Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, Number 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4199

Implementation And Simulation Of Dynamic Arp Inspection In Cisco Packet Tracer For Network Security

Fauzan Prasetyo eka putra[1*], Ubaidi[2], Alief Badrit Tamam[3], Reynal Widya Efendi[4]
[1,2,3,4]University Of Madura, Indonesia
[1] prasetyo@unira.ac.id, [2]ubed@unira.ac.id, [3]aliefbadrittamam@gmail.com, [4]reynalwidya91@gmail.com

open access

***Corresponding Author**

Article History:
Submitted: 29-06-2024
Accepted: 30-06-2024
Published: 22-07-2024

Keywords:
ARP spoofing; Cisco Packet Tracer; Dynamic ARP Inspection; DHCP snooping; network security.

ABSTRACT

Dynamic ARP Inspection (DAI) is a security feature that helps prevent Address Resolution Protocol (ARP) spoofing attacks, which can compromise the integrity and confidentiality of data in a network. This paper presents the implementation and simulation of DAI using Cisco Packet Tracer, a network simulation tool. The goal is to show how DAI can be configured and used to improve network security by verifying ARP packets in a switched network. The implementation involved setting up a network topology with switches and end devices, configuring DHCP snooping, and enabling DAI on the switches. Simulations tested various scenarios, including normal operation, ARP spoofing attacks, and the network response to these attacks with DAI enabled. The results show that DAI effectively mitigates ARP spoofing attacks, ensuring only legitimate ARP packets are forwarded, thus protecting the network from potential security breaches. The study concludes that implementing DAI is an important step in securing networks, especially in environments with sensitive data and high security needs. This paper serves as a practical guide for network administrators looking to improve their network security posture using Cisco Packet Tracer.

INTRODUCTION

In today's digital era, many academic service systems in the realm of education, especially in the area around me, still use manual methods for learning and in the digital era, the development of information technology cannot be ignored(Informasi et al. 2024), Computer networks have become very important in almost every aspect of our lives, be it in the fields of business, education, and everyday life (Saputri and Kartikasari n.d.). The widespread use of computer networks in various fields of human life requires everyone to know and learn various kinds of supporting applications that can operate on these computers (Anon n.d.-a). By understanding network technology, one can build and manage an effective computer network, which can help in increasing productivity and efficiency in various fields (Publikasi et al. 2023). However, in reality, it has not been implemented due to lack of understanding and not understanding the functions and advantages of a computer network and limited capital equipment, so that the tools used are still lacking in quality (Anon n.d.-b)(Kemendikbud, Widodo, and Kelana Simpony n.d.). With the basic network using Cisco Packet Tracer software, it will make it easier to simulate computer networks and this allows students to learn from their mistakes without the risk of damaging the actual network infrastructure and this can also produce students who have insight and experience in their fields. (Eka Putra, Irwanto, and Heryadi 2019) (Salsabila and Sutabri 2024). *Cisco packet Tracer* can display network simulations with topology views and hardware visualizations so that it can be used as a computer network simulation and design tool and can also solve the main challenge is the availability of reliable network infrastructure and adequate hardware conditions (Prasetyo, Putra, et al. 2024)(Pembuatan Simulasi Jaringan Komputer Dengan Gns et al. 2022). The utilization of the Cisco Packet Tracer application provides encouragement and motivation for the teaching team to carry out the Learning Process in the hope of optimizing the learning experience of participants (Andrianto Putra et al. 2023). By using this application, the teaching team can create an interactive learning environment and dynamize the learning material with realistic network simulations. This allows participants to be more engaged in learning, improve their understanding of networking concepts, and enhance their practical skills in network configuration and troubleshooting. Therefore, with the development of information technology, criminals use various cyber spaces to increase cyber crime (Prasetyo, Badrit Tamam, et al. 2024). with the Cisco Packet Tracer media, learning tasks can be designed in such a way that they are not as complicated as they seem in the real world, so that participants can easily and quickly master skills that would be very difficult when they try to master them in the real world. (Resi, Baitanu, and Tamal n.d.). *Cisco Packet Tracer* can also be used as an alternative e-learning media. So that the learning process becomes optimal and the learning process becomes interactive and interesting (Anjelica and Sulandjari 2022) (Sutiyono et al. 2024). all resources owned by the network, by monitoring the network can analyze outside attacks such as arp spoofing attacks this attack can see the activities of the target being attacked such as stealing usernames and passwords (Arsalan 2023).

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, Number 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4199

LITERATURE REVIEW

Dynamic ARP Inspection (DAI) is a network security feature designed to prevent ARP spoofing attacks, where an attacker can send fake ARP messages to trick other devices on the network into sending data through the attacker's computer. By implementing DAI, network administrators can verify and filter out unauthorized ARP packets, thus protecting the integrity and confidentiality of data on the network. Several literatures have examined the implementation and effectiveness of DAI in improving network security and it also has outstanding security standards and plays an important role in network management (Prasetyo, Badrit Tamam, et al. 2024).

In the guidebook "Implementing Dynamic ARP Inspection" by Cisco Systems, detailed steps for configuring and implementing DAI on Cisco switches are described. The guide covers basic setup, DHCP snooping configuration, and DAI activation, as well as how to verify and monitor DAI operation. It provides a solid foundation for network administrators in implementing this feature. due to the importance of the ARP protocol as each frame must contain the Media Access Media Access Control (MAC) address to be transmitted. In addition, ARP spoofing attacks can be used to perform many other important attacks such as Denial-of-Service (DDoS) and Session (Morsy and Nashat 2022).

Hijacking Attacks

The book "Dynamic ARP Inspection and DHCP Snooping" by Pearson Education explains the theory and practice related to DAI and DHCP snooping, including basic concepts, configuration, and practical scenarios. The book also includes simulations using tools such as Cisco Packet Tracer to reinforce understanding. This allows readers to learn how to implement and test DAI in a simulated environment before implementing it in a production network.

Suspicious ARP traffic detection is aimed at identifying suspicious network activities such as zero-day zero-day attacks and malicious broadcast requests to find vulnerable hosts in the network. For example, Whyte et al. proposed DAI feature-based anomaly detection (Sun, Ochiai, and Esaki 2022). compared to other techniques and provides a quantitative analysis of the performance of DAI in various network scenarios. This provides empirical evidence of the benefits of DAI in protecting networks.

The use of the Cisco Packet Tracer simulator is considered to increase understanding of the theory that has been given. Suggestions that can be used as input in the implementation of this service activity are the need for further training on Computer Network material with topics such as configuration (Sun et al. 2022).

This research simulates ARP spoofing attacks on one portable device and one network router. This process involves gathering information and researching relevant literature, as well as creating simulations to detect ARP spoofing attacks. The simulation results showed that the ARP Spoofing attack was successfully detected with a 100% success rate. The data obtained includes the MAC addresses of the attacker and victim, as well as the time of the attack. This research shows that the NIST method is effective in detecting ARP spoofing attacks that can lead to new attacks (Prakoso and Khamas Heikmakhtiar 2024).

With the process of testing the wifi network security system in the form of intrusion experiments with ARP spoofing attacks to find usernames and passwords and port scanning experiments to find open ports and ddos attack experiments to send packets to the target and implement firewall rules against attacks that have been carried out and this test is carried out to determine the function of the DAI feature (Prakoso and Khamas Heikmakhtiar 2024)(Eka Putra et al. 2023).

METHOD

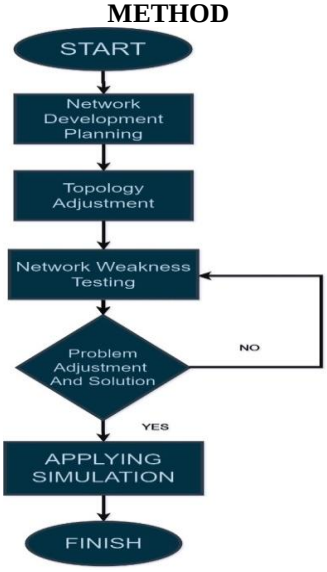

Figure 1. Flowchart Method

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, Number 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4199

Network Development Planning

This research method starts with Network Development Planning. At this stage, network security needs that can be addressed by Dynamic ARP Inspection (DAI) are identified. After these needs are identified, a feasibility analysis is performed to ensure that the implementation of DAI using Cisco Packet Tracer can be done with the available resources. A network architecture design was created to support the implementation of DAI, including the setup of switches, routers, and end devices.

Network Topology Adjustment

At this stage, the existing network topology is evaluated to identify weaknesses and areas that require improvement. Based on this evaluation, a new network topology is designed or the existing topology is customized to support DAI implementation. These adjustments are then applied to the network, including the device configurations and settings required to enable DAI.

Network Weakness Testing

Once the topology customization is complete, the next step is Network Weakness Testing. At this stage, network performance, security, and reliability testing is carried out to identify any weaknesses that may exist. This test aims to ensure that the DAI implementation does not reduce network performance, is effective in preventing ARP spoofing attacks, and that the network remains stable and functioning properly.

Problem Adjustment and Solution

If problems are found during testing, the next stage is Problem and Solution Adjustment. Problems found during testing are identified and analyzed to understand their cause and impact on the network. After that, solutions are designed and implemented to address the issues. Once the solution is implemented, network weakness testing is again conducted to ensure that the solution is effective.

Implementing Simulation

If the implemented solution successfully addresses the problem and the network is functioning properly, the next step is to Implement Simulation. At this stage, a network simulation model is created in Cisco Packet Tracer, including the Dynamic ARP Inspection configuration. The simulation is run to test how DAI works in near-real conditions. Simulation results are evaluated to ensure that the DAI implementation successfully improves network security as expected.

The implementation and research results are documented.

The last stage is Completion. In this stage, the entire implementation process and research results are documented. The tested and customized network configuration is then deployed into the production environment. Continuous monitoring is carried out to ensure that the network remains secure and functioning properly, and can handle future changes in requirements. By following these steps, this research method can help in developing, customizing, and testing the implementation of Dynamic ARP Inspection in Cisco Packet Tracer to effectively improve network security.

RESULT

Dynamic ARP Inspection (DAI)

Cisco Dynamic ARP Inspection or DAI is a layer 2 access switch security feature on Cisco. With this feature you can mitigate ARP Spoofing attacks, namely Man-in-Middle Attacks. ARP Spoofing is a technique in which a hacker / cracker will associate the MAC Address of the hacker's machine with the IP address of another machine, for example the Server IP address or MAC address of the default gateway.

Dynamic ARP Inspection (DAI) uses the DHCP Snooping binding database created by DHCP Snooping by listening to DHCP Messages between nodes. Based on the DHCP Snooping binding database, DAI decides what to do. If there is a record in the database of the sender's IP and MAC addresses, then the DAI receives an ARP packet. If there is no record in the database, the ARP packet is rejected.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4199

Network Devices

In running Cisco Packet Tracer simulations, it is necessary to set the network tool features. The list of network tool devices is in the following Table.

Table 1. Network Tool Devices

No	Network Devices	Total	Description
1	Router 2911	3	Configuration on IP for PC-PT with DHCP IP protocol
2	Switch 2960-24TT	2	Switch with 24 FastEthernet ports
3	PC-PT	4	Common user devices
4	Serial DTE	1	Wireless network or wireless for public places
5	Copper Straight-Through	7	Connecting cables used for Router 2911, Switch 2960-24TT, and PCs

Network System

The DHCP protocol is automatic after successfully setting the IP port on the 2911 Router. The configuration requires a Default IP Gateway which is required if you want to connect to all network devices. A list of default IP Gateway settings for types of computer and network devices in the following table.

Table 2. Network Sistem

No	Network Devices	IPv4 Address	Subnet Mask	Default Gateway	DNS Server
1	DHCP Server	172.16.10.9	255.255.255.0	-	-
2	R1	172.16.10.1 (Int Gig 0/0) & 172.16.12.1 (Int Gig 0/2/0)	255.255.255.0	-	-
3	R2	172.16.20.2 (Int Gig 0/0) & 172.16.12.2 (Int Gig 0/2/0)	255.255.255.0	-	-
2	PC-PT	172.16.20.101 -172.16.20.102 (DHCP)	255.255.255.0	172.16.20.2	172.16.10.9

Dynamic ARP Inspection (DAI) Configuration

To configure Dynamic ARP Inspection (DAI) on a Cisco switch, we will use the topology below.

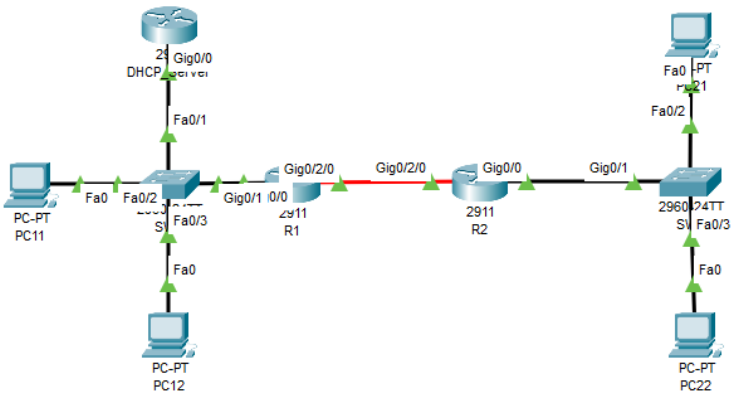

Figure 2. Cisco Topology

Note that the router configuration to provide DHCP service, which will dynamically assign IP addresses to endpoint devices in this topology has already been done. Dynamic ARP Inspection (DAI) will be performed through the VLAN on SW1 (Switch). To show the active VLAN on S1, click S1 and then enter the CLI tab. Then enter a command like this

SW1>en
SW1#sh vlan
Output:

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4199

```
SW1#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   VLAN0010                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Figure 3. Vlan Output

Here, we will configure DAI for VLAN 10. The next step is to enable DHCP snooping on the switch to prevent DHCP spoofing. DHCP Snooping works by the switch will register a legitimate port as a DHCP server and other than the legitimate port, the DHCP Offer, DHCP Acknowledge and DHCP Negative Acknowledge processes will be blocked so that the DHCP Rouge (fake) cannot provide an incorrect IP Address. The last command disables the addition of information 82 information. Option 82 is additional information added by the switch to DHCP messages to provide details about the physical location of the device (such as port and VLAN).

SW1#conf terminal
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 10
SW1(config)#no ip dhcp snooping information option

Configure ports on the switch to mark ports that can be trusted (connected to the DHCP server) and ports that cannot be trusted (connected to endpoint devices). In this example, the port of the DHCP Server, interface 0/1, will be configured to *Trust*. All hosts in VLAN 10 except those connected to a legitimate DHCP Server will be *Untrusted.*

SW1(config)#int fa 0/1
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#ip arp inspection trust
SW1(config-if)#ex

Then enable Dynamic ARP Inspection (DAI) on VLAN 10 to monitor and verify ARP packets.
SW1(config)#ip arp inspection vlan 10
Verify the Dynamic ARP Inspection (DAI) configuration on VLAN 10 by entering commands like this.
SW1(config)#do show ip arp inspection
Output:

```
SW1(config)#do show ip arp insp

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   10     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
   10     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   10              0              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
   10              0              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   10                    0                        0                      0
```

Figure 4. IP Arp Inspection

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4199

It can be seen from the picture above that the Dynamic ARP Inspection (DAI) configuration on VLAN 10 is enabled (active). There are several options that increase security when using DAI, namely validation of MAC, MAC source, and IP address but in this example it is not used. The goal will be to validate these fields in every request and response which can be enabled individually or as a group.

Verify DHCP Snooping Binding using MAC Address and IP Address on VLAN 10 by entering commands like this.

SW1(config)#do show ip dhcp snooping binding

Output:

```
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------------
02:00:BB:BB:12:12   172.16.10.121    86400       dhcp-snooping  10    FastEthernet0/3
02:00:BB:BB:11:11   172.16.10.122    86400       dhcp-snooping  10    FastEthernet0/2
Total number of bindings: 2
```

Figure 5. DHCP Snooping binder table / DHCP Snooping Binding

DHCP Snooping has bound the two end points that received configuration from the DHCP Server in the table above. The table includes the MAC Address, IP Address, VLAN and the interface to which each end point is connected. The implementation of Dynamic ARP Inspection (DAI) configuration can also be seen by showing each interface that can be trusted (connected to the DHCP server) is called Trusted and ports that cannot be trusted (connected to endpoint devices) are called Untrusted.

SW1(config)#do show ip arp inspection interface
Output:

```
SW1(config)#do show ip arp ins inter
Interface        Trust State     Rate(pps)    Burst Interval
---------------  -----------     ---------    --------------
Fa0/1            Trusted              15                 1
Fa0/2            Untrusted            15                 1
Fa0/3            Untrusted            15                 1
Fa0/4            Untrusted            15                 1
Fa0/5            Untrusted            15                 1
Fa0/6            Untrusted            15                 1
Fa0/7            Untrusted            15                 1
Fa0/8            Untrusted            15                 1
Fa0/9            Untrusted            15                 1
Fa0/10           Untrusted            15                 1
Fa0/11           Untrusted            15                 1
Fa0/12           Untrusted            15                 1
Fa0/13           Untrusted            15                 1
Fa0/14           Untrusted            15                 1
Fa0/15           Untrusted            15                 1
Fa0/16           Untrusted            15                 1
Fa0/17           Untrusted            15                 1
Fa0/18           Untrusted            15                 1
Fa0/19           Untrusted            15                 1
Fa0/20           Untrusted            15                 1
```

Figure 6. Interface IP Arp Inspection

It can be seen that interface Fa 0/1 is the only Trusted port because the port is connected to the DHCP Server which should provide a valid IP Address configuration to the end point. Interface Fa 0/2 to Fa0/20 is configured as Untrusted. So any response from this interface will be detected by the Dynamic ARP Inspection (DAI) mechanism. This interface will be validated for security depending on the options used, such as destination MAC Address validation, Source MAC Address, IP Address validation or a combination of the two and three options.

Dynamic ARP Inspection (DAI) is an excellent security feature, but before configuring DAI, we need to think and make some decisions based on the purpose, topology, and role of the device. We don't want to block critical traffic after enabling it.

DISCUSSION

The importance of simulating a network before building a physical network cannot be underestimated. In this context, simulation using Cisco Packet Tracer allows network administrators to test and verify security configurations such as Dynamic ARP Inspection (DAI) in a secure and controlled environment. Simulation allows testing of various configurations without risk to the production network. Administrators can detect and correct configuration errors that may not be apparent at first. This is especially important for security features such as DAI, which can cause network disruptions if not configured properly. With simulation, no additional hardware or expensive physical infrastructure is required. All testing is done virtually, which saves the cost and time required for setup and configuration changes on real hardware.

E-ISSN : 2807-9035
Volume 4, Number 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4199

Simulations provide an opportunity for administrators and students to understand how security protocols and features work under real conditions. This includes seeing how DAI verifies and blocks unauthorized ARP packets, as well as how DHCP Snooping works together with DAI to improve network security. By simulating attack scenarios such as ARP spoofing, administrators can test the network response and assess the effectiveness of the security features that have been implemented. This provides practical insight into how attacks can be prevented and mitigates the risks associated with such attacks.

Cisco Packet Tracer is an excellent tool for training and education. By using simulation, students and networking professionals can practice configuration and troubleshooting skills without the risk of damaging a real network. It also helps them prepare for real-world challenges. Simulation allows for better planning before physical network implementation. Administrators can plan network topologies, test failover scenarios, and ensure that the desired configuration works as intended before being deployed on a production network. Simulating a network using Cisco Packet Tracer provides the opportunity to perform various tests and verifications, which ultimately helps in building a more secure, efficient, and reliable network.

CONCLUSION

From the discussion above, it can be concluded that it is very important to carry out simulations in addition to learning simulations are very important because testing or experimenting with problems when building networks, because these experiments will not damage physical devices or damage real networks, besides that this use is important in education because it provides troubleshooting experience on the network and does not need to provide or wait for problems to provide an overview of network problems and there are still many features that can provide images of other problems, therefore it is important to apply the Cisco Packet Tracer simulation to various problems without having to give up the real network.

REFERENCES

Andrianto Putra, Asrar, Asrika Denalda, Desire Alfiyah Tuffahati, M. Adi Siswanto, Salwa Nurakmalia, Teja Suratman, Ukri Arianto, Yaldi Saputra, Jl Raya Puspitek, and Tangerang Selatan. 2023. "PENGENALAN SISTEM OPERASI DAN JARINGAN KOMPUTER DI SMK BINA PUTRA MANDIRI." *Jurnal Pengabdian Kepada Masyarakat* 1(1).

Anjelica, Amanda Ayu, and Siti Sulandjari. 2022. *PENGARUH PENGGUNAAN APLIKASI CISCO WEBEX UNTUK MENINGKATKAN PENGETAHUAN GIZI SEIMBANG PADA MAHASISWA JURUSAN PKK UNESA*. Vol. 02.

Anon. n.d.-a. "Pembelajaran Dan Pelatihan Jaringan Komputer Menggunakan Aplikasi Cisco Packet Tracer Sebagai Pembekalan Kompetensi Pada Siswa SMK Insan Cendikia."

Anon. n.d.-b. "Pendahuluan 4."

Arsalan, M. L. 2023. "Keamanan Jaringan Wireless Fidelity (Wi-Fi) Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus: PT Akurat Sentra MediaA." *Repository.Uinjkt.Ac.Id*.

Eka Putra, Fauzan Prasetyo, Taurina Jemmy Irwanto, and Ahmad Yudi Heryadi. 2019. "The Design and Implementation of Management Information System on Student Real Work (KKN) in Madura University." *International Journal of Civil Engineering and Technology* 10(2):159–75.

Eka Putra, Fauzan Prasetyo, Muhammad Umar Mansyur, Khana Zulfana Imam, and Sukron Katsir. 2023. "Optimalisasi Pengembangan Sistem Informasi Laboratorium Terintegerasi Sistem Akademik Menggunakan Metode Scrumb." *Jurnal Informatika* 23(2):183–98. doi: 10.30873/ji.v23i2.3749.

Informasi, Jurnal, Fauzan Prasetyo, Eka Putra, Moh Riski, Yayu Rahma Febriani, and Muhammad Umar Mansyur. 2024. "Optimization of Web Based Academic Information System Design to Increase Efficiency in Junior High Schools." 6:150–58. doi: 10.60083/jidt.v6i2.545.

Kemendikbud, Terakreditasi, Pudji Widodo, and Bambang Kelana Simpony. n.d. "J-INTECH (Journal of Information and Technology) Analisis Instalasi Jaringan Internet Desa Karangjati."

Morsy, Sabah M., and Dalia Nashat. 2022. "D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing." *IEEE Access* 10:49142–53. doi: 10.1109/ACCESS.2022.3172329.

Pembuatan Simulasi Jaringan Komputer Dengan Gns, Pelatihan, Dan Cisco Packet Tracer Kepada Para Guru SMKS Yapinuh Muara Gembong Kabupaten Bekasi Jawa Barat, Ali Idrus, Lipur Sugiyanta, Murien Nugraheni, Olifvia Afrillazhary, Zahwa Putri Rahmayani, and Sistem dan Teknologi. 2022. "Training In Making Computer Network Simulation With Gns3 And Cisco Packet Tracer To Teachers Of Yapinuh Smks Muara Gembong, Bekasi Regency, West Java." doi: 10.30645/.v1i1.

Prakoso, Gilang, and Aulia Khamas Heikmakhtiar. 2024. "Analisis Keamanan Jaringan: ARP Spoofing Dan DNS Spoofing Dengan Metode National Institute of Standards and Technology." *Journal on Education* 06(02):12895–902.

Prasetyo, Fauzan, Alief Badrit Tamam, Reynal Widya Efendi, MZaini Mun, Kata Kunci, Jaringan Komputer, and Keamanan Jaringan. 2024. "Pertahanan Tingkat Server Terhadap Serangan Dns Spoofing Di Jaringan Modern."

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4199

14(2):80–149.

Prasetyo, Fauzan, Eka Putra, Ahmad Muzayyin, and Muhammad Umar Mansyur. 2024. "Analisis Kualitas Layanan Absensi Berbasis Finger Berdasarkan Quality Of Service." 24(1):17–25.

Publikasi, Abdi Jurnal, Abdullah Al Ghifari, Aditya Rizqiandri Saputra, Alif Nur Qalbani, Arief Nur Febrianto, Gilang Nur Dwiansyah, Hendrik Louis Mahdi, Irfan Maulana, Muhammad Alfito, Risky Pratama, Muhammad Rizal, and Provinsi Banten. 2023. "SOSIALISASI PEMBUATAN JARINGAN LOKAL DI SMK TRI DHARMA 3 KOTA BOGOR." 1(3):305–8.

Resi, Nene Helena, Zet Y. Baitanu, and Crispinus P. Tamal. n.d. "Pengaruh Penggunaan Media Cisco Packet Tracer Terhadap Hasil Belajar Di SMK Negeri 4 Kupang."

Salsabila, Adinda, and Tata Sutabri. 2024. "IJM: Indonesian Journal of Multidisciplinary Analisis Pembelajaran Teknologi Jaringan Untuk Mengetahui Simulasi Jaringan Dengan Menggunakan Switch Dan Router Di Aplikasi Cisco Packet Tracer." *IJM: Indonesian Journal of Multidisciplinary* 2.

Saputri, Octaviani, and Ratna Dewi Kartikasari. n.d. *"Analisis Efektivitas Penggunaan Aplikasi Simulator Cisco Packet Tracer Pada Mahasiswa Teknik Informatika Di Universitas Muhammadiyah Jakarta "*.

Sun, Yuwei, Hideya Ochiai, and Hiroshi Esaki. 2022. "Suspicious ARP Activity Detection and Clustering Based on Autoencoder Neural Networks." *Proceedings - IEEE Consumer Communications and Networking Conference, CCNC* 743–44. doi: 10.1109/CCNC49033.2022.9700697.

Sutiyono, Tion, Imroatul Karimah, Taufik Hidayat, and Ali Miftakhu Rosyad. 2024. "Pelatihan Topologi Jaringan Pada Sekolah Berbasis Cisco Paket Tracer." *Jurnal Pengabdian Masyarakat Sultan Indonesia* 1(2):9–15. doi: 10.58291/abdisultan.v1i2.203.