المؤتمر العلمي الأول للتطبيقات الهندسية (ICEA'2024)

The First Scientific Conference on Engineering Applications (ICEA'2024)

Conference homepage: www.icea.ly

Network Monitoring Using Port-Mirroring Technology (SPAN and RSPAN)

*Reema Alshebani Saad, Fatima Bashir Alkekli, Hibah Basheer Gshera

Department Of Computer Network , Faculty of Information Technology ,Tripoli University ,Tripoli, Libya

Keywords:

ASDM
GNS3
Port Mirroring
RSPAN
SPAN
switch
VPN
Wireshark

ABSTRACT

This paper includes the creation of an integrated network consisting of two branches, where a network is designed and linked using virtual networks, monitored and analyzed using monitoring and analysis tools. The analysis results identify network errors and propose solutions, if possible-for example, a particular server stops, the user is unable to reach a certain destination within the network, the loss of transmitted data and not reaching the destination are some of the most common network errors that may occur within a network that lead to poor network service quality. VPN (Virtual private network) techniques have been used, which provide the creation of a protected network connection when using public networks, where they encrypt network traffic on the Internet and hide electronic identity, which makes tracking online activity and data theft very difficult. One of the monitoring techniques was used (Port Mirroring) where a copy of the traffic is sent to a separate port for monitoring and analysis to help detect network failures without affecting the traffic flow. This technique will improve network performance and save time and effort wasted in searching for the cause of the problem in the network. The results show the impact of using Port Mirroring and VPN techniques to improve the security of the network by analyzing access to the network and identifying potential issues before they occur , detecting malicious activities and protecting the data when it was transmitted over the Internet.

مر اقبة الشبكة باستخدام تقنية نسخ المنفذ (تحليل منفذ المبدل ,تحليل منفذ المبدل عن بعد)

*ريما الشيباني سعد و فاطمة بشير الككلي و هبة بشير قشيره

قسم شبكات الحاسوب, كلية تقنية المعلومات, جامعة طرابلس ,طرابلس ,ليبيا

الكلمات المفتاحية:

مدير جهاز الأمان التكيفي
برنامج محاكاة الشبكة الرسومية
نسخ المنفذ
تحليل منفذ المبدل عن بعد
المبدل
تحليل منفذ المبدل
الشبكة الخاصة الافتراضية
اداة تحليل بيانات الشبكة

الملخص

يتضمن هذا البحث إنشاء شبكة متكاملة تتكون من فرعين، حيث يتم تصميم الشبكة وربطها باستخدام الشبكات الافتراضية، ومراقبتها وتحليلها باستخدام أدوات المراقبة والتحليل. تحدد نتائج التحليل أخطاء الشبكة وتقترح الحلول، إن أمكن - على سبيل المثال، توقف خادم معين، عدم قدرة المستخدم على الوصول إلى وجهة معينة داخل الشبكة، فقدان البيانات المرسلة وعدم وصولها إلى الوجهة هي بعض من أكثر أخطاء الشبكة شيوعًا التي قد تحدث داخل الشبكة والتي تؤدي إلى جودة خدمة شبكة سيئة. تم استخدام تقنيات الشبكة الافتراضية الخاصة، التي توفر إنشاء اتصال شبكة محمي عند استخدام الشبكات العامة، حيث تقوم بتشفير حركة مرور الشبكة على الإنترنت وإخفاء الهوية الإلكترونية، مما يجعل تتبع النشاطات عبر الإنترنت وسرقة البيانات أمرًا صعبًا للغاية. تم استخدام إحدى تقنيات المراقبة (نسخ المنفذ) حيث يتم إرسال نسخة من الحركة إلى منفذ منفصل للمراقبة والتحليل للمساعدة في اكتشاف أعطال الشبكة دون التأثير على تدفق الحركة. ستُحسّن هذه التقنية أداء الشبكة وتوفر الوقت والجهد المبذولين في البحث عن سبب المشكلة في الشبكة. تُظهر النتائج تأثير استخدام تقنيات نسخ المنافذ والشبكات الافتراضية الخاصة (VPN) لتحسين أمان الشبكة من خلال تحليل الوصول إلى الشبكة وتحديد المشكلات المحتملة قبل حدوثها، واكتشاف الأنشطة الضارة وحماية البيانات عند نقلها عبر الإنترنت.

1. Introduction

Tools for network monitoring and analysis are becoming more and more necessary as networks continue to expand. The administrators' responsibilities extend beyond preventing network failure due to network overload or external threats and promptly resolving network

*Corresponding author:

E-mail addresses: Ranem_reem@yahoo.com, (F. Alkekli) fatima.basher.kk@gmail.com, (H. Gshera) hebagshera@gmail.com

Article History : Received 25 March 2024 - Received in revised form 20 September 2024 - Accepted 15 October 2024

issues [1]. The administrator uses the network traffic data to serve his or her purposes. For instance, network utilization and network traffic characteristics can be used to identify security flaws, and the type of application that uses the most bandwidth can be taken into account when planning a network. [1]. Network traffic can be seen using a technique called port mirroring, sometimes referred to as SPAN (Switched Port Analyzer). The switch delivers a copy of every network packet observed on one port (or an entire VLAN (Virtual Local Area Network)) to another port when port mirroring is activated, allowing Wireshark Software to analyze the packet [2]. The main objective of this study is to develop a switch port mirror giving detailed information about the network of modern systems and technology. This technique enables the network administrator to view the entire mirror port, to perform control and monitor in real-time, to find LAN (Local Area Network) traffic and failure. As an administrator, we need to monitor and detect the problem with traffic on the network. This monitoring, enables for ensuring security in the network [3]. To carry out its functions, the network monitor system typically uses packet.

interception, protocol analysis, address filtering, cheating, etc. These techniques need additional time during the typical data transmission process, which could have an impact on network performance, particularly when a network is busy and the monitor server is performing poorly.

2. Network switch

Devices on LAN are connected by use of a network switch . The same fundamental tasks carried out by a bridge are also carried out by a switch, albeit at considerably higher speeds and with many more characteristics. A switch's ports can operate in full duplex mode and are each in their own collision domain, allowing connected hosts to send to the switch at the same time that the switch is transmitting to them.

Typically, an Ethernet switch operates at the OSI model's(Open Systems Interconnection Model) data link layer (Layer 2). By looking at the incoming frame's destination MAC address(Media Access Control Address) and only forwarding the frame to the host that the message was intended for, it controls the flow of data across a network. The MAC address table, a dynamic table found in every switch, assigns MAC addresses to ports. A switch can determine which system is sitting on which port and where to deliver the received frame using this information [4].

1. Type of switch

1. Layer 2 switches*:* Layer 2 switches primarily work on switching, therefore they use the MAC addresses of connected devices to reroute data packets from the source port to the destination port. To remember which ports are assigned which MAC addresses, it is done by keeping a MAC address table. Within Layer 2 of the OSI reference model, a MAC address operates. Each device is assigned a unique MAC address, which serves as a simple means of differentiating one from another. To manage traffic in a LAN, it uses hardware-based switching algorithms. Because Layer 2 switching merely sorts MAC addresses at a physical layer, the procedure is quite quick. A Layer 2 switch essentially serves as a bridge between several devices. [5]

2.Layer 3 switch: A Layer 3 switch operates in the exact opposite manner from a Layer 2 switch. Data packets cannot be routed by layer 2 switches. Layer 3 switches use IP (Internet Protocol) addresses for routing, not Layer 2 switches. It is a specialized hardware tool used for data packet routing. Fast switching is possible on Layer 3 switches, and they have more ports. They significantly outperform older routers in terms of performance. The main benefit of using Layer 3 switches is that they can route data packets without requiring additional network hops, making them faster than routers. However, they are missing a few extra router features. Large-scale businesses frequently employ them. To put it simply, a Layer 3 switch is nothing more than a fast router devoid of WAN (Wide Area Network) connectivity [5].

Layer-specific functionality is a feature that many contemporary commercial switches include. Multiport layer-2 bridging is an Ethernet switch's primary purpose. A lot of switches also conduct activities at higher tiers. A multilayer switch is a device with additional functionality to bridging. Switches may acquire knowledge of topologies at numerous layers and transmit at one or more layers [7].

1. **Layer 1 :** A physical layer switch, also known as a Layer 1 switch, functions at the physical layer of the OSI model. A Layer 1 switch does not read, modify, or use packet/frame headers while routing data. Layer 1 switches often have very minimal latency and are totally transparent to the traffic.
2. **Layer 2:** A layer 2 switch is a specific kind of network switch or device that operates at OSI Layer 2's data connection layer and uses the MAC Address to identify the direction the frames should take when being forwarded. A layer 2 switch is largely in charge of carrying out error checking on each sent and received frame as well as data transfer on the physical layer. To transmit data, the switch needs the MAC address of the NIC (Network Interface card) on each network node. It automatically acquires MAC addresses by copying the MAC address from each frame it receives, or it listens to network devices and keeps track of their MAC addresses in a forwarding table.
3. **Layer 3:** A Layer 3 switch is an Ethernet switch that switches packets based on both their physical address and their network address (for instance, their IP or IPX (Internetwork Packet Exchange) address (for example, their MAC address). This kind of switch functions at the OSI reference model's network layer (layer 3), as well as the data-link layer (layer 2). For the construction of sophisticated, high-speed Ethernet networks, a Layer 3 switch combines the speed of an Ethernet switch with some of the features of a router [12].
4. **Layer 4:** A layer 4 switch, commonly referred to as a session switch, offers policy-based switching mechanisms that restrict certain traffic kinds and prioritize packets based on the value of the base application. A layer 4 switch is one of the different kinds of multilayer switches and is an improvement over a layer 3 switch that employs switching methods based on hardware.
5. Layer 5: A layer 5 switch decides how to initiate, control, and end a session between the two systems [13].
6. Layer 6: In a layer 6 switch, data formats are specified. This layer is responsible for operations like encryption and compression [13].
7. Layer 7: Having both routing and switching capabilities, a Layer 7 switch is a network device. Even though it operates at Layer 2 speed and uses Layer 7 or application layer data, it can nevertheless pass traffic and make forwarding and routing decisions. It's also known as a Layer 4-7 switch, a content switch, a content service switch, a web switch, and an application switch [11].

3. Network Security Solution

Hundreds of network security management technologies are also available to handle specific threats or exploits or to help with other mission-critical infrastructure requirements like ongoing compliance. Employing a platform approach that puts integration and automation first, organizations should give top priority to network security solutions that address the wide range of threats [19].

1. **Firewall**:

is a network device that separates a company's internal network from the Internet and other external networks. To restrict illegal access to or from the internal network, a hardware, software, or combination system may be used [20].

2. **VPN:**

An encrypted connection between a device and a network via the Internet is known as a virtual private network, or VPN. Secure transmission of sensitive data is aided by the encrypted connection. It makes it impossible for unauthorized parties to eavesdrop on the traffic and enables remote work for the user. In corporate settings, VPN technology is frequently employed [22].

3. **Traffic Network Monitoring:**

The security of a network is considerably enhanced by a monitoring solution. For the IT(Information technology) team, the solution's report of a rapid surge in traffic levels that considerably depart from the usual might be a key indicator of potential malware or phishing attacks[23].

4. **Port Mirror:**

Network packets delivered as input from one port to another port of a monitoring computer, switch, or device are copied and sent using the port mirroring technique. It is a method of network monitoring that is used with network switches and other related hardware [24]. SPAN and RSPAN (Remote Switch Port Analyzer) are further names for port mirroring [24] . The port mirroring method was used throughout this paper.

1. **Port Mirroring (SPAN) Terminology:**

1. Ingress traffic: is the flow of traffic into the switch.
2. Egress traffic: Traffic that leaves the switch.
3. Source (SPAN) port: A port that is monitored by use of the SPAN function.`
4. Source (SPAN) VLAN: A VLAN whose traffic is monitored using the SPAN function.
5. Destination (SPAN) port: Usually attached to a network analyzer, this port monitors the source ports. [29]. **Fig 1** shows the place of each port.

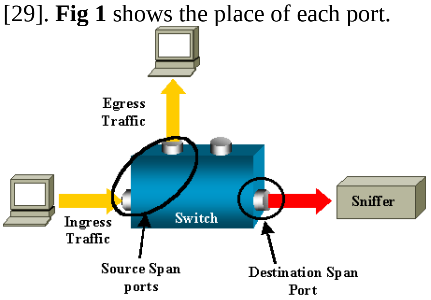


Fig.1: Terminology of Port Monitoring

2. **Port mirroring types :**

There are two types of port mirroring: local and remote port mirroring (SPAN and RSPAN), which have different mirroring ranges. They operate according to different principles [30].

1. **Local SPAN** : The most basic type of mirroring is local port mirroring. The same network device that hosts the destination ports also hosts all of the source ports. Local port mirroring allows the network switch to send a copy of the packet from the source port (Eth 1/1) to the destination port (Eth 1/2), as seen in figure 1. the packet can then be monitored and analyzed by the monitoring device connected to the destination port. [30]. **Fig 2** shows how the local SPAN works.

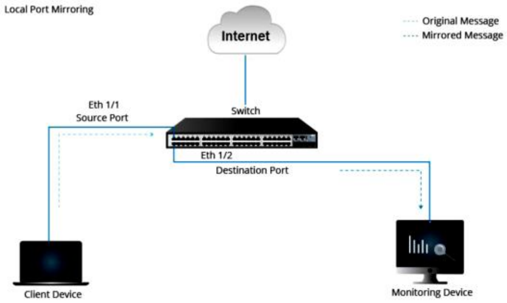


Fig.2: Local SPAN

Traffic is mirrored from a SPAN source. It could include one or more of the following:

1. Access switch ports.
2. Trunk ports.
3. Routed interfaces.
4. Ether Channels.
5. Entire VLANs.

SPAN has the ability to mirror both inbound and outbound traffic on a source. The place to which traffic is mirrored is a SPAN destination. It is exclusively intended for that use and can only have one switch port. The port cannot be a SPAN source port and can only take part in one SPAN session. The bandwidth of the SPAN destination port may be exceeded by the traffic from the SPAN source. For example, a single Gigabit Ethernet port's capacity can easily be exceeded by a SPAN source for an entire VLAN. Moreover, an Ether Channel as a SPAN destination is not supported by the majority of Cisco platforms. For the limited models that do, the Ethernet Channel should be manually configured as on port aggregation protocols are not supported [27].

2. **Remote SPAN (RSPAN):**

RSPAN enables the SPAN source and destination to be located on several switches. Setting up an RSPAN VLAN is required for the mirrored traffic to be transferred from switch to switch through this VLAN [27].

As **Fig 3** shows, source port (Eth 1/3) is on one switch, and destination port (Eth 1/3) is on the other switch. Using the uplink connection made possible by the port (Eth 1/4) on the two switches, the source port transfers the packet copy to the destination port. As a result, local port mirroring enables device-wide data monitoring and analysis. [30]. **Fig 3** shows how the Remote SPAN works.

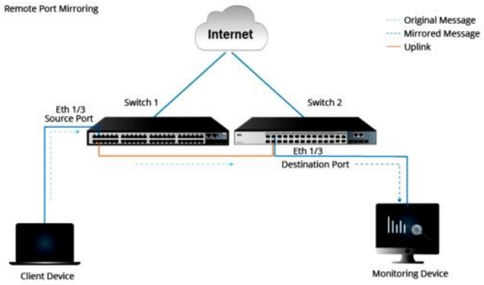


Fig .3: Remote SPAN

3. **The benefit of using a port mirroring solution:**

The cost of the port-mirroring solution, which comes with most managed switches on the market for free, as well as how simple it is to use and how easily it can be adjusted remotely, are its main benefits [31]. This benefit indicates why the port mirroring technique has become a popular technique to get packet traces for various purposes. Switches are not too impacted by port mirroring, according to Cisco Systems, the top manufacturer of network switches. Mirroring merely replicates an output that the switch was already required to process, thus it is not required to process the additional stream [31].

4. **Challenges with port mirroring:**

Data confidentiality issues could arise during full packet capture and storage. Even while the majority of network data will be encrypted if it is going to external sites, not all internal traffic will be. The network's mail traffic won't be encrypted by default unless a company adds additional security for emails [32].

4. **Implementation Phases**:

This section explains all the settings and techniques implemented to get a more secure network; it begins with:

1. **Software used in this paper**

the software used in the paper to monitor network performance are:

1. **GNS3(Graphical Network Simulator-3)**

An open-source tool that simulates networks while coming as close as possible to the behavior of real networks.

2. **VMWare Workstation (Virtual Machine software)**

Virtualization software like VMware Workstation program enables running multiple operating systems on one pc (personal computer).

3. **Wireshark**

A network packet analyzer displays collected packet data in as much detail as feasible.

4. **ASDM (Adaptive Security Device Manager)**

Cisco's GUI (Graphical User Interface) for managing Cisco ASA (Adaptive Security Appliance) security appliances is called ASDM.

2. **Network Design:**

The network design for this project that was built with GNS3 software is shown in **Fig 4**.

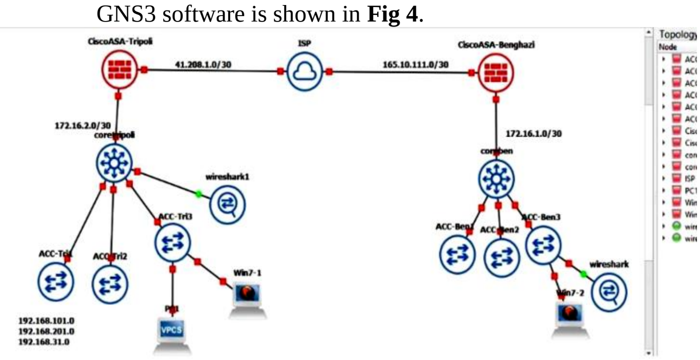
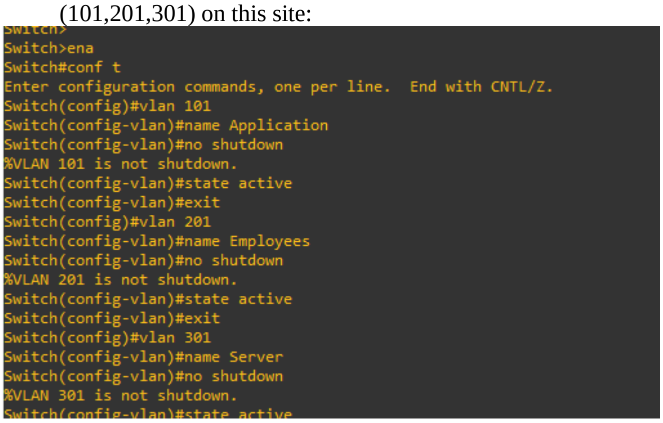


Fig.4: Network Design Using GNS3

1. **In core switch in left side** *:*

The **Fig.5.** shows the configuration of adding the Vlans (101,201,301) on this site:

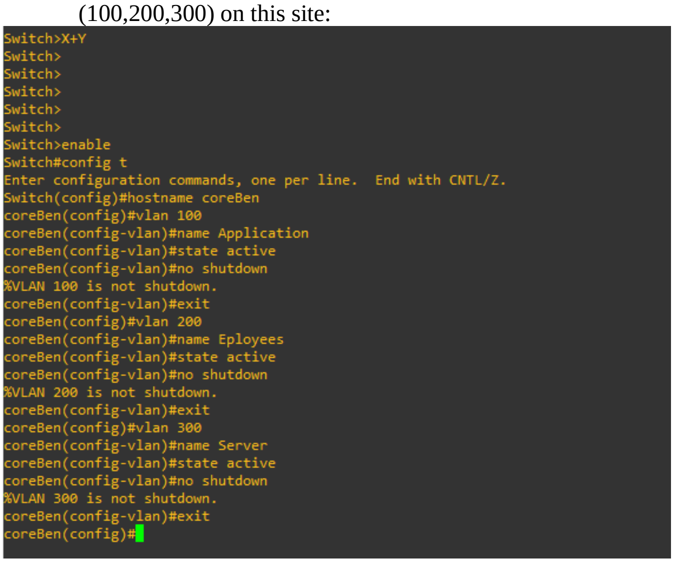


```
Switch>
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 101
Switch(config-vlan)#name Application
Switch(config-vlan)#no shutdown
%VLAN 101 is not shutdown.
Switch(config-vlan)#state active
Switch(config-vlan)#exit
Switch(config)#vlan 201
Switch(config-vlan)#name Employees
Switch(config-vlan)#no shutdown
%VLAN 201 is not shutdown.
Switch(config-vlan)#state active
Switch(config-vlan)#exit
Switch(config)#vlan 301
Switch(config-vlan)#name Server
Switch(config-vlan)#no shutdown
%VLAN 301 is not shutdown.
Switch(config-vlan)#state active
```

Fig.5.: Vlan Configuration in Core switch in left side

2. **In core switch in right side***:*

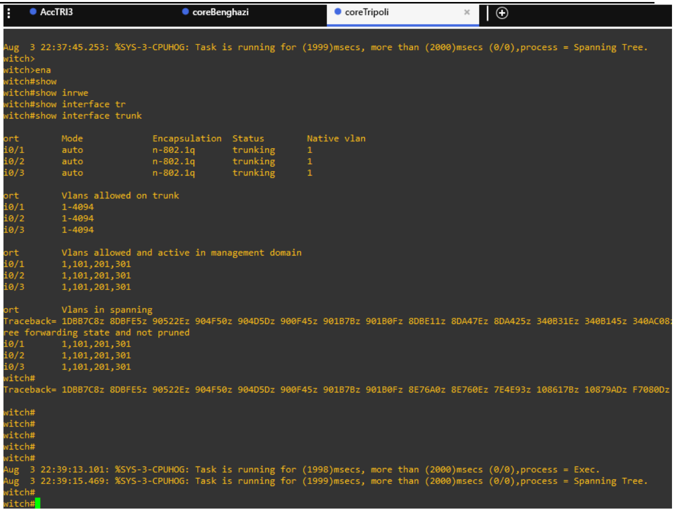
Fig (6). shows the configuration of adding the Vlans (100,200,300) on this site:



```
Switch>X+Y
Switch>
Switch>
Switch>
Switch>
Switch>
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname coreBen
coreBen(config)#vlan 100
coreBen(config-vlan)#name Application
coreBen(config-vlan)#state active
coreBen(config-vlan)#no shutdown
%VLAN 100 is not shutdown.
coreBen(config-vlan)#exit
coreBen(config)#vlan 200
coreBen(config-vlan)#name Eployees
coreBen(config-vlan)#state active
coreBen(config-vlan)#no shutdown
%VLAN 200 is not shutdown.
coreBen(config-vlan)#exit
coreBen(config)#vlan 300
coreBen(config-vlan)#name Server
coreBen(config-vlan)#state active
coreBen(config-vlan)#no shutdown
%VLAN 300 is not shutdown.
coreBen(config-vlan)#exit
coreBen(config)#
```

Fig.6.: Shows Vlan Configuration in core switch in right side

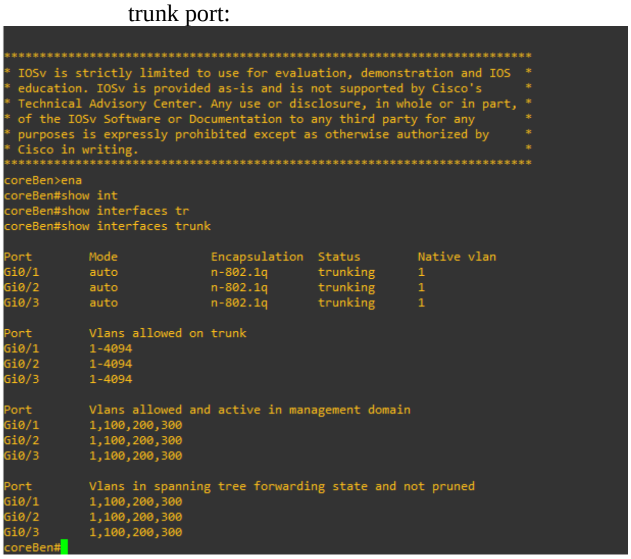
3. **In core switch in left side :** Fig (7) shows the all trunk port:



```
Aug  3 22:37:45.253: %SYS-3-CPUHOG: Task is running for (1999)msecs, more than (2000)msecs (0/0),process = Spanning Tree.
witch>
witch>ena
witch#show
witch#show inrwe
witch#show interface tr
witch#show interface trunk

ort       Mode             Encapsulation  Status        Native vlan
i0/1      auto             n-802.1q       trunking      1
i0/2      auto             n-802.1q       trunking      1
i0/3      auto             n-802.1q       trunking      1

ort       Vlans allowed on trunk
i0/1      1-4094
i0/2      1-4094
i0/3      1-4094

ort       Vlans allowed and active in management domain
i0/1      1,101,201,301
i0/2      1,101,201,301
i0/3      1,101,201,301

ort       Vlans in spanning
Traceback= 1DBB7C8z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 901B7Bz 901B0Fz 8DBE11z 8DA47Ez 8DA425z 340B31Ez 340B145z 340AC08z
ree forwarding state and not pruned
i0/1      1,101,201,301
i0/2      1,101,201,301
i0/3      1,101,201,301
witch#
Traceback= 1DBB7C8z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 901B7Bz 901B0Fz 8E76A0z 8E760Ez 7E4E93z 108617Bz 10879ADz F7080Dz

witch#
witch#
witch#
witch#
witch#
Aug  3 22:39:13.101: %SYS-3-CPUHOG: Task is running for (1998)msecs, more than (2000)msecs (0/0),process = Exec.
Aug  3 22:39:15.469: %SYS-3-CPUHOG: Task is running for (1999)msecs, more than (2000)msecs (0/0),process = Spanning Tree.
witch#
witch#
```

Fig.7. :show Vlan Command in core switch in left side

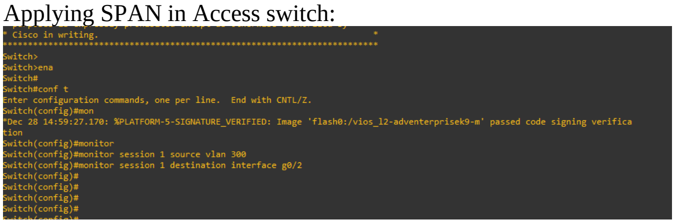
4. **In core switch in right side:** Fig (8) shows the all trunk port:



```
**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************
coreBen>ena
coreBen#show int
coreBen#show interfaces tr
coreBen#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/1       auto             n-802.1q       trunking      1
Gi0/2       auto             n-802.1q       trunking      1
Gi0/3       auto             n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gi0/1       1-4094
Gi0/2       1-4094
Gi0/3       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1,100,200,300
Gi0/2       1,100,200,300
Gi0/3       1,100,200,300

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1,100,200,300
Gi0/2       1,100,200,300
Gi0/3       1,100,200,300
coreBen#
```

Fig.8.: Show Vlan Command in In core switch in right side

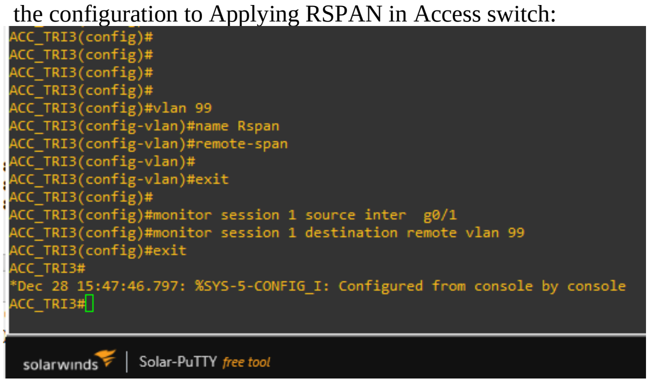
1. **SPAN:** Select the source which is the VLAN that has been monitored and the destination is the port to which the network analyzer is connected to it. Fig (9) shows the configuration to Applying SPAN in Access switch:



```
* Cisco in writing.                                                      *
**************************************************************************
Switch>
Switch>ena
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#mon
*Dec 28 14:59:27.170: %PLATFORM-5-SIGNATURE_VERIFIED: Image 'flash0:/vios_l2-adventerprisek9-m' passed code signing verifica
tion
Switch(config)#monitor
Switch(config)#monitor session 1 source vlan 300
Switch(config)#monitor session 1 destination interface g0/2
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
```

Fig.9.: Shows How to Apply SPAN in Access Switch

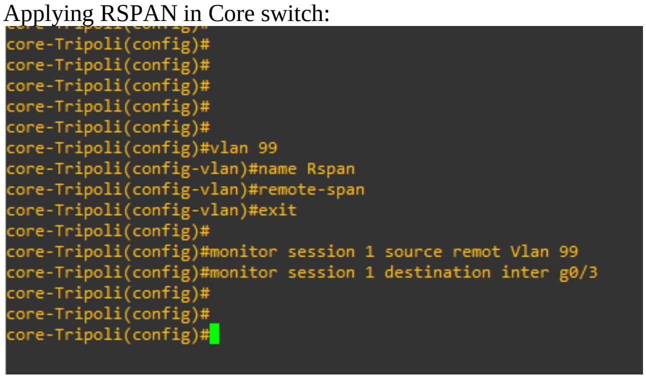
2. **RSPAN:** the same with rspan Select the source and destination and create VLAN with the same id in both switches the source here is the port has been monitored and the destination is the VLAN that been create. Fig (10) shows the configuration to Applying RSPAN in Access switch:



```
ACC_TRI3(config)#
ACC_TRI3(config)#
ACC_TRI3(config)#
ACC_TRI3(config)#
ACC_TRI3(config)#vlan 99
ACC_TRI3(config-vlan)#name Rspan
ACC_TRI3(config-vlan)#remote-span
ACC_TRI3(config-vlan)#
ACC_TRI3(config-vlan)#exit
ACC_TRI3(config)#
ACC_TRI3(config)#monitor session 1 source inter  g0/1
ACC_TRI3(config)#monitor session 1 destination remote vlan 99
ACC_TRI3(config)#exit
ACC_TRI3#
*Dec 28 15:47:46.797: %SYS-5-CONFIG_I: Configured from console by console
ACC_TRI3#
```

Fig.10.: Shows How to Apply RSPAN in Access Switch

Select the source which is the VLAN has been created in both switches, and the destination is the port to which the network analyzer is connected to it. Fig (11) shows the configuration to Applying RSPAN in Core switch:

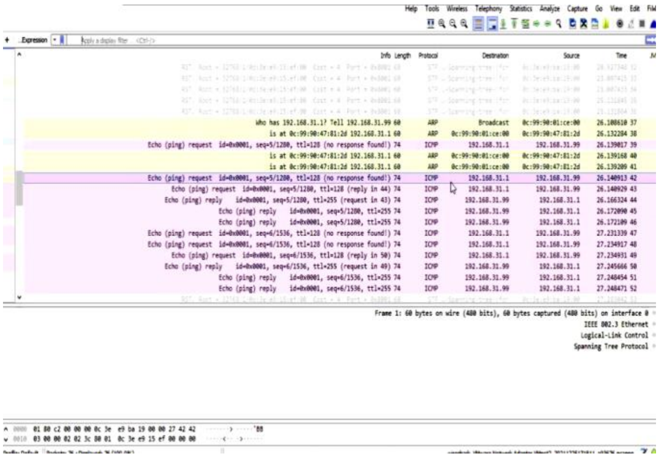


```
core-Tripoli(config)#
core-Tripoli(config)#
core-Tripoli(config)#
core-Tripoli(config)#
core-Tripoli(config)#
core-Tripoli(config)#vlan 99
core-Tripoli(config-vlan)#name Rspan
core-Tripoli(config-vlan)#remote-span
core-Tripoli(config-vlan)#exit
core-Tripoli(config)#
core-Tripoli(config)#monitor session 1 source remot Vlan 99
core-Tripoli(config)#monitor session 1 destination inter g0/3
core-Tripoli(config)#
core-Tripoli(config)#
core-Tripoli(config)#
```

Fig.11.: (Shows How to Apply RSPAN in Core Switch)

5. RESULTS:

1. **In core switch in left side :** Fig (12) shows the result of the Wireshark ping command, which illustrate this process, when it happened, the source IP address and the destination IP address, as well as the protocols used when executing this command & some information of the data:

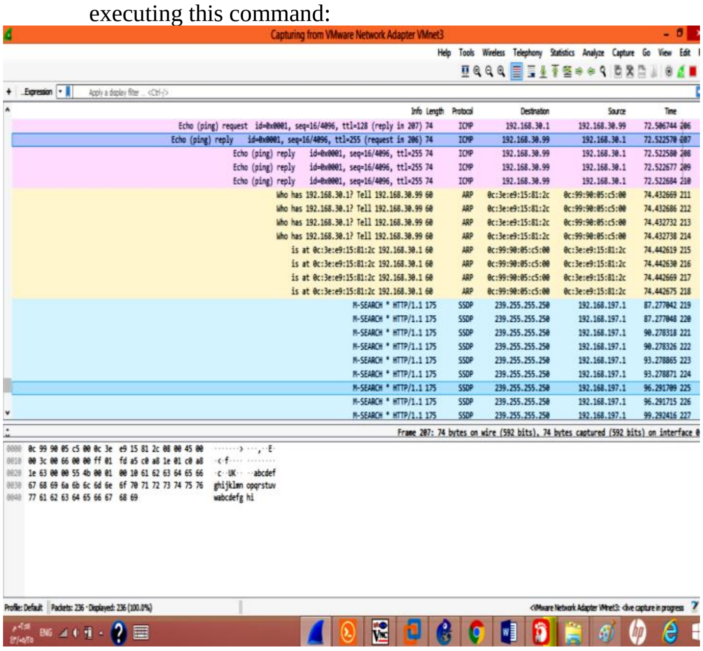


Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
Expression
Apply a display filter ... <Ctrl-/>

```
                                                     Info Length  Protocol      Destination            Source          Time
                        Who has 192.168.31.1? Tell 192.168.31.99 60  ARP          Broadcast  0c:99:90:01:ce:00  26.108610 37
                          is at 0c:99:90:47:81:2d 192.168.31.1 60  ARP  0c:99:90:01:ce:00  0c:99:90:47:81:2d  26.132284 38
Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (no response found!) 74  ICMP  192.168.31.1  192.168.31.99  26.139017 39
                          is at 0c:99:90:47:81:2d 192.168.31.1 60  ARP  0c:99:90:01:ce:00  0c:99:90:47:81:2d  26.139168 40
                          is at 0c:99:90:47:81:2d 192.168.31.1 60  ARP  0c:99:90:01:ce:00  0c:99:90:47:81:2d  26.139209 41
Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (no response found!) 74  ICMP  192.168.31.1  192.168.31.99  26.140913 42
    Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 44) 74  ICMP  192.168.31.1  192.168.31.99  26.140929 43
   Echo (ping) reply    id=0x0001, seq=5/1280, ttl=255 (request in 43) 74  ICMP  192.168.31.99  192.168.31.1  26.166324 44
            Echo (ping) reply    id=0x0001, seq=5/1280, ttl=255 74  ICMP  192.168.31.99  192.168.31.1  26.172090 45
            Echo (ping) reply    id=0x0001, seq=5/1280, ttl=255 74  ICMP  192.168.31.99  192.168.31.1  26.172109 46
Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (no response found!) 74  ICMP  192.168.31.1  192.168.31.99  27.231339 47
Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (no response found!) 74  ICMP  192.168.31.1  192.168.31.99  27.234917 48
    Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 50) 74  ICMP  192.168.31.1  192.168.31.99  27.234931 49
   Echo (ping) reply    id=0x0001, seq=6/1536, ttl=255 (request in 49) 74  ICMP  192.168.31.99  192.168.31.1  27.245666 50
            Echo (ping) reply    id=0x0001, seq=6/1536, ttl=255 74  ICMP  192.168.31.99  192.168.31.1  27.248454 51
            Echo (ping) reply    id=0x0001, seq=6/1536, ttl=255 74  ICMP  192.168.31.99  192.168.31.1  27.248471 52

                    Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
                                                                                IEEE 802.3 Ethernet
                                                                               Logical-Link Control
                                                                             Spanning Tree Protocol

0000  01 80 c2 00 00 00 0c 3e  e9 ba 19 00 00 27 42 42   ......>.....'BB
0010  03 00 00 02 02 3c 00 01  0c 3e e9 15 ef 00 00 00
```

Fig.12.: Shows Ping Command Result in GNS3

2. **In core switch in right side:** Fig (13) shows the result of ping command in the Wireshark, which illustrate this process, when it happened, the source IP address and the destination IP address, as well as the protocols used when executing this command:

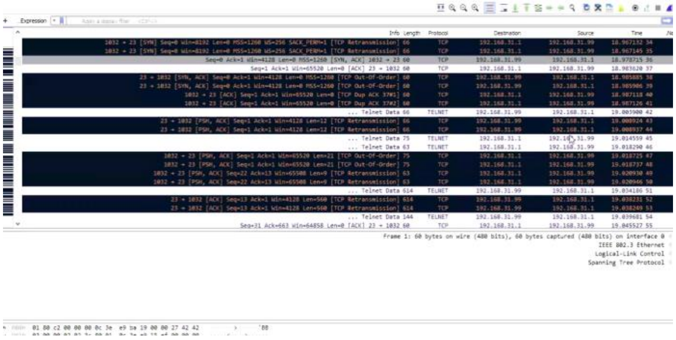


Capturing from VMware Network Adapter VMnet3
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit
Expression
Apply a display filter ... <Ctrl-/>

```
                                                       Info Length  Protocol      Destination            Source           Time
Echo (ping) request  id=0x0001, seq=16/4096, ttl=128 (reply in 207) 74  ICMP     192.168.30.1     192.168.30.99  72.506744 206
  Echo (ping) reply    id=0x0001, seq=16/4096, ttl=255 (request in 206) 74  ICMP  192.168.30.99   192.168.30.1   72.522570 207
          Echo (ping) reply    id=0x0001, seq=16/4096, ttl=255 74  ICMP  192.168.30.99      192.168.30.1       72.522580 208
          Echo (ping) reply    id=0x0001, seq=16/4096, ttl=255 74  ICMP  192.168.30.99      192.168.30.1       72.522677 209
          Echo (ping) reply    id=0x0001, seq=16/4096, ttl=255 74  ICMP  192.168.30.99      192.168.30.1       72.522684 210
                 Who has 192.168.30.1? Tell 192.168.30.99 60  ARP  0c:3e:e9:15:81:2c  0c:99:90:05:c5:00  74.432669 211
                 Who has 192.168.30.1? Tell 192.168.30.99 60  ARP  0c:3e:e9:15:81:2c  0c:99:90:05:c5:00  74.432686 212
                 Who has 192.168.30.1? Tell 192.168.30.99 60  ARP  0c:3e:e9:15:81:2c  0c:99:90:05:c5:00  74.432732 213
                 Who has 192.168.30.1? Tell 192.168.30.99 60  ARP  0c:3e:e9:15:81:2c  0c:99:90:05:c5:00  74.432738 214
                   is at 0c:3e:e9:15:81:2c 192.168.30.1 60  ARP  0c:99:90:05:c5:00  0c:3e:e9:15:81:2c  74.442619 215
                   is at 0c:3e:e9:15:81:2c 192.168.30.1 60  ARP  0c:99:90:05:c5:00  0c:3e:e9:15:81:2c  74.442630 216
                   is at 0c:3e:e9:15:81:2c 192.168.30.1 60  ARP  0c:99:90:05:c5:00  0c:3e:e9:15:81:2c  74.442669 217
                   is at 0c:3e:e9:15:81:2c 192.168.30.1 60  ARP  0c:99:90:05:c5:00  0c:3e:e9:15:81:2c  74.442675 218
                                M-SEARCH * HTTP/1.1 175  SSDP  239.255.255.250  192.168.197.1  87.277042 219
                                M-SEARCH * HTTP/1.1 175  SSDP  239.255.255.250  192.168.197.1  87.277048 220
                                M-SEARCH * HTTP/1.1 175  SSDP  239.255.255.250  192.168.197.1  90.278318 221
                                M-SEARCH * HTTP/1.1 175  SSDP  239.255.255.250  192.168.197.1  90.278326 222
                                M-SEARCH * HTTP/1.1 175  SSDP  239.255.255.250  192.168.197.1  93.278865 223
                                M-SEARCH * HTTP/1.1 175  SSDP  239.255.255.250  192.168.197.1  93.278871 224
                                M-SEARCH * HTTP/1.1 175  SSDP  239.255.255.250  192.168.197.1  96.291709 225
                                M-SEARCH * HTTP/1.1 175  SSDP  239.255.255.250  192.168.197.1  96.291715 226
                                M-SEARCH * HTTP/1.1 175  SSDP  239.255.255.250  192.168.197.1  99.292416 227

                  Frame 207: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

0000  0c 99 90 05 c5 00 0c 3e  e9 15 81 2c 08 00 45 00   .......>...,..E.
0010  00 3c 00 66 00 00 ff 01  fd a5 c0 a8 1e 01 c0 a8   .<.f............
0020  1e 63 00 00 55 4b 00 01  00 10 61 62 63 64 65 66   .c..UK....abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi

Profile: Default   Packets: 236 · Displayed: 236 (100.0%)        <VMware Network Adapter VMnet3>: <live capture in progress>
```

Fig.13.: Ping Command Result

Fig (14) shows the result on wireshark when remotely accessing with TELNET(Telecommunications Network) which gives the source & destination IP, time of trying accessing with TELNET, illustrate TCP(Transmission Control Protocol) & TELNET protocol, and some of packet information as example request & response.



```
                                                                   Info Length  Protocol  Destination     Source          Time
1032 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 [TCP Retransmission] 66  TCP  192.168.31.1   192.168.31.99  18.967132 34
1032 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 [TCP Retransmission] 66  TCP  192.168.31.1   192.168.31.99  18.967145 35
                 Seq=0 Ack=1 Win=4128 Len=0 MSS=1260 [SYN, ACK] 1032 → 23 60  TCP  192.168.31.99  192.168.31.1   18.978715 36
                                Seq=1 Ack=1 Win=65520 Len=0 [ACK] 23 → 1032 60  TCP  192.168.31.1   192.168.31.99  18.983620 37
     23 → 1032 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1260 [TCP Out-Of-Order] 60  TCP  192.168.31.99  192.168.31.1   18.985885 38
     23 → 1032 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1260 [TCP Out-Of-Order] 60  TCP  192.168.31.99  192.168.31.1   18.985906 39
              1032 → 23 [ACK] Seq=1 Ack=1 Win=65520 Len=0 [TCP Dup ACK 37#1] 60  TCP  192.168.31.1   192.168.31.99  18.987118 40
              1032 → 23 [ACK] Seq=1 Ack=1 Win=65520 Len=0 [TCP Dup ACK 37#2] 60  TCP  192.168.31.1   192.168.31.99  18.987126 41
                                                         ... Telnet Data 66  TELNET  192.168.31.99  192.168.31.1   19.003900 42
         23 → 1032 [PSH, ACK] Seq=1 Ack=1 Win=4128 Len=12 [TCP Retransmission] 66  TCP  192.168.31.99  192.168.31.1   19.008924 43
         23 → 1032 [PSH, ACK] Seq=1 Ack=1 Win=4128 Len=12 [TCP Retransmission] 66  TCP  192.168.31.99  192.168.31.1   19.008937 44
                                                         ... Telnet Data 75  TELNET  192.168.31.1   192.168.31.99  19.014559 45
                                                         ... Telnet Data 63  TELNET  192.168.31.1   192.168.31.99  19.018290 46
          1032 → 23 [PSH, ACK] Seq=1 Ack=1 Win=65520 Len=21 [TCP Out-Of-Order] 75  TCP  192.168.31.1   192.168.31.99  19.018725 47
          1032 → 23 [PSH, ACK] Seq=1 Ack=1 Win=65520 Len=21 [TCP Out-Of-Order] 75  TCP  192.168.31.1   192.168.31.99  19.018737 48
      1032 → 23 [PSH, ACK] Seq=22 Ack=13 Win=65508 Len=9 [TCP Retransmission] 63  TCP  192.168.31.1   192.168.31.99  19.020930 49
      1032 → 23 [PSH, ACK] Seq=22 Ack=13 Win=65508 Len=9 [TCP Retransmission] 63  TCP  192.168.31.1   192.168.31.99  19.020946 50
                                                        ... Telnet Data 614  TELNET  192.168.31.99  192.168.31.1   19.034186 51
         23 → 1032 [ACK] Seq=13 Ack=1 Win=4128 Len=560 [TCP Retransmission] 614  TCP  192.168.31.99  192.168.31.1   19.038231 52
         23 → 1032 [ACK] Seq=13 Ack=1 Win=4128 Len=560 [TCP Retransmission] 614  TCP  192.168.31.99  192.168.31.1   19.038249 53
                                                        ... Telnet Data 144  TELNET  192.168.31.99  192.168.31.1   19.039681 54
                             Seq=31 Ack=663 Win=64858 Len=0 [ACK] 23 → 1032 60  TCP  192.168.31.1   192.168.31.99  19.045527 55

                    Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
                                                                                IEEE 802.3 Ethernet
                                                                               Logical-Link Control
                                                                             Spanning Tree Protocol

0000  01 80 c2 00 00 00 0c 3e  e9 ba 19 00 00 27 42 42   ......>.....'BB
```

Fig.14.: Shows the Result of accessing telnet remotely

6. Acknowledgment

The port mirror features described in this paper are an excellent starting point for strengthening switch port mirror networks and should be used in the context of an enterprise's larger security policy. Data security, data collection, and monitoring are all made possible by monitoring. Monitoring results in more stable and dependable computer systems even while it does not fix problems. Without the need of any extra parts, Port Mirroring technology can be monitored over a normal network switch. It is economical, easy to use, and doesn't interrupt with normal network operations . By Appling the VPN technology, online activity is hidden. VPNs are used to protect against hackers and snoopers on public networks, but they are also helpful for hiding the IP address, browsing activity, and personal information on any Wi-Fi (Wireless Fidelity) network. Also, network monitoring tools have been used and this monitoring helps point out the exact location of the network problem. Continuous monitoring can help identify potential issues before they occur which means that problems are solved proactively before they get to the users. When Port Mirroring technology was applied, the problems was identified faster and time and efforts were saved in searching for the root of the detected problems. And by using a Virtual private network, data was protected when it was transmitted over the Internet.

7. References

[1]- https://www.cse.wustl.edu/~jain/cse56706/ftp/net_monitoring/ndex.html [Accessed 20 December 2022 / 6:39 pm].

[2]- https://blog.niagaranetworks.com/blog/port-mirroring-for network-monitoring-explained [Accessed 20 December2022 / 7:02 pm].

[3]- https://ieeexplore.ieee.org/document/5137879 [Accessed 21December 2022 / 8:12 pm].

[4]- https://geek-university.com/ccna/what-is-a-network-switch> [Accessed 29 December 2022 / 5:54pm].

[5]- http://www.difference between.net/ technology/difference-between-layer-2-switch-and-layer-switc/#ixzz6v9qams16> [Accessed 16 March 2020 / 7:55 pm].

[6]- https://www.fiberopticshare.com/what-is-the-purpose-of-a-switch-in-networking.html> [Accessed 5 June 2021 / 4:22pm]

[7]- [7]https://www.networxsecurity.org/membersarea/glossary/n/network-switches.html> [Accessed 10 November 2021 / 8:22 pm]

[8]- https://www.slideshare.net/irisdan/network-switches-functions-role-in-networks> [Accessed 3 November 2021 / 6:46 pm].

[9]- https://ipwithease.com/what-are-key-functions-of-a-network-switch> [Accessed 3 November 2020 / 6:02 pm].

[10]- http://www.leptonsys.com /blog/layer-1-switches-key-functions-and-technologies> [Accessed 3 November 2022 / 6:10 pm].

[11]- https://www.techopedia.com/definition/8011/layer-2-switch>[Accessed 3 November 2020 / 6:24 pm].

[12]- https://networkencyclopedia.com/layer-3-switch> [Accessed 4 November 2022 / 4:30 pm].

[13]- http://www.leptonsys.com/blog/layer-1-switches-key-functions-and-technologies> [Accessed 3 November 2022 / 5:01 pm].

[14]- https://www.networkworld.com /article/ 2268110/ chapter-1--understanding-network-security-principles.html> [Accessed 20 November 2022 / 3:11 pm].

[15]- https://www.tutorialspoint.com/network_security/network_security_critical_necessity.htm> [Accessed 21 March 2022 / 3:20pm].

[16]- https://www.sangfor.com/en/info-center/blog-center/cyber-security/the-basics-of-authentication-in-cyber-security>[Accessed 18 March 2021 / 9:26 pm].

[17]- https://www. knowitallninja.com/lessons/how-internal-threats-occur/> [Accessed 26 March 2021 / 9:37 pm].

[18]- https://www.jigsawacademy.com/blogs/cyber security/different-types-of-hackers/> [Accessed 27 November 2022 / 8:20 pm].

[19]- https://www.fortinet.com/solutions/enterprise-midsize-business/network-security> [Accessed 2 December 2022 / 6:15 pm].

[20]- https://www.tutorialspoint.com/network_security/network_security_firewalls.htm> [Accessed 16 February 2021 / 7:55 pm].

[21]- https://www.comms-express.com/products/cisco-asa5525/?product=cisco-asa5525/> [Accessed 10 December 2022 / 8:20 pm].

[22]- https://www.cisco.com/c/en/us/products/security/vpn endpoint-security-clients/what-is-vpn.html>[Accessed15December 2022 / 10:20 pm].

[23]- https://www.unitedtelecom.gr/index.php/en/services/network-monitoring-solution.html> [Accessed 12 February 2021 / 5:12 pm].

[24]- https://www.techopedia.com/definition/16134/port-mirroring> [Accessed 17 July 2021 / 4:33 pm].

[25]- https://www.miarec.com/faq/what-is-port-mirroring> Accessed 17 July 2021 / 4:48 pm].

[26]- [26]https://www.a10networks.com/blog/traffic-monitoring/> [Accessed 21 July 2021 / 9:12 pm].

[27]- Balchunas, A―Switched Port Analyzer (SPAN)‖.7(4), 2014, p.4.

[28]- Berg, J, Interactive workstations: Hardware component.Computer Standards & Interfaces, 2019, p.6.

[29]- https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html>. ―Catalyst SwitchedPort Analyzer (SPAN) Configuration Example‖. [11 August 2021 9:54 am]

[30]- https://community.fs.com/blog/port-mirroring-explained-basis-configuration-and-fa-qs.html> [Accessed 21 October2021 / 5:30 pm].

[31]- Moore, A , Traffic Trace Artifacts due to Monitoring Via Port Mirroring. University of Cambridge, 2007, p.9.

[32]- https://www.comparitech.com/net-admin/ultimate-guide-to-port-mirroring/> [Accessed 24 October 2021 / 3:42 pm].