

Estudio del uso de Inteligencia Artificial en la configuración de ruteadores CISCO (2024)

César Enrique Estrada Gutiérrez

Universidad Autónoma del Estado de México

ORCID 0000-0002-0936-8157

cestradag@uaemex.mx

María de la Luz Imelda Sánchez

Universidad Autónoma del Estado de México

ORCID 0000-0002-9113-6047

mdsanchezp@uaemex.mx

Juan Alberto Ruiz Tapia

Universidad Autónoma del Estado de México

ORCID 0000-0002-4317-1112

jaruizt@uaemex.mx

RESUMEN

Cuando se usa la Inteligencia Artificial (IA) en todos los aspectos científicos y tecnológicos de la actualidad y en lo particular en la configuración de ruteadores CISCO, en realidad se está representando un avance significativo en la optimización de redes de computadoras, ya que con esto se ofrecen soluciones más eficientes, rápidas y adaptativas. Actualmente la forma más tradicional de configuración de ruteadores requiere de un alto nivel de experiencia técnica, tiempo y de recursos humanos y financieros, lo que conlleva por consecuencia a posibles errores humanos y vulnerabilidades en la configuración. Sin embargo, la IA ahora nos ayuda y nos permite automatizar gran parte de estas tareas, minimizando los errores y así mejorando en la seguridad. En este contexto, la IA puede aplicarse para optimizar el rendimiento de la red, mediante el ajuste automático de parámetros clave como la asignación de ancho de banda, la priorización del tráfico y quizás la detección de anomalías que de manera tradicional no se podrían ver. Además, si se piensa en el aprendizaje automático, las redes podrán adaptarse a patrones de tráfico emergentes y con esto se podrían predecir posibles fallos, lo que hará que se incremente la robustez y eficiencia operativa de las redes de comunicación. La implementación de IA en la configuración de ruteadores disminuye de acuerdo con lo observado en gran medida, la carga operativa de los administradores de redes, para así facilitar enfocarse en tareas más estratégicas dentro de la organización. Esto deberá ser relevante en instituciones académicas y organizaciones, como centros de investigación, donde las redes de gran escala requieren de una gestión constante y adaptable, al mejorar la seguridad y rendimiento de la infraestructura.

Palabras clave: Inteligencia Artificial, Ruteadores, CISCO, configuración.

Study of the use of Artificial Intelligence in the configuration of CISCO routers

(2024)

ABSTRACT

When Artificial Intelligence (AI) is used in all scientific and technological aspects today, particularly in the configuration of CISCO routers, it represents a significant advancement in optimizing computer networks, offering more efficient, faster, and adaptive solutions. Currently, the traditional way of configuring routers requires a high level of technical expertise, as well as significant time, human, and financial resources, which can lead to potential human errors and vulnerabilities in the configuration. However, AI now helps automate a large portion of these tasks, minimizing errors and improving security. In this context, AI can be applied to optimize network performance by automatically adjusting key parameters such as bandwidth allocation, traffic prioritization, and detecting anomalies that might not have been identified through traditional methods. Furthermore, when machine learning is incorporated, networks can adapt to emerging traffic patterns, allowing potential failures to be predicted, thereby increasing the robustness and operational efficiency of communication networks. The implementation of AI in router configuration significantly reduces the operational burden on network administrators, allowing them to focus on more strategic tasks within the organization. This is particularly relevant for academic institutions and organizations like research centers, where large-scale networks require constant, adaptable management to improve both security and performance of the infrastructure.

Keywords: Artificial Intelligence, Routers, CISCO, configuration.

INTRODUCCIÓN

La configuración de ruteadores de la marca CISCO en particular por ser una de las marcas más importantes en el mundo, es una tarea crítica en la gestión de redes, ya que con esto se garantiza la conectividad, el rendimiento y la seguridad de la infraestructura de comunicaciones. Tradicionalmente, este proceso siempre se ha realizado en gran medida mediante los conocimientos técnicos y experiencia de los administradores de la red, lo que fácilmente conlleva errores humanos, ineficiencias y sobre todo una gestión reactiva a los pormenores que surgen en el día a día en la operatividad de la red. El uso de la inteligencia artificial (IA) en la configuración de los ruteadores, nos ofrece una solución innovadora para automatizar y optimizar los procesos que actualmente se hacen de manera manual, para así mejorar la eficiencia operativa y reduciendo el margen de error. Cabe resaltar que la forma de aprendizaje en el aula en gran medida es a través de simuladores y de teoría que difícilmente se ponen en práctica debido a la infraestructura con que cuentan las diferentes instituciones.

Esta investigación se justifica en la necesidad de explorar las capacidades de la IA al momento de configurar los ruteadores y de la forma de aprendizaje por parte de estudiantes de licenciatura en informática administrativa. Mediante la IA, los ruteadores podrán predecir fallos, ajustarse dinámicamente para controlar mejor el tráfico y mejorar la seguridad, lo que resulta especialmente relevante en los entornos académicos y empresariales donde las redes son fundamentales para la operación diaria.

METODOLOGÍA

La presente investigación será de tipo observacional, Analítica, Transversal y prospectiva, se trabajó con un total de 26 estudiantes inscritos en la materia de comunicación entre computadoras de la licenciatura en informática administrativa ofertada en la facultad de contaduría y administración de la Universidad Autónoma del Estado de México en el periodo de clases 2024A, debido a la selección total de los casos, no se requiere de aleatoriedad.

Se solicitó realizar una actividad que consistía en la configuración de un ruteador CISCO 2901 conectado a un switch 2960 en el cual se crearon 3 VLANs de las cuales solo una no debería conectarse a internet, se pidió a la mitad del grupo configurarlo de acuerdo con lo visto en clase y a la otra mitad configurarlo usando inteligencia artificial. Al finalizar la actividad se compararon los resultados y el tiempo de respuesta de ambos equipos

MARCO TEÓRICO Y CONTEXTUAL

Modelo OSI

Como todo en las comunicaciones entre computadoras es muy importante conocer el modelo de referencia OSI (Open Systems Interconnection), el cual es un modelo de siete capas que nos ayuda a comprender la interoperabilidad de las redes (Forouzan, 2017) para el caso de la actividad se ocuparon las capas 2 de enlace de datos y la 3 de red.

Dirección IP

Una dirección IP (Internet Protocol) se puede catalogar como un identificador numérico único asignado a un dispositivo conectado a una red con el cual se permite su identificación y ayuda a la comunicación. Existen prácticamente hoy en día dos versiones principales: el IPv4 (por ejemplo, 192.168.0.1) y el IPv6 (por ejemplo, 2001:0db8::1) (Tanenbaum & Wetherall, 2011).

En el caso de la actividad, las direcciones IP que se solicitó se asignaran fueron las direcciones IP clase C privadas 192.168.10.0, 192.168.20.0 y 192.168.30.0 las cuales son esenciales para la asignación de las configuraciones correspondientes a las subinterfaces del ruteador el cual permite el enrutamiento y acceso a internet restringiéndolo a una de las VLANs

SWITCH

Un switch es un dispositivo que se ocupa en una red en su capa 2 (enlace de datos) de referencia en el modelo OSI. Su función principal es recibir, procesar y reenviar datos entre los dispositivos que se conectarán a través de sus puertos, mediante el uso de direcciones MAC. A diferencia de un hub, el switch realiza conexiones directas a través de una tabla, lo que mejora la eficiencia de la red ya que con esto se evitan colisiones innecesarias (Forouzan, 2017).

En la actividad el switch que se solicitó es un switch Cisco 2960 el cual actúa como punto de conexión entre los dispositivos de cada VLAN y con ello se garantiza la segmentación adecuada del tráfico.

DIRECCIÓN MAC

Una dirección MAC (Media Access Control) es un identificador único que se asigna a una tarjeta de red de un dispositivo hecho por algún fabricante, dicha dirección se ocupa en la capa 2 de enlace de datos del modelo de referencia OSI, el cuál sirve para identificar y comunicar dispositivos dentro de una red de área local (LAN) (Tanenbaum & Wetherall, 2011).

El switch CISCO 2960 ocupará estas direcciones para poder conectar cada puerto a sus respectivos dispositivos y con ello estar en condiciones para segmentar la red correspondiente.

VLAN

Una VLAN (Virtual Local Área Network) es una subred lógica dentro de una red física que nos ayuda a segmentar dispositivos ocupando diferentes dominios de difusión y así mejorar la seguridad y rendimiento, dichas VLANs operan a nivel de capa 2 del modelo OSI, pero requieren de un router o de un switch de nivel 3 para la comunicación entre ellas (Forouzan, 2017).

Para el caso de la actividad se requiere que 2 de las VLANs tengan acceso a Internet y otra quedará aislada, por lo tanto, la segmentación de las mismas es indispensable en este caso.

Puerto troncal

Un puerto troncal es una interfaz que se configura en un switch para transportar tráfico de múltiples VLANs, se utiliza para etiquetar tramas en un estándar, que por ejemplo puede ser el IEEE 802.1Q. Esto permite que varias VLANs se puedan comunicar con otros switches o en su defecto con un ruteador (Cisco Systems, 2020).

El puerto troncal sería el enlace que conectará en el caso de la práctica el switch 2960 y el router Cisco 2901, con lo que se permitiría que las VLANs transmitan su tráfico hacia el router correspondiente y su enrutamiento y acceso hacia Internet

IEEE 802.1Q

El estándar IEEE 802.1Q es un protocolo desarrollado por el Institute of Electrical and Electronics Engineers (IEEE) con el que se definió como se etiquetarían los diferentes paquetes de datos que ayudan a identificar y manejar múltiples VLANs dentro de una red local, en realidad es una extensión del protocolo ETHERNET que permite que un único enlace físico pueda transportar tráfico de varias VLANs (IEEE, 2018)

El puerto troncal configurado con el switch CISCO 2960 y el router CISCO 2901 utilizará el estándar IEEE 802.1Q para transportar el tráfico entre las diferentes redes VLANs, con esto el router identificará a qué VLAN pertenece cada paquete y aplicará las políticas necesarias para el enrutamiento o bloqueo de estas.

Ethernet

Etherneth se refiere a una tecnología de red estándar que ha permitido la comunicación entre dispositivos en una red local, que ha tenido auge en las últimas décadas. Fue desarrollada por Xerox en la década de 1970 y estandarizada por el IEEE a través del estándar IEEE 802.3. Ethernet define las reglas para el formato y transmisión de datos en una red cableada, donde se consideran los tipos de cables, conectores y velocidades de transferencia de datos (IEEE, 2018)

Ethernet por consecuencia es la tecnología que soportará la conexión entre los dispositivos finales y el switch, así como la interconexión entre el switch y el ruteador.

Ruteador o router

Un ruteador es un dispositivo que opera a nivel de la capa 3 del modelo OSI, el cual se encarga de conectar diferentes redes mediante el enrutamiento de paquetes según sus direcciones IP. También realiza las traducciones de las direcciones de red (NAT) y aplica las directivas de seguridad (Tanenbaum & Wetherall, 2011).

En el caso de la práctica, el ruteador Cisco 2901 será el responsable de interconectar las VLANs y así proporcionar acceso a internet para dos de ellas y restringirlo para la tercera

Otros conceptos relevantes

NAT (Network Address Translation): Es una tecnología que permite que los dispositivos en una red privada puedan acceder a Internet utilizando una sola dirección IP pública (Cisco Systems, 2020). En el caso de la práctica, las direcciones IP privadas se encontrarán en las VLANs y el ruteador deberá contar con una dirección IP pública.

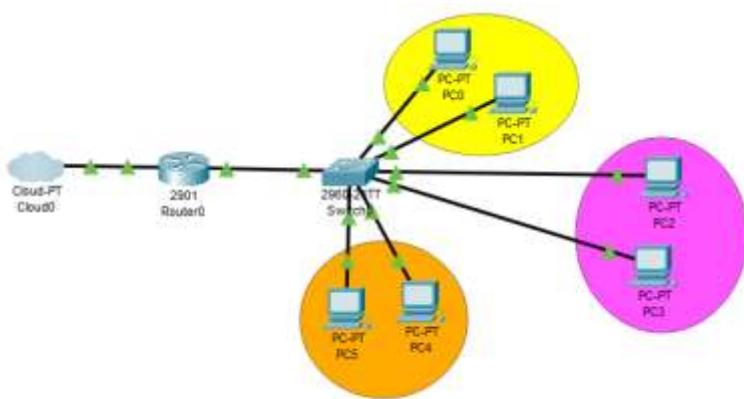
ACL (Access Control List): Es una herramienta para definir políticas de seguridad y filtrar el tráfico en routers o switches (Cisco Systems, 2020). Para la práctica se utilizará para bloquear el acceso a Internet de la VLAN restringida.

RESULTADOS Y DISCUSIÓN

La actividad consistió en realizar en packet tracer versión 8.2.0, software de Cisco, el diagrama que se muestra en la figura 1, configurar cada uno de los dispositivos y realizar una serie de pruebas de comunicación entre las 3 vlans que se solicitaron.

Figura No. 1

Diagrama solicitado donde se observan las 3 VLANs, el switch y el router correspondiente



Nota: El diagrama se hizo en el software de Cisco Packet Tacer versión 8.2.0, 2024

La VLAN amarilla y la rosa son las que se comunicarán hacia Internet, dejando fuera, la comunicación de la VLAN naranja. En el switch se configuran las VLANs correspondientes y en el ruteador se generan las ACLs para decirle cual de las VLANs tienen acceso a internet

En la figura 2 se observa cómo se configuraron las computadoras conectadas en cada VLAN y las direcciones IP que se pidió ocuparan en cada una de ellas.

Figura No. 2

Configuración

- VLAN 10 (Amarillo): Rango de direcciones 192.168.10.0/24
 - PC0: IP: 192.168.10.2, Máscara: 255.255.255.0, Gateway: 192.168.10.1
 - PC1: IP: 192.168.10.3, Máscara: 255.255.255.0, Gateway: 192.168.10.1
- VLAN 20 (Rosa): Rango de direcciones 192.168.20.0/24
 - PC2: IP: 192.168.20.2, Máscara: 255.255.255.0, Gateway: 192.168.20.1
 - PC3: IP: 192.168.20.3, Máscara: 255.255.255.0, Gateway: 192.168.20.1
- VLAN 30 (Naranja): Rango de direcciones 192.168.30.0/24
 - PC4: IP: 192.168.30.2, Máscara: 255.255.255.0, Gateway: 192.168.30.1
 - PC5: IP: 192.168.30.3, Máscara: 255.255.255.0, Gateway: 192.168.30.1

Nota: Desarrollo realizado por IA Chatgpt, 2024

Así mismo en la figura 3 se observa la configuración del router, su configuración de direcciones IP en las subinterfaces y la encapsulación en el estándar IEEE 802.1Q

Figura No. 3:

Configuración del router

```
Router> enable
Router# configure terminal
! Subinterfaz para VLAN 10
Router(config)# interface gigabitethernet0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
! Subinterfaz para VLAN 20
Router(config)# interface gigabitethernet0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
! Subinterfaz para VLAN 30
Router(config)# interface gigabitethernet0/0.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip address 192.168.30.1 255.255.255.0
Router(config-subif)# exit
```

Nota: Creado con IA Chatgpt, 2024

Como se comentó el grupo se dividió en 2, al primer grupo solo se les dio la instrucción y se les pidió usaran inteligencia artificial para resolver el problema, al segundo grupo se les explicó puntualmente cada uno de los conceptos y el por qué de las configuraciones, obteniéndose resultados que apoyan la hipótesis de que el uso de la inteligencia artificial es útil para la resolución de problemas de configuración de dispositivos de comunicación pero no para comprender conceptos necesarios para la resolución de los mismos.

Dentro de las ventajas que se observaron del uso de la inteligencia artificial destacan las siguientes:

1. Puede ser utilizada en cualquier momento de dudas, sin necesidad de distraer al profesor o de tenerlo presencialmente para una explicación
2. Se pueden encontrar detalles de la problemática y ejemplos parecidos o relacionados con el tema a solucionar
3. El aprendizaje autodidacta en todo su esplendor, ya que de tener la disciplina correcta es una herramienta muy importante para obtener resultados en poco tiempo
4. Se encuentra diversa información de índole teórico y práctico que pueden apoyar la resolución de problemas para dispositivos de comunicación

Por otro lado, las ventajas que se detectaron relacionadas con un profesor o asesor sobre la problemática fueron las siguientes:

1. El profesor tiene experiencia en resolver problemas con base en el mundo real, lo que puede ayudar en el momento de enfrentarse con problemas no contemplados por la IA.

2. El docente puede ajustar el nivel de explicación dependiendo de su sensibilidad en el conocimiento del alumno que se encuentra realizando la actividad
3. En el caso de laboratorios de redes un profesor puede ayudar directamente con las conexiones físicas
4. Se pueden plantear nuevas preguntas en el momento y contestarse para todo el grupo, no solo para el alumno que se encuentra realizando la actividad

CONCLUSIONES

De acuerdo con los resultados obtenidos se puede concluir que la mejor estrategia por ahora será usar ambos recursos, es decir que el docente haga una introducción al problema a realizar y que la IA ayude en obtener información inicial, pasos detallados e incluso la documentación correspondiente. Desde luego dependerá del objetivo que se persiga, por ejemplo, si se requiere una solución rápida sin pensar en el cómo se está haciendo, entonces la IA sería el camino, por otro lado si se busca una explicación más profunda y personalizada el profesor sería el camino para ayudar a comprender mejor el por qué de las configuraciones, en un entorno práctico, también un profesor será más útil para resolver los problemas físicos o relacionados con el equipo.

A pesar de que el grupo que uso la IA concluyó en un 75% más rápido que los que no la usaron, en su mayoría no supieron el por qué funcionaba, solo se limitaron a observar que daba resultados y que se consiguió el objetivo, lo que reafirma que hasta el momento se debe combinar el uso de la IA con apoyo docente para reafirmar y confirmar los conocimientos adquiridos

REFERENCIAS BIBLIOGRÁFICAS

- Cisco Systems. (2020). *Cisco Networking Essentials* (1st ed.). Cisco Press. <https://www.ciscopress.com/>
- Forouzan, B. A. (2017). *Data Communications and Networking* (5th ed.). McGraw-Hill Education. ISBN: 9780073376226
- Institute of Electrical and Electronics Engineers. (2018). IEEE Standard for Ethernet (IEEE Std 802.3™-2018). IEEE. <https://doi.org/10.1109/IEEESTD.2018.8512542>
- Institute of Electrical and Electronics Engineers. (2018). IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks (IEEE Std 802.1Q™-2018). IEEE. <https://doi.org/10.1109/IEEESTD.2018.8403927>
- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson Education. ISBN: 9780132126953