualización, redes, infraestructura, equipamiento.

Summary. This paper proposes a virtual network infrastructure as a resource for universities and/or colleges aiming to obtain accreditation for their programs in information and communications technology. One of the most important aspects considered in the accreditation process includes the evaluation of available infrastructure. However, not all universities and/or colleges have a physical infrastructure of networks available (e.g., facilities, active telecommunications equipment, racks, and uninterruptible power supplies [UPS]). A second emphasis in evaluations is on students' access and use of technological resources to perform networking practices with computer equipment, switching, routing and perimeter security devices. The main characteristics of the virtual infrastructure proposed in this paper include the scalability and reconfigurability of multiple scenarios in network infrastructures.

Keywords: Accreditation, Virtualization, Networking, Infrastructure, equipment.

1 Introducción

El proceso enseñanza-aprendizaje en las áreas disciplinares de computación, particularmente las definidas en el documento “Modelos Curriculares del Nivel Superior de Informática y Computación” publicado por la Asociación Nacional de Instituciones de Educación en Tecnologías de la Información, A.C. (ANIEI) y el Consejo Nacional de Acreditación en Informática y Computación, A.C: (CONAIC) requiere la participación activa del estudiante a través de prácticas como elemento fundamental para el desarrollo de competencias en redes de acuerdo al modelo curricular: transmisión y comunicación de datos, modelos, protocolos, intercomunicación de redes, seguridad e integridad de la información y sistema distribuidos [1].

La categoría 9 definida en el marco de referencia para la Acreditación de Programas Académicos de Informática y Computación señala que la Infraestructura y equipamiento constituyen un elemento fundamental para que las actividades del programa académico se lleven de manera eficiente y sea posible cumplir los objetivos del programa, contribuyendo a garantizar la calidad del mismo [2].

El criterio 9.1 Infraestructura evalúa la suficiencia y el uso racional y eficiente de la infraestructura, donde el primer indicador determina que se deben contar con espacios físicos donde se ofrezcan los servicios de cómputo. Para el caso de programas con modelos curriculares donde se incorporan software de base, sistemas operativos y redes [1], ha resultado un tema complicado el financiamiento para la adquisición de equipo de telecomunicaciones específico para realización de prácticas por parte de los estudiantes.

Los indicadores 9.2.5 y 9.2.7. del formato de evaluación resaltan la necesidad de contar con diversas plataformas de sistemas operativos y la existencia de una red de área local con software adecuado para las aplicaciones mas comunes del programa [3].

1.1 Modelo curricular Redes

Las redes como modelo curricular [1] tiene como objetivo estudiar la teoría y conocer los elementos operativos para la transmisión y recepción de la información. Se abordan las diversas formas de distribuir y compartir recursos computacionales, procesos e información, considerando los aspectos de seguridad e integridad a través de las siguientes temáticas: señales, transmisión de voz, imágenes y datos, topologías, protocolos para la comunicación, interconectividad, interoperabilidad, integridad, seguridad y confiabilidad de la información.

1.2 Modelo curricular Software de Base

Los sistemas operativos como modelo curricular [1] tienen como objetivo estudiar la teoría, técnicas y metodologías para el diseño y construcción de sistemas operativos, con énfasis en cada uno de sus componentes. En la sección 5.2.2 del documento modelos curriculares del nivel superior de informática y computación “Tipos de sistemas operativos”, se mencionan los sistemas operativos orientados a los servicios de red, virtualización, hipervirtualización y los ambientes gráficos.

1.3 Objetivo General

Proponer una infraestructura de red híbrida, virtual y controlada para la realización de prácticas de redes y seguridad informática.

1.4 Objetivos específicos

- Implementación de una topología de red con equipos reales adecuados y suficientes para soportar la instalación de la plataforma virtual.
- Implementación de la plataforma de software para emulación de redes.
- Diseño e implementación de un escenario virtual con diversos protocolos de red, servidores, clientes, equipo para realización de pruebas de seguridad informática, cortafuegos, enrutadores y conmutadores.

1.5 Marco conceptual

Virtualización. Crea un entorno informático simulado, o virtual, en lugar de un entorno físico. A menudo, incluye versiones de hardware, sistemas operativos, dispositivos de almacenamiento, etc., generadas por un equipo. Esto permite a las organizaciones particionar un equipo o servidor físico en varias máquinas virtuales. Cada máquina virtual puede interactuar de forma independiente y ejecutar sistemas operativos o aplicaciones diferentes mientras comparten los recursos de una sola máquina host [4].

Virtualización de redes. Es la combinación de los recursos de red del hardware con los recursos de red del software en una única unidad administrativa. El objetivo de la virtualización de redes consiste en facilitar un uso compartido de recursos de redes eficaz, controlado y seguro para los usuarios y los sistemas [5].

La *emulación de redes* permite diseñar topologías de red complejas y realizar simulaciones dentro de ellas. Se pueden incorporar imágenes binarias de sistemas operativos de enrutamiento privativos, máquinas virtuales con sistemas operativos cliente, de servidor, y dispositivos de seguridad perimetral, entre otros [6].

2 Desarrollo

Para el desarrollo del laboratorio virtual se consideró el software emulador de redes GNS3, el cual integra productos de diversos fabricantes que se encuentran actualmente en el mercado como, por ejemplo: Juniper Networks [7], Cumulus Networks, Inc.[8], Fortinet [9], PfSense [10]; también incluye los IOSv (versiones del sistema operativo de enrutadores y conmutadores) de VIRL (Virtual Internet Routing Lab) [11].

2.3 Metodología

Se tomó como referencia a las redes jerárquicas diseñadas con la metodología Top-Down dentro de las posibilidades para el diseño de topología lógica, que por lo general representa la infraestructura de red con un ambiente real similar; lo anterior con la finalidad de representar ataques remotos. El modelo en cuestión tiene considerado lo siguiente en términos de virtualización:

- *Redundancia.* Simular esta característica permite la disponibilidad en las conexiones y las pruebas de pen-testing.
- *Seguridad.* Las diferentes políticas de seguridad a nivel de acceso y de distribución expondrá mejor las evasiones que se quieran probar en determinados experimentos más avanzadas.
- *Escalabilidad.* Para expandir en caso necesario la topología para pruebas puntuales.
- *Facilidad de administración.* El diseño de la topología facilita la gestión de cada dispositivo para una mejor visualización del ambiente de laboratorio.
- *Facilidad de mantenimiento.* En técnicas de modularidad, si un dispositivo falla rápidamente se puede revertir el incidente ya sea por medio de un snapshot, la copia de configuraciones por TFTP y/o la restauración de imágenes.
- *Rendimiento.* Considerando la atención oportuna hacia un ambiente de red adecuado para las distintas pruebas, el rendimiento es relevante cuando se demanda una alta carga de datos; en especial cuando el trabajo se lleva a cabo de forma remota. Por lo anterior, se utilizaron enlaces 1000BASE-TX entre cada capa, para el grupo de conexión entre los enrutadores WAN y el enrutador nube central se ocuparon interfaces de fibra óptica virtuales SONET.
- *Capas de jerarquía.* Para representar esta característica inherente al diseño, se dividieron en dos zonas (sin contar la zona WAN), cada una con su dominio y capa correspondiente, simulando así dos infraestructuras independientes. La organización fue la siguiente:
 - Capa de acceso: S1, S2, S3, S4-A, S5-A y S6-A.
 - Capa de distribución: SL3-D1, SL3-D2, SL3-D3, SL3-D4 y SL3-D5.
 - Capa de núcleo: MANnet, ISP, F1-Core y F2-Core.

Actualmente es posible encontrar diversos desarrollos y aplicaciones orientadas a la mejora de las habilidades de programación, configuración y seguridad de redes de computadoras a través de la propuesta de laboratorios virtuales y contribuyendo así en la experiencia práctica de la formación de alumnos de nivel superior. Por ejemplo, en [13] se presenta un laboratorio virtual basado en WEB con la finalidad de que usuarios puedan acceder a un conjunto de dispositivos virtuales de red y con ello evaluar el desempeño de diversas configuraciones de red y sus componentes. Por otra parte, en [14] se presenta un simulador de red para estudiantes de ingeniería que empiezan a adquirir conocimientos en la configuración de redes de computadoras y con ello mejorar sus habilidades en la programación de equipos de red. Así mismo, una propuesta de laboratorio virtual de redes es presentado en [15], con el cual los estudiantes pueden realizar diversas configuraciones sobre una red virtual y sus componentes. Adicionalmente, este último trabajo presenta los resultados de intenciones de uso en este tipo de alternativas. Se comenta que las herramientas de virtualización de redes de computadoras vienen a ser una solución asequible para lograr que los alumnos de nivel superior adquieran la experiencia de configuración y manipulación de equipos de red ante la limitada accesibilidad de recursos físicos de infraestructura de red que pudiera existir en un laboratorio de redes y telecomunicaciones. Nuestra propuesta viene a contribuir en la formación de ingenieros en redes de la Universidad de Quintana Roo y a contribuir en el desarrollo y formación de habilidades de configuración de equipos de red.

3 Conclusiones

La infraestructura física que soporta a la presente propuesta es de dos equipos de escritorio con 16 GiB de RAM, Disco duro de 500 GiB, procesador AMD A8, que permiten configurar un entorno virtualizado con diversas tecnologías, además de la capacidad de integrar otros servicios de red de acuerdo a necesidades específicas. El escenario presentado brinda facilidades de uso, experimentación y puesta en práctica de las competencias que se derivan de los modelos curriculares de redes que de otra forma sería complicado para los programas educativos poseerla ya que tendrían que gestionar presupuesto y financiamiento que permitiera a los estudiantes contar con los espacios físicos y equipamiento para realizar las prácticas de laboratorio.

La virtualización de redes ofrece el mejoramiento de las capacidades tecnológicas a los Programas Educativos, permite un mayor desarrollo de competencias informáticas en los estudiantes, optimiza los recursos

con los que cuenta la Institución y permite acceder y probar nuevas tecnologías, en un ambiente controlado y benéfico para el proceso enseñanza-aprendizaje.

Referencias

1. A. R. García Gaona, F. J. Álvarez Rodríguez y M. d. L. Sánchez Guerrero, Modelos Curriculares de Nivel Superior de Informática y Computación, México: Pearson Educación de México S.A. de C.V., 2015.
2. Consejo Nacional de Acreditación en Informática y Computación, A.C., «Marco de referencia para la Acreditación,» Consejo Nacional de Acreditación en Informática y Computación, A.C., México, 2017.
3. Consejo Nacional de Acreditación en Informática y Computación A.C., «Formato de autoevaluación,» Consejo Nacional de Acreditación en Informática y Computación A.C., México, 2018.
4. Microsoft , «Microsoft Azure,» Microsoft Azure, 2019. [En línea]. Available: <https://azure.microsoft.com/es-mx/overview/what-is-virtualization/>. [Último acceso: 29 Mayo 2019].
5. Oracle, «Administración de Oracle Solaris: interfaces y virtualización de redes,» Diciembre 2011. [En línea]. Available: https://docs.oracle.com/cd/E26921_01/html/E25833/toc.html. [Último acceso: 16 Mayo 2019].
6. Galaxy Technologies, LLC, «GNS3 The software that empowers network professionals,» Galaxy Technologies, LLC, Enero 2019. [En línea]. Available: <https://www.gns3.com/>. [Último acceso: 16 Mayo 2019].
7. Juniper Networks, «Juniper Networks,» Juniper Networks, Enero 2019. [En línea]. Available: <https://www.juniper.net/us/en/>. [Último acceso: 17 Mayo 2019].
8. Cumulus Networks Inc, «Networking software for the open, modern data center,» [En línea]. Available: <https://cumulusnetworks.com/>. [Último acceso: 17 Mayo 2019].
9. Fortinet Inc., «Security for the Enterprise,» Enero 2019. [En línea]. Available: <https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-security.html>. [Último acceso: 17 Mayo 2019].
10. Rubicon Communications, LLC (Netgate), «PfSense Open Source Security,» Rubicon Communications, LLC (Netgate), 2019. [En línea]. Available: <https://www.pfsense.org/>. [Último acceso: 17 Mayo 2019].
11. Cisco Systems, «Virtual Internet Routing Lab,» Cisco Systems, 2019. [En línea]. Available: 17. [Último acceso: Mayo 2019 2019].
12. QEMU, «2019,» Software Freedom Conservancy., [En línea]. Available: <https://www.qemu.org/>. [Último acceso: 17 Mayo 2019].
13. M. W. a. H. Nakano, «NVLab, a Networking Virtual Web-Based Laboratory that Implements Virtualization and Virtual Network Computing Technologies,» *IEEE Transactions on Learning Technologies*, vol. 3, n° 2, pp. 129-138, 2010.
14. M. Bazdresch, «A small network simulator for learning routing fundamentals,» *IEEE Frontiers in Education Conference (FIE)*, pp. 1-7, 2018.
15. T. W. a. W. A. W. Sommoool, «Exploring the factors that influence the intention to use a virtualization-based laboratory,» de *8th International Conference on Ubi-Media Computing*, Colombo, 2015.