Exploration and Practice of Complex Teaching Cases Based on Campus Network

Qian Wang[a], Shan Jing[b,*], Yue Gao[c] and Lei Guo[d]

School of Information Science and Engineering, University of Jinan, Jinan, Shandong, China

[a]ise_wangqian@ujn.edu.cn, [b]jingshan@ujn.edu.cn, [c]13066009630@163.com,

[d]20171222003@mail.ujn.edu.cn

*Corresponding author

Keywords: Campus Network; Teaching Case; Network Troubleshooting; Application-Oriented Talents; Practice Teaching

Abstract: Based on the university campus network, through analyzing the current situation of network engineering teaching case, further study of the network troubleshooting methods, network fault classification technology, and through the effective integration of campus network breakdown case, form a practical and effective teaching case and its practice in the teaching of the application-oriented talents training daily, in order to improve the teaching effect. g cases, further improve the teaching level and quality, has good application value. Case teaching in combination with the teaching content positioning students need to master the ability to target, converting the real case to integrating authenticity, practicality, innovation of teaching case, further improve the teaching level and quality, and has good application value.

1. Introduction

With the rapid development of computer network technology in China, the dominant position of educational informationization has become more prominent. As an important part of information construction, campus network's daily management and good operation directly affects the development of university information construction [1].

Chinese colleges and universities have basically established complex and perfect campus networks, which serve as an important tool and carrier to provide resource sharing, information exchange and collaborative work for teaching, scientific research and administration. In the daily operation and management of campus network, a large number of complex and comprehensive network failures occur frequently. Therefore, it becomes more and more significant to quickly troubleshoot the causes of failures and solve the problems [2-3]. In the daily operation and maintenance of campus network, there are a large number of real fault cases, how to effectively transform these actual fault cases into teaching cases on the course, so that students can master network knowledge and related network technology through the study of real cases is a very meaningful work. It can not only enrich the course experimental teaching content, improve the teaching effect, but also further meet the network engineering specialty's goal and requirements for application-oriented talents training [4-5].

This paper introduces the common network troubleshooting tools and fault troubleshooting methods for network management. The key technologies of network networking are studied, and various faults of key protocol technologies are analyzed in depth. At the same time, real cases were effectively classified and integrated with the knowledge and difficulty level of the course, and Packet Tracer was used for the verification test of design cases. Finally, the teaching cases are applied to the daily experiments of professional courses, so that students can truly feel the occurrence of network fault cases, and their ability to analyze, investigate and solve problems can be improved. In addition to better teaching effects, the overall quality and level of undergraduate application-oriented talent training can be improved.

2. Troubleshooting and Tool Introduction

2.1. Network Troubleshooting Methods

Campus network application of a variety of networking technology, large scale and many users, there are a variety of network failures. To maintain a campus network, you first need to understand the causes of network failures and network configuration knowledge.

The common network faults of campus network can be divided into physical faults and logical faults. Physical fault refers to the physical problems of equipment or line, including line fault, port fault, network equipment fault, host physical fault, etc. When this kind of failure occurs, the network will be interrupted directly or occasionally. The logical failure refers to the network equipment configuration error or the host network information configuration error, such as the network equipment configuration, network protocol fault, security fault, etc [6].

In order to quickly and accurately repair the campus network fault, we must first find the fault cause that is, troubleshooting. The network fault troubleshooting process is shown in Figure 1.

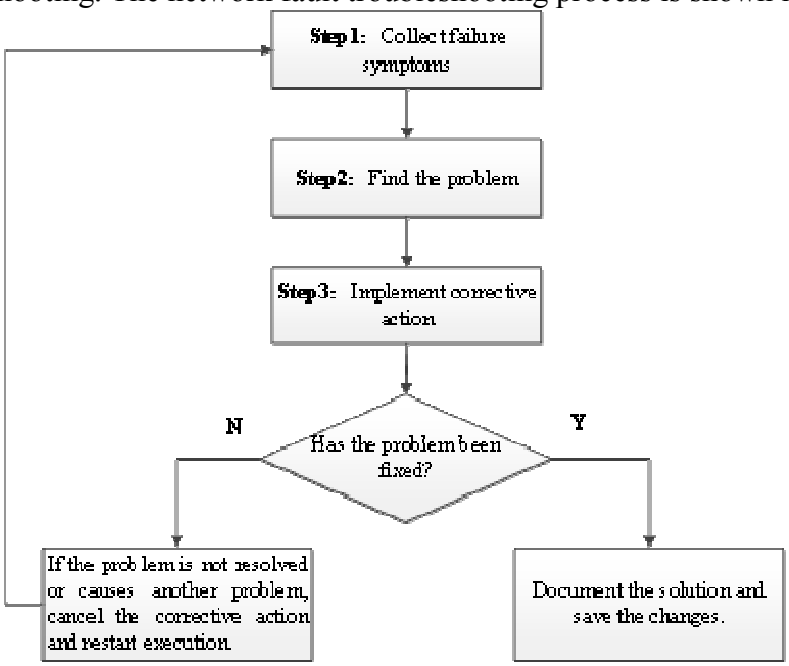

Figure 1. Network fault troubleshooting process

In the process of specific troubleshooting, various testing tools can be used to monitor the operation state of the network, troubleshoot the network fault, improve the efficiency of troubleshooting, efficient, fast location and solve the fault. Software testing tools include operating system built-in diagnostic instructions and protocol analysis software. Common network diagnostic commands include ping, ipconfig, NSLookup, tracert, and so on. Protocol analysis software analyzes network traffic in real time by means of data packet capture, decoding and transmission. The most commonly used network analyzers are Sniffer and Wireshark. Hardware tools can be used to locate physical link problems and analyze protocol working status. Common hardware tools include multimeter, cable tester, protocol analyzer and network multimeter.

2.2. Tool Introduction

2.2.1. Introduction of Packet Tracer

Packet Tracer is an auxiliary learning tool released by Cisco to provide network simulation environment for network design, configuration and troubleshooting for beginners in Cisco networking courses. Packet Tracer supports the creation of network topologies by dragging directly from the user interface of the software and provides detailed processing of packets as they travel through the network. Observe the real-time operation of the network, learn the configuration of IOS

and exercise the troubleshooting ability, so as to make practical teaching easier and improve students' learning efficiency.

2.2.2. Introduction of Activity Wizard

Activity Wizard is essentially an automatic evaluation tool, which can be used to efficiently and simply create a specific network simulation environment, set instructions for it, configure the basic network environment through the initial network configuration, and set standard answers through the question-and-answer network, so as to achieve automatic evaluation. Therefore, it not only facilitates students' self-test and self-assessment in their usual practice and practical assessment, but also greatly reduces teachers' workload in assessment.

3. Introduction of Networking Technology

3.1. VLAN

VLAN (Virtual Local Area Network) solves the problems such as using switch to do LAN interconnection and unable to limit broadcasting, how to prevent the leakage of commercial secrets in communication, and how to manage the connection of network units flexibly [7]. The advantages include: (1) to prevent the occurrence of broadcast storms; in different vlans, broadcast and unicast traffic will not be forwarded, so as to reduce the waste of network resources (limited bandwidth traffic); (2) Effectively ensure network patency to prevent network traffic conflicts; (3) To reduce the input cost of equipment; (4) To reduce the trouble caused by rewiring and make network operation and maintenance more safe, convenient and effective.

3.2. Inter-VLAN Routing

Because the VLANs in the switch are isolated from each other, the data between VLANs need to be transmitted by means of the router, that is, the inter-VLAN routing. It is the process of using routing devices to forward traffic from one VLAN to another.

3.3. Routing Technology

Routing is the process that determines the network scope of the end-to-end path by grouping from source to destination. Routing works at the third layer of the OSI reference model, the packet forwarding device at the network layer. Routers interconnect networks by forwarding packets. Although routers can support a variety of protocols (such as TCP/IP, IPX/SPX, AppleTalk, etc.), the vast majority of routers in China run TCP/IP [8].

(I) Static routing

Static routing: A method of routing in which entries are manually configured rather than dynamically determined. Unlike dynamic routing, static routing is fixed and does not change, even if the network condition has changed or been re-configured. In general, static routing is added to the routing table item by item by network administrator.

The advantage of static routing is high network security confidentiality. Dynamic routing requires frequent exchange of routing tables between routers, and analysis of routing tables can reveal information such as network topology and network address. Therefore, the network can also adopt static routing for security reasons. It does not take up network bandwidth because static routing does not generate update traffic.

(II) RIP protocol

RIP(Routing Information Protocol) is an internal gateway protocol (IGP) and a dynamic routing protocol for the transmission of routing information within autonomous systems (AS) [9] . The RIP protocol is based on Distance Vector Algorithms and uses "hops" (also known as metric) to measure the routing distance to destination addresses. RIP is applied to the application layer of the OSI network seven-layer model. Each manufacturer will define the management distance (AD), Huawei defines the priority as 100, and Cisco defines the priority as 120.

(III) OSPF protocol

OSPF routing protocol is a typical Link-state routing protocol, generally used in the same routing domain [10]. OSPF includes single-area OSPF and multi-area OSFP. This paper mainly discusses the single area OSPF protocol. All routers in single-area OSPF are located in the backbone area (area 0), which is useful in small networks with fewer routers. Multi-region OSPF implementation using a two-layer region level's all regions must be connected to the trunk region (region 0), which is useful in large network deployment, can reduce processing and memory overhead, and has the advantages of smaller routing tables, link status update overhead, OSPF computing frequency reduction.

3.4. ACL

ACL (Access Control List) is a protocol configured on network devices for traffic Access Control, which plays the role of supervisor when different traffic is forwarded. Network level security policy enforcement mostly involves traffic categorization using access control lists, and gateway devices that perform lane traffic filtering can deploy ACLs of thousands of rules. A series of access control rules are developed to filter the data traffic related to each protocol, destination IP, source IP and port number, so as to restrict the forwarding of complex traffic in network environment. ACL optimization can greatly improve the performance of packet forwarding devices.

The common network faults of campus network can be divided into physical faults and logical faults. Physical fault refers to the physical problems of equipment or line, including line fault, port fault, network equipment fault, host physical fault, etc. When this kind of failure occurs, the network will be interrupted directly or occasionally. The logical failure refers to the network equipment configuration error or the host network information configuration error, such as the network equipment configuration, network protocol fault, security fault, etc.

3.5. NAT

NAT (Network Address Translation) was proposed in 1994. Use NAT when you want to communicate with a host on the Internet that is already assigned a local IP address (that is, a private address that is used only within the private network) but doesn't require encryption.

NAT helps mitigate the depletion of available IP address space by using a small number of public IP addresses to represent a large number of private IP addresses. In addition, NAT can effectively prevent attacks from outside the network, hide and protect the computer inside the network.

3.6. Port Aggregation

Port aggregation, also known as EtherChannel, was developed by Cisco for multi-link bundling between switches. Its basic principle is: bind multiple physical links between two devices together to form a logical link, so as to achieve the purpose of doubling the bandwidth (this logical link bandwidth is equivalent to the sum of the physical link bandwidth) [11]. In addition to increasing bandwidth, port aggregation can also evenly distribute traffic on multiple links and play the role of load sharing. When one or more links fail, as long as there are normal links, the traffic will be transferred to other links. The whole process is completed within a few milliseconds, thus playing a redundant role and enhancing the stability and security of the network. EtherChannel formation between two switches can also be automatically negotiated by protocol.

There are currently two negotiating protocols: PAgP and LACP. PAgP(Port Aggregation Protocol) is a private Cisco Protocol, while LACP(Link Aggregation Control Protocol) is based on the international standard of IEEE 802.3 AD, and it is a protocol to realize dynamic aggregation of links.

4. Analysis of Networking Technical Fault Cases

Networking technology is a variety of highly difficult protocols, including DHCP, ACL, DNS, PAT and Ethernet channels, etc., and it is difficult to eliminate errors during configuration, which requires a good command of knowledge points and a deep understanding.

4.1. DHCP Fault Analysis

The basic configuration of DHCP is as follows:

```
Router(config)# ip dhcp excluded-address low-address [high-address] (Excluding IP addresses)
Router(config)# ip dhcp pool pool-name (Define address pool)
Router(dhcp-config)# network ip-address subnet-mask
Router(dhcp-config)#default-router address
```

DHCP executable tasks and commands are shown in Table 1.

Table 1. DHCP executable tasks and commands

Executable tasks	Command
Define DNS server	dns-server *address*[*address2...address8*]
Define domain name	domain-name domain
Defines the duration of a DHCP lease	lease {*days* [*hours*] [*minutes*] | *infinite*}
Define the NetBIOS WINS server	netbios-name-server *address*[*address2...address8*]

DHCP failure usually occurs when the DHCP service is configured, the subnet mask, DNS address and default gateway Settings of the network segment are wrong, which causes the wrong address to be assigned to the PC and the PC cannot access the network. Or if the occupied IP address is not excluded, the used IP address cannot be reassigned, resulting in DHCP acquisition failure.

4.2. Physical Interface Fault and DNS Fault Analysis

(1) Physical interface failure

Physical interface failure means that the connection between devices is connected to the wrong interface, which leads to a blocked line. If the line is blocked, red dots will appear; if the line is unblocked, green dots will appear, as shown in Figure 2.

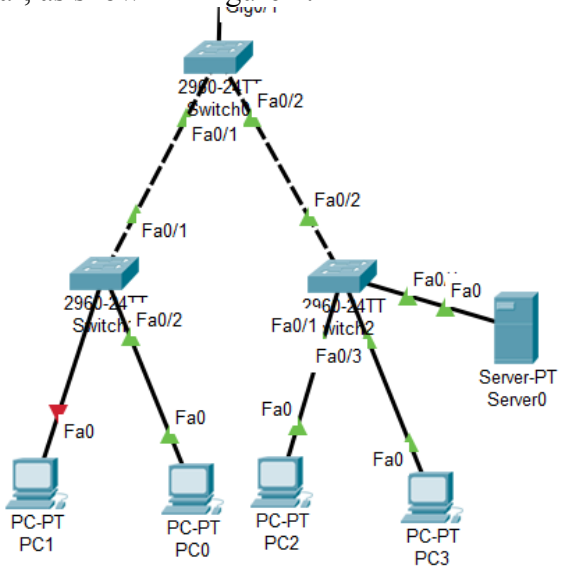

Figure 2. Physical interface and DNS fault topology diagram

(2)DNS failure

DNS failure refers to the failure of PC's DNS address configuration to access web pages through the browser.

4.3. ACL Fault Analysis

(1) ACL statement error

ACL statements are prone to errors when set, and every deny statement implicitly rejects all traffic, while not adding permit statements rejects all traffic.

(2) ACL port implementation error

ACLs are enforced on the router's port or VLAN, and the flow of traffic is controlled by in and out. ACL enforcement on the wrong port invalidates ACL statements.

4.4. PAT Fault Analysis

The basic configuration commands for NAT are as follows:

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 interface serial 0/1/0
R2(config)# interface serial 0/0/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/0
R2(config-if)# ip nat outside
```

PAT needs to be configured in conjunction with the ACL command, first making sure that the ACL statement has no errors. In addition, the configuration of static routing and internal and external ports is also a high point of failure, which requires careful consideration.

5. Design of Teaching Cases

Take the VLAN failure case as an example, and the VLAN case topology diagram is shown in Figure 3.

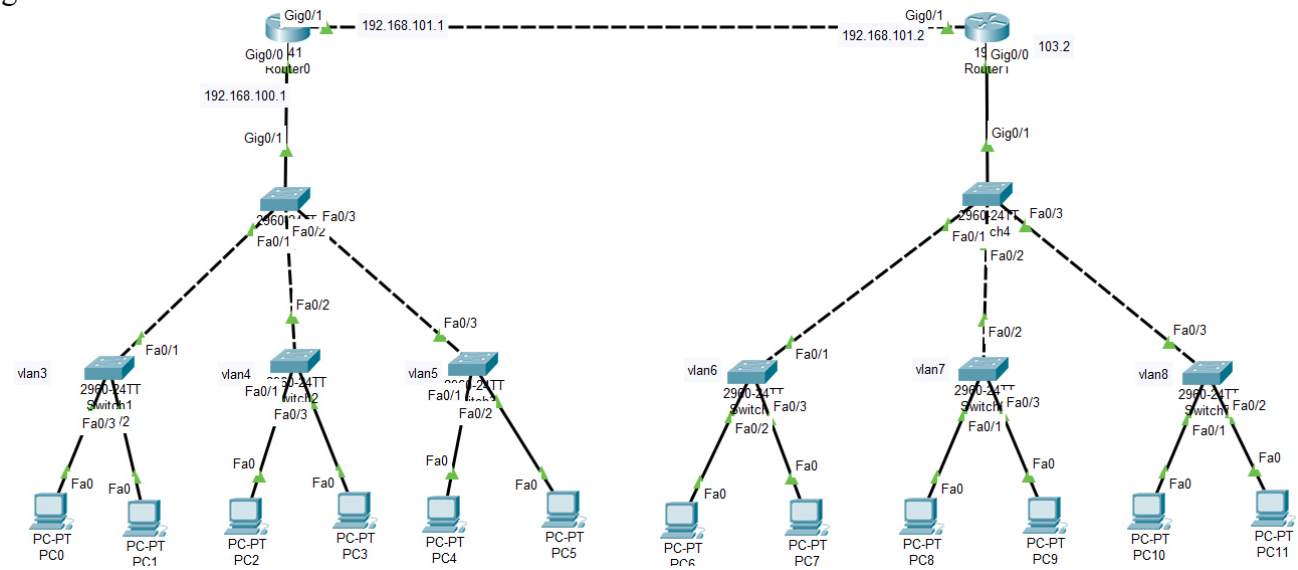

Figure 3. VLAN case topology

5.1. Cases Design I：Missing VLAN

Description of failure: In Figure 3, the router configuration is correct. PC2 can ping other PCs in VLAN4, but not other VLANs.

Failure analysis: PC2 is able to ping other PCs under VLAN4, which indicates that the configuration of PC2 itself and S2 are correct. Now PC2 is used to try to ping the G0/0 port of R0, and it is found that it cannot ping, so it is speculated that the fault occurs between S2 and R0, that is, S8.

Open the CLI interface of S8, enter privilege mode, type “show vlan brief”, and get the result as shown in Figure 4.

```
Switch#Show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
--------------------------------
1    default                           active    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, Gig0/2
2    VLAN0002                          active
3    VLAN0003                          active
5    VLAN0005                          active
7    VLAN0007                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Figure 4. VLAN summary

It was found that VLAN4 was not created in S8 and a VLAN was missing, resulting in VLAN4 being unable to communicate with other VLANs. VLAN8 should be created in S8.

The configuration is as follows:

```
Switch >enable
Switch #configure terminal
Switch(config)# vlan 20
```

5.2. Cases Design II：VLAN Table is Incorrect

Fault description: PC0 and PC1 can only ping each other, not other VLANs.

Fault analysis: now PC0 and PC1 are used to try to ping the G0/0 port of R0, but it is found that it cannot be ping. It is speculated that the fault occurs between S2 and R0, namely S8. There is VLAN3 in S8. It is speculated that the port setting of S8 is wrong. Enter the privilege model and enter the “show interface trunk” to get the results shown in Figure 5.

```
Port        Vlans in spanning tree forwarding state and not
pruned
Fa0/1       2,3,5
Fa0/2       2,3,5
Fa0/3       2,3,5
Gig0/1      2,5
```

Figure 5. VLAN table

Found that S8's G0/1 port does not allow VLAN3 traffic through, VLAN table error. Modify the command as follows:

```
Switch >enable
Switch #configure terminal
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport trunk allowed vlan 2,3,5
```

5.3. Cases Design III：The Native Table Does Not Match

Description of failure: The CLI interface for S7 always generates console notifications as shown: “Native VLAN mismatch discovered on FastEthernet0/3(1), with Switch FastEthernet0/3(2)”.

Failure analysis: Trunk ports are configured with different native VLANs that generate console notifications, resulting in miscommunication of control and management traffic and security threats. The native VLAN should be modified to VLAN1 with the following command:

```
Switch >enable
Switch #configure terminal
Switch(config)#interface gigabitEthernet 0/3
Switch(config-if)#switchport trunk native vlan 1
```

5.4. Cases Design IV：TRUNK Mode Mismatch

Fault description: PC10 can ping each other, but not other VLANs.

Fault analysis: According to the analysis, the fault is between S7 and S4, and the fault of (1) and (2) is eliminated. Enter the privilege modes for S4 and S7 respectively and enter “show interfaces f0/3 switchport” to get the results shown in Figures 6 and 7.

```
Switch#show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dotlq
Operational Trunking Encapsulation: dotlq
```

Figure 6. The F0/3 port summary for S4

```
Switch#SHow INterfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dotlq
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
```

Figure 7. The F0/3 port summary for S7

If a pattern mismatch is found on both sides of the TRUNK link, the f0/3 port of S7 should be corrected to be in TRUNK mode. The command is as follows:

```
Switch >enable
Switch #configure terminal
Switch(config)#interface gigabitEthernet 0/3
Switch(config-if)#switchport mode trunk
```

6. Conclusion

This paper mainly studies the application of fault cases based on campus network in teaching practice. Combined with real fault cases of campus network, it is transformed into teaching cases, which enriches the teaching resource base and achieves better teaching effect and evaluation. All kinds of basic fault cases and comprehensive fault cases have been designed and deployed. The topological network runs smoothly and has certain innovation. The design of complex teaching cases based on campus network can not only stimulate students' learning initiative, promote the improvement of their ability to solve practical complex engineering problems, but also help to improve the quality of application-oriented talents training in network engineering.

Acknowledgements

This work was Supported by Shandong Provincial Key Research and Development Project (No. 2018CXGC0706), Natural Science Foundation of Shandong Province (No. ZR2019LZH015), Projects of Ministry of Education Industry-University Cooperation Education (No. 201901234008, 201901166007, 201801154085).

References

[1]. Nie, L., & Hu, S. (2019) Simulation and analysis of campus network based on OPNET. Journal of Computational Methods in Sciences and Engineering, 19(1), 3-12.

[2]. Xu, L. (2020) Research on the Reform and Practice of Secretarial Teaching Work based on the Training of Applied Talents. Journal of Contemporary Educational Research, 4(7).

[3]. ZHANG, X., LIU, Y.W., DENG, S.W. and Dong, Y.I.N., (2018) "Exploration and Reform of the Practical Teaching Mode of Computer Composition Principle Experiment under the Target of Applied Talents Training". DEStech Transactions on Social Science, Education and Human Science, (emass), 2018, 11-17.

[4]. Jimena Medina, I., Gómez-Luque, M. A., Peña Amaro, J., Luque Ruiz, I., & Gómez-Nieto, M. A. (2019) HistoNFC: An innovative tool for the practical teaching of histology using NFC technology. Wireless Communications and Mobile Computing, 2019, 1-16.

[5]. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018) Smart contract-based access control for the internet of things. IEEE Internet of Things Journal, 6(2), 1594-1605.

[6]. Qian Wang, Shan Jing and Bin Xiao. (2017) Study on Network Troubleshooting Teaching Case Based on Campus Network. Proceedings of 2017 4th International Conference on Economic, Business Management and Education Innovation, 86, 329-334.

[7]. Mathew, A., & Prabhu, B. (2017) A Study on Virtual Local Area Network (VLAN) and Inter-VLAN Routing. International Journal of Current Engineering and Scientific Research (IJCESR), 4(10).

[8]. Chanak, P., Banerjee, I., & Sherratt, R. S. (2017) Energy-aware distributed routing algorithm to tolerate network failure in wireless sensor networks. Ad Hoc Networks, 56, 158-172.

[9]. Yang, H., & Liu, Z. (2019) An optimization routing protocol for FANETs. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-8.

[10]. Irawati, I. D., Hadiyoso, S., & Hariyani, Y. S. (2017) Link Aggregation Control Protocol on Software Defined Network. International Journal of Electrical and Computer Engineering, 7(5), 2706.

[11]. Takashi Kurimoto, Shigeo Urushidani, Eiji Oki. (2018) Optimization Model for Designing Multiple Virtualized Campus Area Networks Coordinating With Wide Area Networks, IEEE Trans. Netw. Serv. Manag, 15(4), 1349-1362.