

ANALYSYS AND IMPLEMENTATION IEEE 802.1Q TO IMPROVE NETWORK SECURITY

Muhammad Syaeful Bahry
Master of Informatics
Sunan Kalijaga State Islamic University
Yogyakarta, Indonesia
saifulbahary37@gmail.com

Bambang Sugiantoro
Lecturer of Informatics Engineering
Sunan Kalijaga State Islamic University
Yogyakarta, Indonesia
bambang.sugiantoro@uin-suka.ac.id

Abstract- *The development of technology today is very fast one only with the existence of the use of the computer network. This can be seen in the increasing number of organizations or companies that use the computer network to facilitate the flow of information within the organization or the company. But with the abundance of the use of network technology is only advancing network progressed only, but not maximize resource so that sometimes allows for the problem or traffic network. For that can be needed by network development solution made VLAN topology using NDLC method (Network Development Life Cycle). Vlans are able to improve the capabilities of the network and can reduce the amount of data that is sent to a destination that does not need to be so that the traffic in the network will be reduced by itself. In addition there is another reason why requires a VLAN is to reduce the possibility of the misuse of access rights. It can use the Mode Access. With the Mode will divide each Host into the VLAN each. With the existence of a VLAN shows can increase network ability as much as 13.4 %. With the data shows that a VLAN successful and able to make the network more efficient. In the VLAN network security aspect is able to optimize network security with the existence of access mode, so that the new host are not capable of entering it into the existing network topology.*

Keywords : LAN (Local Area Network), NDLC (Network Development Life Cycle), VLAN (Virtual Local Area Network), Mode Access, Network.

I. INTRODUCTION

A. Research Backgorund

The current technological development is very rapid one with the use of computer networks. It can be seen growing number of organizations or companies that use computer networks to facilitate the flow of information within your organization or company. The incidence of the development of network technology itself cannot escape the need for the use of shared resources that exist in the network be it hardware or software.

In building a computer network engineering capabilities required in the areas of the network, but in fact there are not many people who have the ability compared to users of the internet itself, for it is still needed people who can build a network to be utilized in order to be better again. (Yani, 2007:2). At the moment every instance of course there is already a network information system for encouraging the activities and performance of the Office. One of them is SMK Muhammadiyah 3 Yogyakarta, which is a special vocational schools in the field of engineering. For network system at SMK Muhammadiyah 3 Yogyakarta there are many computers connected to the LAN (Local Area Network).

There are several majors in SMK Muhammadiyah 3 Yogyakarta, namely Computer Network Engineering, automotive, Light Vehicles, electrical installation, Building Images, Audio Video. As for the problems that often happen in the system network SMK Muhammadiyah 3 Yogyakarta, such as network congestion in data transmission in LAN environment, for example by having the amount of data that is sent simultaneously to the same purpose eg. PC Server. With the onset of the case will allow the occurrence of problems or network traffic can mean data sent to the server are not all sent, even fails to make delivery and if successful would certainly require quite a long time so that the data up to the delivery destination.

For that it needs the network development solution of establishing VLAN topology. VLAN capable of enhancing the capabilities of the network and can reduce the amount of data that is sent to a destination that does not need to be so that the traffic on the network itself will be reduced. In addition there are other reasons why need a VLAN that is to reduce the possibility of abuse of the right of access. Network access to the ISP also became an important factor. Internet access becomes slow due to LAN environments it often happens that a traffic jam the network. On that basis SMK Muhammadiyah 3 Yogyakarta wants to develop a standard LAN system into the concept of Virtual LAN. VLAN concepts is intended also to avoid damages that occur on the hard disk which is certainly expensive price. Concept created using Packet

Tracer 6.2 Student this will show the result that is a virtual network that is connected and can be implemented into the real network development.

B. Formulation of Research

The problems will be discussed on this research are as follows:

- How is the performance of the network VLAN are able to make more efficient the LAN network.
- How are grouped into several groups to separate between one field with another field in the network VLAN.
- How the system network VLAN can limit user access and reduce abuse of the data on the network by digitally dibuatkannya some of the VLAN group.

C. Research Purpose

The purposes of this research are:

- a. Test the level of efficient network at SMK Muhammadiyah 3 Yogyakarta.
- b. Using VLAN network topology to reduce the Troubleshooting.
- c. Divide the access based on each group's section to improve the security of computer networks.

II. STUDY LITERATUR

A. Computer Network

Computer network is a group of interconnected autonomous computer between each other using communication protocols through a communication medium so that it can share information, use of programs along with hardware such as a printer, hard disk, and so on. In addition the network computer bias is defined as a collection of a number of communication terminals that are located in various locations consisting of more one interconnected computers.

B. Network Topology

Network topology is the rule that describes how computers, printers, and other devices connected over a network. In addition to tu topology can be interpreted as a pattern of relations between terminal in a computer network system that would affect the level of effectiveness of the performance of computer networks (MADCOMS, 2013:24). Seen from the topology, a network can also be divided into two types, namely Physical Topology and a Logical Topology.

C. IP Address

IP Address is the identifier that is used to give an address on each computer in the network. The format of the IP Address is a 32 bit number that each 8 bit, separated by a comma. As for the format of the IP Address can be either a binary form (xxxxxxxx xxxxxxxx xxxxxxxx... xxxxxxxx x is a binary number 0 or 1). Or with four decimal numbers form, each separated by a period. This

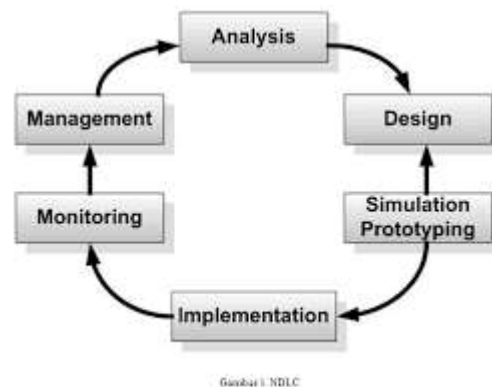
form is known as dotted decimal (xxx.xxx.xxx.xxx where x is a value from 1 octet originating from 8 bits).

D. Subnetting

Subnetting is the process of dividing or split a network into multiple smaller network or a subnet called often. With subnetting, we can determine the number of hosts that will be used on the network. If we only have 5 hosts, but we aren't we set subnetmask corresponds to the number of hosts, then packages the data that goes into the network will be dibroadcast to the rest of IP addresses (host), even though the host was in fact never existed. Therefore, we need to use subnetting to mengefisiensikan the use of different bandwidth network.

III. RESEARCH METHODOLOGY

The methods used in doing this is to use a system development method NDLC (Network Development Life Cycle), using structured analysis approach. The use of the tool of the NDLC method will be used, in order to be able to simplify network administrators see an overview of the process of the system of network performance. (Ladjmudin,213:2005).



Figur 1. NDLC Method Flow (Network Development Lifecycle)

A. Analysis

This stage is the stage of the analysis of the needs, problems, requests the user and network topology. Methods that can be used for the analysis phase include: Needs Analysis, Analysis Problem, User Analysis, Topology Analysis.

B. Design

At this stage, the data has been retrieved will be the basis in making the network topology design will be built. The design can be a topological structure design, design layout of cable. Here illustrates how the design or an existing network topology at the moment in SMK Muhammadiyah 3 Yogyakarta. The topolgi structure describes the design of an existing network or networks that are used today.

C. Simulation Prototyping

The next step is to conduct a simulation based on the prototype and create a design that has been designed. Tools that can be used to perform a simulation network is Packet Tracer, GNS3. With the existing topology, can do on the network VLAN prototype SMK Muhammadiyah 3 Yogyakarta. Prototype does is illustrate the simulation application of VLAN in the network. For it using Packet Tracer Version 6.2 for the Student to perform the VLAN in the network prototype SMK Muhammadiyah 3 Yogyakarta.

D. Implementation

This stage is the stage that takes longer than the previous stage. The purpose of this stage is to find out the success of the design of the networks that have been built. At this stage of implementing results from an existing prototype.

The implementation is done in jaringan SMK Muhammadiyah 3 Yogyakarta who accompanied directly by the parties there. One of these implementations do test connectivity between the network of the same or different networks.

E. Monitoring

After implementation, this step is an important stage in designing the network. The goal is to make sure the computer network run according to the purpose at this stage of the analysis. In this stage also carried out monitoring of the results of the application of the VLAN that is already done. Monitoring that is done is to compare the network that previously have not implemented the concept of a VLAN with a network that already apply the VLAN.

F. Management

Management is the last stage in the NDLC method. At this stage, policy making is an important thing to get special attention. Policies drawn up depending upon the policy of dimiliki by management level. At this stage it is the policy of the school concerned.

IV. RESULT AND DISCUSSION

A. VLAN Connectivity Test

Test the Connectivity here aimed to check whether the network VLAN simulation that was made is in compliance or not yet appropriate. The first test is carried out on the same VLAN network. For example, will test the connectivity to the network VLAN 21 which is the VLAN 1 TKJ. In VLAN 1 there are 2 TKJ end user and both on the same network. PC 1 has the Ip Address 192.168.21.2 as for PC 2 has the IP Address 192.168.21.3. Testing is done using metode PING. A PING is performed on one PC and directed to PC the other PC or other (missal there are 3

PC on the network the same VLAN). Following are the results of the PING made on network 21 TKJ VLAN 1:

```
PC>ping 192.168.21.3

Pinging 192.168.21.3 with 32 bytes of data:

Reply from 192.168.21.3: bytes=32 time=165ms TTL=128
Reply from 192.168.21.3: bytes=32 time=140ms TTL=128
Reply from 192.168.21.3: bytes=32 time=0ms TTL=128
Reply from 192.168.21.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.21.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 165ms, Average = 76ms
```

Figur 2. VLAN Connectivity Test

B. Trunk Configuration On The Switch

Trunk is the Protocol that serve to filter VLANS which can go against the desired interface, e.g. Interface fastEthernet 0/1 is port will do a fashion trunk. The trunk on this interface are configured directly to the router. The VLAN dizinkan into trunk mode it will be filtered through a routing process will make communication between VLANS.

Granting the term trunk between switches to configure to swich the other is very necessary. In one term trunk Switch is not required for configuration, but in a different switch trunking is very important to be able to connect the inter-VLAN. To be able to understand the trunking, see picture below. The following configuration is done on Trunk Interface fastEthernet 0/1 switch on ICT.

```
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
*LINEPROTO-0-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*LINEPROTO-0-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#no sh
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#
```

Figur 3. Trunk Configuration on Switch

A. Router Configuration

For example, to configure the router on ICT. A router is a device that a VLAN between liaison with other VLAN to be connected. Router here could serve as a sub-interface Default Gateway address on each VLAN that is present in every Switch.

```

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#int fa0/0.21
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.21, changed state to up

Router(config-subif)#encapsulation dot1Q 21
Router(config-subif)#ip address 192.168.21.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int fa0/0.22
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.22, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.22, changed state to up
    
```

```

Router(config-subif)#encapsulation dot1Q 22
Router(config-subif)#ip address 192.168.22.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int fa0/0.23
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.23, changed state to up

Router(config-subif)#ip address 192.168.23.1 255.255.255.0

% Configuring IP routing on a LAN subinterface is only allowed if that subinterface is already configured as part of an IEEE 802.1Q, IEEE 802.1Q, or IEEE VLAN.

Router(config-subif)#encapsulation dot1Q 23
Router(config-subif)#ip address 192.168.23.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int fa0/0.24
Router(config-subif)#int fa0/0.24
%LINK-5-CHANGED: Interface FastEthernet0/0.24, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.24, changed state to up
Router(config-subif)#int fa0/0
Router(config-subif)#encapsulation dot1Q 24
Router(config-subif)#ip address 192.168.24.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int fa0/0
Router(config-subif)#
    
```

Figure 4. Router Configuration

B. Test Efficiency Of The Network VLAN.

VLAN can maximize the performance of your existing network so that the network can work with efficiently. The following is a comparison of before and after implementation of the VLAN in the network.

```

PC>ping 192.168.21.3

Pinging 192.168.21.3 with 32 bytes of data:

Reply from 192.168.21.3: bytes=32 time=165ms TTL=128
Reply from 192.168.21.3: bytes=32 time=140ms TTL=128
Reply from 192.168.21.3: bytes=32 time=0ms TTL=128
Reply from 192.168.21.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.21.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 165ms, Average = 76ms
    
```

```

PC>ping 192.168.21.3

Pinging 192.168.21.3 with 32 bytes of data:

Reply from 192.168.21.3: bytes=32 time=0ms TTL=128
Reply from 192.168.21.3: bytes=32 time=0ms TTL=128
Reply from 192.168.21.3: bytes=32 time=0ms TTL=128
Reply from 192.168.21.3: bytes=32 time=123ms TTL=128

Ping statistics for 192.168.21.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 123ms, Average = 30ms
    
```

Figure 5. Efficiency VLAN

First PING takes an average 76ms to perform the delivery of the package. And, after the second PING produces on average 30ms. This indicates that the presence of VLAN implementation then will produce a more efficient network.

C. Test Network Security

Test the security of the network already uses the concept of a VLAN, try adding a foreign host that does not have the same configuration and not on a foreign host port configuration is not done switchport. Testing conducted addition of foreign hosts on the network VLAN. The foreign host has IP Address 192.168.22.4 that is configured in static. Foreign host is connected into the Switch TKJ 1 which is the VLAN 21.

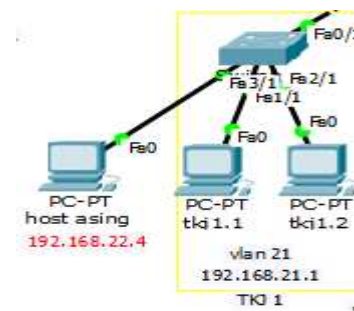


Figure 6. The Addition Of The Foreign Host

To perform a test of security, then the foreign host will try to PING into the network VLAN 21. Following are the results of the PING host foreign headed the network VLAN 21.

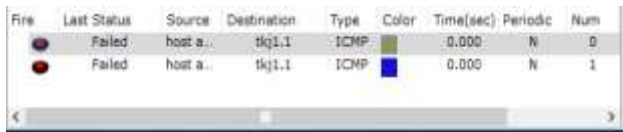
```

PC>ping 192.168.21.2

Pinging 192.168.21.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.21.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    
```



| File | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num |
|------|-------------|-----------|-------------|------|-------|-----------|----------|-----|
| | Failed | host a... | tkj1.1 | ICMP | Green | 0.000 | N | 0 |
| | Failed | host a... | tkj1.1 | ICMP | Blue | 0.000 | N | 1 |

Figure 6. Test Network Security

Although the foreign host IP settings in Addressnya according to one of the network VLAN (VLAN 22) but the foreign host can not connect into the insfratruktur network directly. This is because the port on the Switch that is connected 1 TKJ on foreign host access configurations do not VLANnya. So if you want to enter insfratruktur the network then it needs verification and permission from the network administrator to enter into insfratrukturjaringan. The existence of such results can be concluded that the concept of a VLAN can help or improve the security of the network on the network SMK Muhammadiyah 3 Yogyakarta.

V. CONCLUSION AND SUGGESTION

A. Conclusion

From the previous discussion then the conclusion to be drawn as follows: with the VLANS can make computer networks SMK Muhammadiyah 3 Yogyakarta more efficiently. VLANS improve network Performance by as much as 13.4%. The data show that the VLAN is successful and able to make the network more efficient. Grouping network using VLANS can be used to distinguish networks based on its functionality and make it easy to do the monitoring network. Grouping the Network Access Mode based on differentiated for each VLAN. The existence of such a grouping of network administrators can distinguish the VLAN each section and make it easier for monitoring in the VLAN network topology. To restrict access on a network of existing VLAN can be set with the configuration of VLANS which can communicate and VLANS which can not be communicated. In terms of network security VLAN are able to optimize network security with the access mode, so the new host is not able to enter it into your existing network topology.

B. Suggestion

Network VLANS that have been made there are still many things that need to be fixed. For example on the access rights of each VLAN. This could be developed further research on the back. And also to get good network certainly there must be the correct topology and devices are adequate and better organised. The existence of such a network would be more orderly.

REFERENCES

[1] Alabady, Salah. (2009). Design and Implementasi of a Network Security Model for Cooperative Network. Iraq: Computer Engineering Department, University of Mosul.

- [2] Arifin, Zaenal. (2003). Langkah Mudah Mengkonfigurasi Router Cisco. Yogyakarta : Andi
- [3] Efendi, Rissal., Widiastari, Indrastanti Ratna. (2012). Pengujian Kinerja Jaringan pada Virtual Local Area Network (VLAN) menggunakan Virtual Trunking Protocol (VTP). Salatiga: Universitas Kristen Satya Wacana(UKSW).
- [4] Efendi, Rissal., Widiastari, Indrastanti Ratna. (2012). Segmentasi Broadcast Domain Dalam Virtual Local Area Network (VLAN) Dengan Memanfaatkan Virtual Trunking Protocol (VTP) Pruning Untuk Menghemat Bandwidth. Salatiga: Universitas Kristen Satya Wacana(UKSW).
- [5] Kadir, Abdul., Triwahyuni, Terra. (2003). Pengenalan Teknologi Informasi. Yogyakarta: Andi
- [6] Komputer, Wahana. (2003). Konsep Jaringan Komputer dan Pengembangannya. Jakarta: Salemba Infotek.
- [7] Odum, Wendell. (2005). Computer Networking First-Step. Yogyakarta: Andi
- [8] Pal, Gyan Prakash., Pal, Sadhana. (2013). Virtual Local Area Network(VLAN). Faculty of Electronics & Communication Engineering Department.
- [9] Puspito, Faesol., Widyastutui, Hj. Naniek., Triyono, Joko. (2014). Perancangan Blue Print Jaringan Menggunakan Virtual LAN (VLAN) Dengan Studi Kasus (PT. PLN Persero Area Kudus). Yogyakarta: Institut Sains & Teknologi AKPRIND.
- [10] Shaffi, Abubucker Samsudeen. (2012). Effective Implementation Of VLAN And Acl In Local Area Network. Sultanate of Oman: Faculty of Computing Studies, Gulf College Muscat.
- [11] Supandi, Dede. (2008). Instalasi Dan Konfigurasi Jaringan Komputer. Bandung : Informatika Bandung
- [12] Sutanto, Felix Andreas., Yulianton, Heribertus., Razaq, Jeffri Alfa. (2011). Rancang Bangun VLAN untuk Segmentasi Jaringan pada Cyber Campus Laboratory Universitas Stikubank. Fakultas Teknologi Informasi: Universitas Stikubank.
- [13] Syafrizal, Melwin. (2005). Pengantar jaringan komputer. Yogyakarta: Andi Offset.
- [14] Yani, Ahmad. (2005). Jaringan Komputer. Jakarta: PT.Kawan Pustaka.