Based on Large-Scale Routing Protocol OSPF Security Analysis and Prevention Research

2223-CMT400—MSc Project

Jia Hao Zhang

Student ID：21057061

Project Supervisor： George Theodorakopoulos

22th September 2023

Abstract

In recent years, the number of potential vulnerabilities contained in routing protocols has shown a significant upward trend, posing a serious threat to data security. Once these vulnerabilities are exploited by malicious attackers, they may cause varying degrees of damage to the confidentiality, integrity, and availability of data. In this issue, special attention needs to be paid to the large-scale routing protocol OSPF, as it plays an important role in the core network infrastructure. As an internal gateway protocol, OSPF is widely used in the backbone networks of enterprises and internet service providers to provide efficient routing and forwarding capabilities. However, due to its openness and complexity, the OSPF protocol faces various security challenges, such as malicious attacks, OSPF denial of service attacks, OSPF other LSA forgery, and other security threats. In this situation, it is particularly urgent to conduct comprehensive research on the security issues of routing technology in the current network era. In particular, it is necessary to conduct in-depth research on attack and defense strategies against the OSPF protocol to cope with the constantly evolving network threats. There are three main contributions to this article. Firstly, establish a virtual routing experimental platform. This article has completed the construction of a virtualization routing experimental platform, providing an experimental environment for subsequent experiments, enabling us to better simulate and observe the behavior of routing protocols. Secondly, simulate the attack impact of the Denial-of-Service attack and OSPF Other LSA falsification. By constructing a large number of fake OSPF data packets, we utilized the OSPF Other LSA falsification principle to simulate the OSPF Hello Flooding Attack, sending a large number of illegal data packets to the multicast addresses monitored by the OSPF protocol. The experimental results show that this attack leads to latency issues in OSPF networks, and packet transmission is significantly delayed. Finally, use the OSPF Denial of Service (DoS) attack to steal the routing information of the target router. We utilized the default routing feature of OSPF and combined it with the principle of DoS attack to successfully steal the routing information of the target router. This discovery reveals that attackers may carry out targeted attacks and obtain sensitive information by exploiting protocol vulnerabilities. Through this study, we emphasize the fragility of the OSPF protocol, especially its vulnerability to Hello Flooding and DoS attacks. These attacks not only threaten the normal operation of OSPF networks but may also affect a wider network ecosystem. This article addresses the urgency of OSPF protocol attacks and defense strategies, providing important insights for network administrators and security professionals to take necessary protective measures to ensure network security and stability.

Table of Contents

List of figures

Abbreviations

Abbreviations	**Full Name**
OSPF	Open Shortest Path First
IGP	Interior Gateway Protocol
ICMP	Internet Control Message Protocol
RIP	Routing Information Protocol
ABR	Area Border Router
LSDB	Link State Database
DR	Designated Router
BDR	Backup Designated Router
ACL	Access Control List
NAT	Network Address Translation
LSA	Link State Advertisement
1 LSA	Router LSA
2 LSA	Network LSA
3 LSA	Summary LSA
4 LSA	ASBR Summary LSA
5 LSA	External LSA
7 LSA	Not So Stubby Area LSA
#	# Afterwards, it represents an explanatory statement

Introduction

1.1 Background and significance of the project

With the rapid development of the Internet and the expansion of enterprise networks, the world is facing a severe network security situation, with various network security threats constantly emerging and attacks on network protocols becoming increasingly fierce. Among them, large-scale routing protocols (such as OSPF) play a crucial role in the core network infrastructure. As an internal gateway protocol, OSPF is widely used in the backbone networks of enterprises and internet service providers, providing efficient routing and forwarding. However, the OSPF protocol encounters various security challenges due to its openness and complexity malicious attacks, OSPF Denial of Service attacks OSPF Other-LSA falsification and other security threats pose significant risks to the stability and availability of OSPF networks.

1.2 Purpose of the research project

In this context, the network serves as a bridge for information transmission, relying on routers to connect and extend different network segments. routing protocols play a crucial role as it is the way routers obtain and process information. Therefore, the security of routing protocols directly affects whether information can be accurately and safely transmitted to the destination [1].

The research objective of this paper is to improve the security of OSPF protocol in large-scale networks, reduce security threats faced by networks, and effectively prevent network attacks and data leakage. At the same time, we are committed to improving the quality and reliability of network services, promoting the progress of network OSPF protocol technology, and ensuring the safe operation of enterprise networks. This will help build a more secure and stable network environment, providing users with more reliable network services.

1.3 Current situation of OSPF routing protocol security defects

In the current information age, network security issues have become a global focus of attention. In the entire chain of network security, network routers play a crucial role. They transmit data between routers, maintain smooth network communication, and ensure the stable operation of the entire network. However, routers also face various security threats. Currently, most network technicians' understanding of the OSPF protocol is limited to using it as a tool. Few people have conducted in-depth research on the attack methods of this protocol, let alone the analysis of attack and defense methods. Therefore, it is urgent to conduct in-depth research on the attack technology of OSPF routing protocol, timely understand the attack methods, and make timely responses by analyzing the attack principles to ensure network security [2].

1.4 Based on virtualization simulation platforms

The current Internet environment is becoming increasingly complex, and the security of related routing protocols can no longer meet the growing demands of the Internet environment, resulting in regular network assaults on routing protocols and a deteriorating state of network security. To counter the constantly emerging new types of network attacks, it is urgent to investigate and research various technologies, grasp the latest and cutting-edge attack technologies, and timely propose appropriate prevention plans to ensure communication security. Therefore, it is particularly important to establish an experimental environment that is isolated from the real environment and has a certain scale that can truly and effectively reflect the attack results. The virtualization platform provides an ideal solution to this issue. By using virtualization platforms, multiple virtual machines can be created and managed on physical computers, creating an isolated and controllable simulation environment for simulating real network environments and conducting research on routing protocol attack techniques. Constructing a constructional network on a virtualization platform for routing protocol attack technology research helps to cope with constantly complex and diverse network threats and improve network security defense capacity.

1.5 Research work and main contributions

The main contributions and work of this article include:

(1) A LAN-based OSPF Denial of Service attack and OSPF Other-LSA falsification for OSPF routing protocol has been proposed. This attack method sends a large number of forged OSPF Hello packets to the OSPF multicast addresses monitored by the victim router domain and declares malicious behavior such as default routes that do not exist in the subnet on fake routers. Verify through a virtual experimental platform the network security threats caused by these attack methods, such as network instability and theft of internal network routes.

(2) We have designed and built a LAN platform for routing protocol security, utilizing virtualization platforms and installing important routing protocol software. The platform has developed a protocol security research attack module and adopts a distributed C/S architecture that saves more hardware resources. A comprehensive evaluation of the effectiveness of the proposed preventive measures was conducted through experiments and simulations, revealing the practicality and performance of the proposed solution. The results of this study provide a reference for a deeper understanding of the security issues of the OSPF protocol and practical solutions for protecting OSPF networks from potential attacks.

Thank

I would like to express my heartfelt gratitude to all those who provided support and assistance for the completion of this paper. Without your help and encouragement, this study will not be able to proceed smoothly.

I would like to express my sincere gratitude to my mentor George Theodorakopoulos. You not only provided me with selfless guidance and advice in academia but also provided valuable experience and insights during the research process. Your support and motivation are the driving force for my continuous progress.

1.6 Dissertation outline

The first chapter will provide a background introduction to the theme, as well as the purpose and significance of the research to achieve the expected contribution.

Chapter 2 provides an overview of the background knowledge of routers, routing protocols, and OSPF protocols. Secondly, the process of establishing neighbors and adjacency relationships in the OSPF routing protocol, the division of OSPF regions, the classification of LSA, and the routing rules of the OSPF protocol were studied. Finally, in-depth research was conducted on the shortest path tree algorithm used in the OSPF protocol.

Chapter 3 researches the security of the OSPF protocol itself, providing an in-depth overview of OSPF security mechanisms and hierarchical routing structures, including reliable flooding mechanisms, verification of OSPF packets, and acceptance processes.

Chapter 4 provides an overview of the security mechanism of the OSPF routing protocol, including the hierarchical structure of the OSPF routing, the process of LSA flooding, the acceptance and verification process of OSPF packets, and the analysis of the authentication mechanism of the OSPF protocol itself. It also provides a basic description of the two attack methods of the OSPF protocol in

practice.

Chapter 5 studies the principle of OSPF denial of service attacks proposed by Dr. Gabi Nakibly. A detailed analysis was conducted on the security vulnerabilities in the OSPF adjacency establishment process, explaining the parameters of the special number field in sending false OSPF Hello messages and describing in detail the attack process and parameters that exploit this vulnerability. At the same time, a defense method against OSPF denial of service attacks was proposed. In addition, other LSA forgery methods proposed by Dr. Gabi Nakibly for OSPF were also explored, and the security vulnerabilities of OSPF in the routing learning process were analyzed in detail. The specific method of sending false default routes and the attack methods and processes to exploit this vulnerability were explained. Finally, a method was proposed to defend against OSPF and other LSA forgery attacks.

Chapter 6 aims to provide a basic framework for in-depth research on attacks and defenses in OSPF routing protocols. By utilizing virtualization technology to create an experimental platform, the following main contributions have been achieved. Firstly, a virtualization testing platform was established to lay the foundation for subsequent research. Secondly, the installation and configuration of the required software were completed to ensure the complete functionality of the experimental platform. Importantly, fraudulent OSPF packets were constructed, and different

attack scenarios were simulated by manipulating these packets to analyze potential vulnerabilities and security threats in the OSPF protocol. Successfully established a virtualization testing platform and configured routing software, laying a solid foundation for in-depth exploration of OSPF protocol vulnerabilities and developing corresponding defense measures.

Chapter 7 delves into the construction and attack of OSPF network environment, and enhances network security awareness. The exploration of false packet structures and attack principles provides important experimental data for this article. NMAP scanning detects and constructs forged data packets to verify vulnerabilities in OSPF networks. The load testing of OSPF networks evaluated network performance and provided support for the effectiveness of attack behavior. These studies have had a positive impact in areas such as network security, attack and defense, experimental verification, and performance optimization. At the same time, they also provide substantial reference value for the defense strategies of the OSPF protocol in the following Chapter 8.

Chapter 8 delves into the security enhancement measures of OSPF networks, with a focus on the implementation and significance of OSPF regional authentication and passive-interface protection mechanisms. Firstly, this section provides a detailed introduction to the importance of OSPF regional certification. This mechanism prevents illegal routers from joining by requiring all routers in the area

to use the same authentication password, thereby maintaining the integrity and stability of the network. At the same time, we emphasize the importance of applying passive interface protection mechanisms in OSPF networks. The passive-interface protection mechanism can detect and block unauthorized OSPF Hello messages, thereby reducing the risk of DDoS attacks on the network. These security mechanisms not only help prevent unauthorized access and configuration changes but also protect the network from malicious attacks.

Chapter 9 summarizes the work of the entire article and looks forward to future research directions.

Chapter 2 Overview of OPSF Routing Protocol

2.1 Routers and Routing Protocols

In the 1980s, the emergence of personal computers marked the flourishing development of personal terminal computer applications. During that period, local area networks gradually expanded to wide area networks, enabling efficient sharing and transmission of data files, and greatly promoting information exchange and resource sharing[3]. In the 1990s, with the advancement of the commercialization of the Internet, personal computers gradually became an important node connecting to the Internet. Many enterprises actively use the Internet to conduct business, which has led to the rapid development of the Internet in the commercial field. In the process of achieving close connections between terminal devices such as computers and the Internet, routers have become indispensable network devices. As the core hub of network transmission, routers undertake important tasks such as packet forwarding and routing selection, ensuring efficient and accurate data transmission from source devices to target devices. It greatly enhances the stability and reliability of Internet communication [4]. It is in this historical context that routers have become a key technology for connecting terminal devices such as personal computers to the Internet. Specifically, the main functions of routers include five aspects:

(1) Routing forwarding. Routers determine the optimal forwarding path for data packets by viewing their destination IP address based on a pre-configured routing table. Transfer data packets from the source network to the target network. (2) Network interconnection. Routers establish connections between different networks to achieve network interconnectivity. Through the forwarding function of the router, data packets can be freely transmitted between different networks, achieving communication and exchange between different networks. (3) Packet filtering. Routers can filter and intercept non-compliant packets based on configured access control lists (ACL) or firewall rules. This can protect network security and prevent unauthorized access and attacks. (4) Network Address Translation. Routers support Network Address Translation (NAT), allowing private IP addresses to be accessed on the public internet. Through NAT, routers convert internal private IP addresses to external public IP addresses, enabling communication between internal and external networks. (5) Route notification. Routers are responsible for sending their routing information to other routers through routing protocols such as OSPF, BGP, etc. so that all routers in the network can understand the topology and optimal path of the entire network.

2.2 Fundamentals of Routing Protocol

A routing protocol is a specification in computer networks used for exchanging routing information between routers. It defines how routers communicate, exchange routing table information, and choose the best path to transmit data

packets from the source address to the destination address.

Routers are responsible for transmitting data packets from source devices to destination devices in computer networks. The routing protocol specifies the standards and rules for exchanging network topology and distance information between routers[5].

In computer networks, there are two common types of routing protocols, namely static routing protocols and dynamic routing protocols. Static routing protocols are manually configured, and network administrators need to manually configure the routing table on each router to specify how data packets should be forwarded. The dynamic routing protocol is a protocol that automatically updates the routing table, exchanging routing information between routers and dynamically selecting the best path. Common dynamic routing protocols include RIP, OSPF, BGP, etc. [6].

With the rapid development of the Internet and the expansion of enterprise network scale, static routing can no longer meet the needs of large-scale networks. Static routing protocols cannot quickly exchange network information and can only forward it to fixed node routers according to fixed rules [7]. The dynamic routing protocol can recalculate the latest correct path and forward it promptly based on changes in network topology, without the need for manual intervention

by administrators. Dynamic routing protocols have strong flexibility and automation characteristics [8]. This article will focus on the OSPF protocol in dynamic routing protocols to explore its applications and advantages in large-scale networks.

2.3 Overview of OSPF Protocol

OSPF is an internal gateway protocol used to exchange routing information between routers within an autonomous system. It applies the routing protocol under the TCP/IP protocol cluster[9]. OSPF is a link-state routing protocol that achieves packet forwarding by broadcasting link-state information throughout the entire autonomous system and calculating the shortest path[10]. OSPF is known for its highly reliable and dynamic adaptability to network topology changes.

Firstly, the OSPF protocol discovers neighbors and establishes neighbor relationships through IP data packets, achieving interconnection between routers. Routers exchange Hello messages on the same network, establish neighbor relationships, and exchange link status information through Link State Notification (LSA). These LSAs contain topology information in the network, and through the shortest path priority calculation, each router can calculate the shortest path to reach the target network, thereby achieving efficient packet forwarding [11]. Secondly, to improve the scalability of the network, OSPF divides the autonomous

system into multiple areas. The routers in each region only exchange link state information within the region, reducing the cost of global exchange. The connection between regions is handled by the Area Boundary Router (ABR), which aggregates routing information within the region into the entire autonomous system, promoting the hierarchical design of the network [12]. Finally, the OSPF protocol supports authentication mechanisms to verify the identity of neighboring routers. Authentication ensures that only authorized routers can join the network and prevents the broadcast of malicious link state information, improving network security.

2.4 Operating principle of OSPF

OSPF working principles of include neighbor discovery and establishment, cost calculation, construction of link state database, shortest path priority calculation, routing information exchange, partition and region design, and DR/BDR election mechanism. These steps work together to achieve dynamic routing selection and stable operation of OSPF protocol in large-scale networks.

Firstly, OSPF discovers neighboring routers and establishes neighbor relationships by sending Hello messages. the message is a key component of the OSPF protocol, which is used to achieve neighbor discovery and link state information exchange between routers. As the foundation of the OSPF protocol, Hello messages carry router ID, interface information, and priority information. Each router obtains the

link state information of adjacent routers by sending Hello messages, thereby constructing a network topology map and calculating the optimal path. The periodic sending and receiving of Hello messages are the foundation for establishing neighbor relationships between routers in the OSPF protocol, ensuring the reliability, efficiency, and stability of the network. When two routers receive Hello messages from each other on the same network, they establish a neighbor relationship and begin exchanging link status information. Secondly, the cost value in OSPF is used to calculate the cost or cost of routing. The cost is usually related to the bandwidth of the link, and the larger the bandwidth, the lower the cost. The router will choose the path with the lowest cost as the shortest path. Then, each OSPF router maintains a Link State Database (LSDB), which stores link state information throughout the autonomous system. When routers establish neighbor relationships, they exchange link state information with each other and store the received information in LSDB. Through LSDB, each router can understand the topology of the entire network. In LSDB, each router has a routing table that records the shortest path to each destination network. OSPF uses the shortest path first algorithm (Dijkstra algorithm) to calculate the shortest path. This algorithm considers the cost of the link and selects the path with the lowest cost as the shortest path. OSPF notifies other routers of changes in network topology by sending a Link State Notification (LSA). After receiving LSA, other routers update their own LSDB and routing tables to maintain network consistency and stability [13].

2.5 OSPF adjacency establishment process

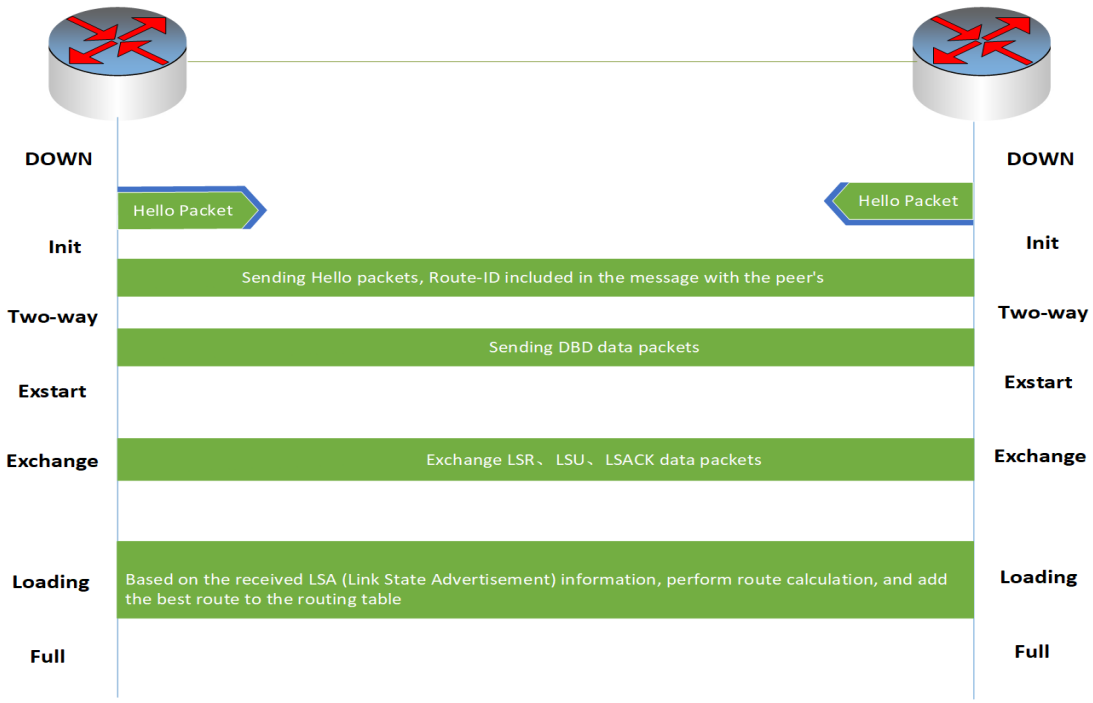


Figure 1: OSPF adjacency establishment process picture

In Figure 1 ensuring consistency in the four fields of Hello message interval, Dead time interval, region ID, and authentication key for establishing OSPF adjacency is a prerequisite for successfully establishing OSPF adjacency. Additionally, the establishment of adjacency requires the participation of Hello, DBD, LSR, LSA, and LSACK messages[14].

(1) Hello message interval. This is the time interval for sending Hello messages, used to detect the survival status of neighbors.

（2）Dead time interval. This is the time interval between determining that a neighbor has expired after receiving no Hello message from the neighbor.

（3）Area ID. In OSPF routers are divided into different areas. The area ID between neighbors must be consistent, otherwise, they will not be able to establish adjacency relationships.

（4）Authentication key. If the authentication function is enabled in OSPF, the authentication keys between neighbors must also be consistent, otherwise, the adjacency relationship cannot be successfully established.

In addition, the types of messages involved in establishing OSPF adjacency relationships are:

（1）Hello message: used to discover and establish neighbor relationships, which includes information such as Hello message interval, Dead time interval, region ID, and authentication key.

（2）DBD (Database Description) message: used to exchange database summary information to determine which link state database (LSDB) entries need to be updated.

（3）LSR (Link State Request) message: used to request neighbors to send specific LSA (Link State Advertisement) information.

（4）LSA (Link State Advertisement) message: used to send link state information to neighbors, describing the network topology that one knows.

（5）LSACK (Link State Acknowledgement) message: used to confirm the received LSA information and ensure that neighbors have received the sent information.

Through the exchange of these packets, OSPF routers can establish adjacency relationships and exchange routing information in the network, achieving optimal path calculation and data transmission

2.6 The process of establishing the adjacency relationship

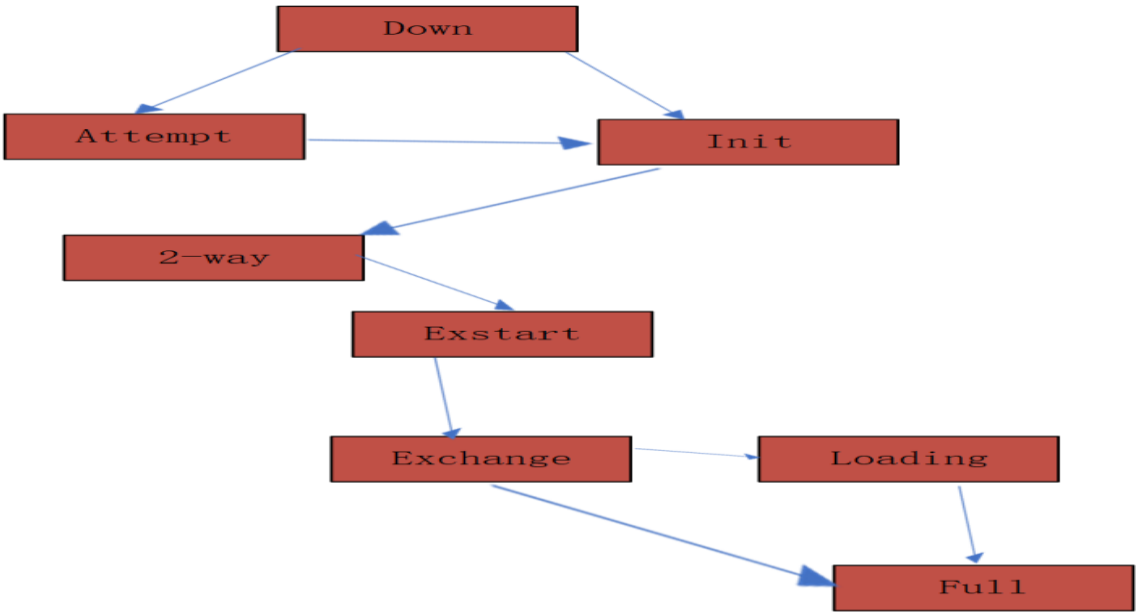


Figure 2: OSPF adjacency establishment process picture

According to Figure 2, there are a total of 8 stages in the OSPF advertising assessment process. Each stage has unique functions.

（1）Downstage: initial state, without neighbors. The router has not received a Hello message from the expected neighbor yet.

（2）Init Stage: When the router receives a Hello message from a potential neighbor, it enters the Init state. At this stage, the router will verify whether the parameters in the Hello message match, including the Hello message interval, Dead time interval, region ID, and authentication key.

（3）2-Way Stage: In this stage, the router establishes two-way communication

with potential neighbors, and they can send Hello messages to each other.

(4) Exstart Stage: In this stage, the router determines who will become the Master and Slave. Master is responsible for sending DBD messages, while Slave is responsible for sending LSR and LSA messages.

(5) Attempt Stage: Between the exstart stage and the Exchange stage, the router attempts to establish a connection or perform other related operations.

(6) Exchange Stage: In this stage, the Master and Slave exchange DBD messages to determine the missing LSA information of the other party.

(7) Loading Stage: In this stage, the Slave sends an LSR message requesting missing LSA information, and the Master sends the corresponding LSA message.

(8) Full stage: In this stage, the databases between all neighbors are fully synchronized, and the adjacency relationship has been established. The router can start exchanging updated LSA information and calculate the optimal path to join the routing table.

Through these eight stages, OSPF adjacency relationships will gradually be established and ensure that the link state database between routers remains

synchronized, thereby achieving effective routing and data forwarding.

2.7 Introduction to OSPF area and different LSA functions

In the OSPF protocol, each router periodically generates LSA and sends it to neighboring routers to share topology information in the network. The main purpose of a Link State Announcement (LSA) is to maintain the Link State Database (LSDB) for each router. LSDB is a local database used by OSPF routers to store topology information in the network, including the topology structure and link state information of the entire network. Accelerate the formation of networks and enhance network stability.

OSPF can be divided into Backbone Area, Normal Area, Stub Area, Complete End Area, Not So Stubby Area, and Complete NSSA. The standards developed by the IETF specify different types of LSAs for OSPF, and each type of LSA carries different link state information [15]. Common types of LSA include:

（1）Type 1 LSA (Router LSA): describes the link state information of the router itself, including direct network connection, link state, and neighbor information connected to the router.

（2）Type 2 LSA (Network LSA): describes the link state information of a multicast network, which is broadcasted by DR (Designed Router) to other routers to

identify members of the multicast network.

（3）Type 3 LSA (Network Summary LSA): Summarizes the network information within an area. Used to describe the connection status of the network and can only spread within this region.

（4）Type 4 LSA (ASBR Summary LSA): Used to describe the information of ASBR (AS Boundary Router) routers connected to other areas in one area, and to notify routers in adjacent areas of information from autonomous systems to area boundary routers.

（5）Type 5 LSA (AS External LSA): Used to describe routing information to external destinations in other regions. It can propagate within the entire autonomous system.

（6）Type 7 LSA (Not So Stubby Area LSA): Used to describe routing information to external destinations in other areas in the Not So Stubby Area (NSSA).

Regardless of the type of LSA, it is composed of LSA headers and LSA content, and each type of LSA has a specific propagation range and unique functions. Through LSA exchange, OSPF routers can maintain the latest link state information. When the network topology changes, the router can update the LSDB in a timely

manner and recalculate the optimal path to ensure that data packets can be transmitted according to the optimal path. Link state notification is a key mechanism of OSPF protocol in implementing dynamic routing and building network topology. It enables OSPF to adapt to complex network environments and provide efficient packet forwarding and routing selection.

2.8 Shortest Path Tree Algorithm

In the OSPF protocol, the shortest path tree algorithm is an important algorithm used to calculate the shortest path between routers. The shortest path tree algorithm is mainly extended based on the Dijkstra algorithm to construct the shortest path tree for each router, thereby determining the best path to reach other nodes in the network [15].

The actual calculation process of the shortest path tree algorithm may involve various optimization techniques, such as using priority queues to accelerate node selection and distance updates and utilizing the characteristics of network topology to simplify the calculation process. Finally, through the shortest path tree algorithm, OSPF routers can calculate the optimal path to other nodes in the network, thereby achieving efficient packet forwarding and routing selection.

2.9 Summary of this chapter

This chapter provides a detailed introduction to the basic concepts of routers and routing protocols, as well as the basic knowledge of OSPF routing protocols, including the process of establishing neighbors and adjacency relationships in OSPF routing protocols, as well as the functional explanations of different LSA. It also provides an actual explanation of the generation method of OSPF shortest-path trees.

Chapter 3 Research on OSPF Protocol Security

3.1 Overview of OSPF Security

With the increasing attention paid to network security issues, routing protocols, as the foundation of network communication, their security is crucial. Although the OSPF protocol introduces some security measures during its design, due to its long history and inherent vulnerabilities, these measures cannot fully guarantee its security. Therefore, this chapter aims to conduct an in-depth analysis of the security of the OSPF protocol from four aspects and comprehensively discuss its potential vulnerabilities. On this basis, we will explore possible attack methods that can be applied to the OSPF protocol and conduct a detailed assessment of the harm these attack methods pose to the network. Subsequently, we will propose a series of solutions to address these potential vulnerabilities to enhance the security of the OSPF routing protocol.

3.1.1 Hierarchical routing structure

OSPF adopts a hierarchical routing structure, aiming to improve the scalability, stability, and management of the network[16]. In the OSPF protocol, multiple subnets and hosts within an autonomous system are combined into a domain through routers, forming a network unit called a domain. Each domain consists of routers that contain network and host interfaces, responsible for forwarding data

and maintaining network topology information within the domain. This approach enables the OSPF protocol to effectively manage and organize complex network structures, providing efficient, flexible, and reliable data transmission and routing choices.

To ensure the security of the OSPF protocol, various security mechanisms have been introduced. The authentication mechanism is used to verify the identity of neighboring routers and prevent unauthorized routers from joining the network and broadcasting malicious information. The message encryption mechanism ensures the confidentiality and integrity of OSPF communication, preventing message tampering and eavesdropping [17]. Timer settings are used to reasonably configure neighbor relationship establishment time, link state information refresh time, etc., to prevent specific attacks. Security zone partitioning divides autonomous systems into multiple zones, reducing network complexity and limiting attack range. Router priority is used for DR or BDR in election areas to improve network stability. The routing filtering mechanism can restrict or prohibit the propagation of specific routing information, avoiding potential attacks and failures.

3.1.2 Reliable flooding mechanism

OSPF adopts a reliable flooding mechanism to achieve the transmission and update of routing information. The flooding mechanism is the core method for

implementing link state broadcasting in OSPF, ensuring that every router in the network can obtain the latest link state information on time [18].

Firstly, neighbor relationship establishment is the process of establishing neighbor relationships between OSPF routers through Hello message exchange. Once the neighbor relationship is established, routers begin to exchange link state information between them.

Secondly, link state broadcasting refers to each OSPF router flooding its link state information to all neighboring routers through Link State Advertisement (LSA).

Thirdly, the update mechanism of LSA refers to when a router receives an LSA sent by a neighboring router, it checks whether the received LSA is more recent than its locally stored information.

Fourthly, when the link state information changes, each OSPF router recalculates the shortest path tree based on the new LSDB information to determine the optimal path to other routers.

Finally, in addition to LSA flooding, OSPF routers also periodically send Hello messages to maintain neighbor relationships. The Hello message contains the ID, interface information, and priority of the router, which is used to confirm whether

the neighbor is alive and establish a neighbor relationship.

3.1.3 Verification mechanism for OSPF messages

The OSPF protocol aims to ensure the integrity and authenticity of messages, to effectively prevent malicious tampering or forgery of messages. OSPF adopts authentication and encryption technology as its core means. The authentication function allows routers to add authentication fields to OSPF messages to verify their legitimacy. The router that sends the message can choose to authenticate and add corresponding authentication information to the message. The router that receives the message will verify the correctness of the authentication information to confirm whether the message comes from a legitimate router. OSPF supports multiple authentication types, including plaintext authentication and MD5 authentication, among which MD5 authentication is a commonly used type. In MD5 authentication, routers use the MD5 algorithm to calculate the authentication digest and attach it to the message. This authentication digest is calculated through the authentication key and message content. The router that receives the message also uses the same authentication key and message content to calculate the authentication digest, and compares it with the received authentication digest. If the two match, it indicates that the message is legal; Otherwise, the message may be tampered with or forged. Through authentication mechanism and MD5 encryption, OSPF messages are verified and protected to a certain extent [19].

3.1.4 The acceptance mechanism of OSPF messages

The receiving mechanism of OSPF messages refers to the process by which routers receive and process OSPF messages from neighboring routers. Its main goal is to parse the message content, update the Link State Database, calculate the shortest path tree, and maintain the state with neighboring routers.

Firstly, when an OSPF router receives an OSPF message sent by a neighboring router, the primary task is to verify the legitimacy of the message, including verifying the authentication information and checking the correctness of the message format.

Secondly, the received message is parsed and the router extracts various fields and information, including message type, sender router ID, region ID, link-state type, neighbor router ID.

Thirdly, based on the parsed message content, the router will update the local link state database to record link state information from neighboring routers, including connection and network topology information learned by neighboring routers.

Fourthly, after updating the LSDB, the router will use the Shortest Path First

algorithm to calculate the shortest path tree to find the optimal path to other routers.

Finally, after establishing a neighbor relationship with the neighboring router, the router will regularly send Hello messages to maintain the status of the neighbors. If the router receives a Hello message from a neighbor, it indicates that the neighbor router is still active and the neighbor relationship is still valid.

Through these steps, OSPF routers can receive and process OSPF packets from neighboring routers, update link status information promptly, calculate the shortest path tree, and maintain neighbor status with neighboring routers. This receiving mechanism ensures the normal operation of the OSPF protocol in the network, achieving dynamic adaptability and stability of the network. In attacks against the OSPF protocol, the attacker's intention to launch an attack is not simply to forge or tamper with a single message but may require a series of complex message constructions. Therefore, this receiving mechanism provides important guarantees for the security of the OSPF protocol.

3.2.1 Research on the vulnerabilities of OSPF routing protocol

The OSPF protocol, as a link-state routing protocol, provides fast and efficient computing and forwarding services for routers running OSPF through its exquisite internal mechanisms. Its advantage is that when the network connection changes,

OSPF can quickly adjust and update routing information to adapt to the new network topology [20].

However, such internal design also brings potential vulnerabilities that may be exploited by illegal attackers, posing a serious threat to the network. Therefore, while providing efficient routing services, it is particularly important to ensure the security of the OSPF protocol.

3.2.2 Local influence global

The OSPF routing protocol achieves a description of the entire network topology by transmitting link state information, enabling each router interface to understand the network structure. Each OSPF router generates link state notification information that describes the status of its various interfaces and passes it on to adjacent OSPF routers, thereby spreading the topology information of the entire network. This interactive process enables OSPF routers to calculate the optimal forwarding path and achieve efficient data forwarding.

However, due to the lack of an end-to-end authentication mechanism in the OSPF protocol itself, once a router is attacked, it may face the threat of link state information being tampered with. If an illegal attacker seizes a router within the OSPF domain, they can not only manipulate and generate incorrect information but also publish this information to other routers running the OSPF protocol,

thereby affecting the routing calculation and data forwarding of the entire network. This potential threat may lead to network instability and unpredictable failures.

3.2.3 OSPF Denial of Service attacking

The Denial of Service attacking attack is a network attack targeting the OSPF protocol. In OSPF networks, routers discover and establish neighbor relationships by sending "hello" messages between them. Malicious attackers utilize this feature to send a large number of forged OSPF hello messages and broadcast them to multiple routers in the network. These forged hello messages impersonate legitimate OSPF routers and are sent to all possible targets [21]. Attackers use forged hello packets to attempt to confuse routers in the network and disrupt the normal neighbor discovery process.

When the network is subjected to OSPF hello flooding attacks, the attacker sends a large number of forged OSPF hello messages, which may contain false router ID, neighbor ID, and other deceptive information. These forged packets will be broadcasted to all routers in the network, leading to neighbor relationship confusion, frequent restarts, network congestion, incorrect routing information, and information leakage among routers.

（1）Neighborhood relationships are chaotic. Due to the attacker sending a large

number of forged hello messages, the normal OSPF neighbor discovery process is disrupted, and the router may establish adjacency relationships with multiple forged neighbors in a short period.

(2) Frequent restarts. Due to the continuous sending of a large number of forged hello messages, routers may be forced to frequently restart the OSPF protocol to cope with changes in neighbor relationships.

(3) Network congestion. A large number of forged hello messages can occupy network bandwidth and processing resources, leading to network congestion.

(4) Incorrect routing information the forged hello message sent by the attacker may contain false routing information , resulting in incorrect forwarding or loss of data packets.

(5) Information leakage. Attackers can obtain information about network topology and routers by sending forged hello packets.

3.2.4 OSPF Other-LSA falsification

OSPF Other LSA falsification is a complex network attack targeting the OSPF routing protocol. In this attack, the attacker attempts to send a fake LSA to deceive the OSPF router and tamper with the default routing characteristics utilized by its

routing table, in order to redirect network traffic to the location controlled by the attacker [22]. Firstly, the attacker conducts network reconnaissance to detect the OSPF router running in the target network and its neighbor relationships. Then, the attacker creates forged OSPF routing information, including fake link state advertisements. In a forged LSA, the attacker claims to have control over a subnet or autonomous system and has the authority to announce the routing information of that subnet.

Secondly, attackers inject forged LSA information into the target network, which can be achieved through fraudulent OSPF hello packets or direct network access. When other OSPF routers receive these forged LSAs, they will include them in their link state database. In the forged LSA, the attacker inserts a new default route, pointing it to the destination controlled by the attacker. Finally, with the operation of the OSPF protocol, forged LSAs will propagate in the network. Once other routers update their routing tables and adopt forged default routes inserted by the attacker, traffic in the network will be directed to the destination specified by the attacker. This may cause data packets to be intercepted, tampered with, discarded, and even cause service interruption and data leakage.

A detailed description of the attack principle:

(1) Network reconnaissance. The attacker first conducts network reconnaissance to detect the OSPF routers running in the target network and their neighboring

relationships.

(2) Forgery of routing information After obtaining the topology information of the target network, the attacker creates forged OSPF routing information.

(3) Inject forged information The attacker injects forged LSA information into the target network.

(4) Default route tampering. In a forged LSA, the attacker will insert a new default route, pointing it to the destination controlled by the attacker.

(5) Information dissemination. Once the forged LSA is injected and propagated to the target network, other OSPF routers will receive these forged LSAs and incorporate them into their own LSDB.

(6) Traffic redirection. When the router updates its routing table and adopts a forged default route inserted by the attacker, the traffic in the network will be directed to the destination specified by the attacker.

Attackers typically use OSPF default route hijacking to carry out malicious activities such as man in the middle attack, data theft, service interruption, or network sniffing.

3.2.5 Analysis of the Authentication Mechanism of OSPF Protocol

The OSPF protocol introduced authentication mechanisms in the early stages of development to increase mutual trust between routers and ensure the authenticity and integrity of the transmitted link state information. The OSPF authentication mechanism mainly includes two methods: simple plaintext password authentication and MD5 authentication.

（1）Simple plaintext password authentication. In simple plaintext password authentication, when OSPF routers exchange Hello messages, plaintext passwords are attached to the messages as credentials for identity authentication. When the router sends a Hello message, it appends the pre-shared plaintext password to the authentication field and sends it to the neighboring router. The router that receives the Hello message will extract the authentication field and compare it with the expected plaintext password.

（2）Based on MD5 authentication. To improve the security of authentication, OSPF supports MD5 authentication. MD5 (Message Digest Algorithm 5) is a commonly used one-way hash function widely used in the field of information security. The design goal of the MD5 algorithm is to generate a unique and irreversible digest (hash value) for data of any length. This means that regardless of the length of the input data, the length of its hash value is fixed, and the original

data cannot be derived backwards from the hash value [23]. Therefore, the MD5 algorithm is commonly used to verify data integrity and check data consistency.

3.3 Summary of this chapter

The OSPF protocol is a widely used routing protocol on the Internet, and its security is crucial for the security of the Internet. Although the OSPF protocol has a certain basic guarantee for security, the current methods for defending against attacks on the OSPF protocol have not been well addressed. This chapter provides a detailed overview of the security mechanism of the OSPF routing protocol, including the hierarchical structure of the OSPF routing, the process of LSA flooding, the acceptance and verification process of OSPF packets, and the analysis of the authentication mechanism of the OSPF protocol itself. It also provides a basic description of the attack methods of the OSPF protocol in practice.

Chapter 4 OSPF Denial of Service attacks

4.1 principle of OSPF Denial of Service attacks

The principle of the OSPF Hello DoS (Denial of Service) attack is to use Hello packets in the OSPF protocol to launch an attack, consuming the resources of the target router by sending a large number of forged Hello packets, resulting in the unavailability of network services.

The attacker utilizes the working principle of the Hello mechanism to construct a large number of forged Hello packets, which contain false neighbor information and link state. These fake Hello packets will be sent to the target router, and the attacker attempts to deceive the target router into believing that these fake packets are control messages from legitimate routers. After receiving a large number of forged Hello packets, the target router will attempt to process these control messages.

Due to these Hello packets being fake, the target router will incorrectly update neighbor information and link status. In this way, the routing table of the target router may become chaotic, leading to incorrect routing path calculation and affecting the normal transmission of data packets. At the same time, processing a large number of fake Hello packets can consume the computing resources and bandwidth of the target router, leading to a decrease in its performance. When the target router runs out of resources, its services will become unavailable,

leading to network communication interruption and data transmission failure.

4.2 Format of OSPF message header and OSPF Hello packet

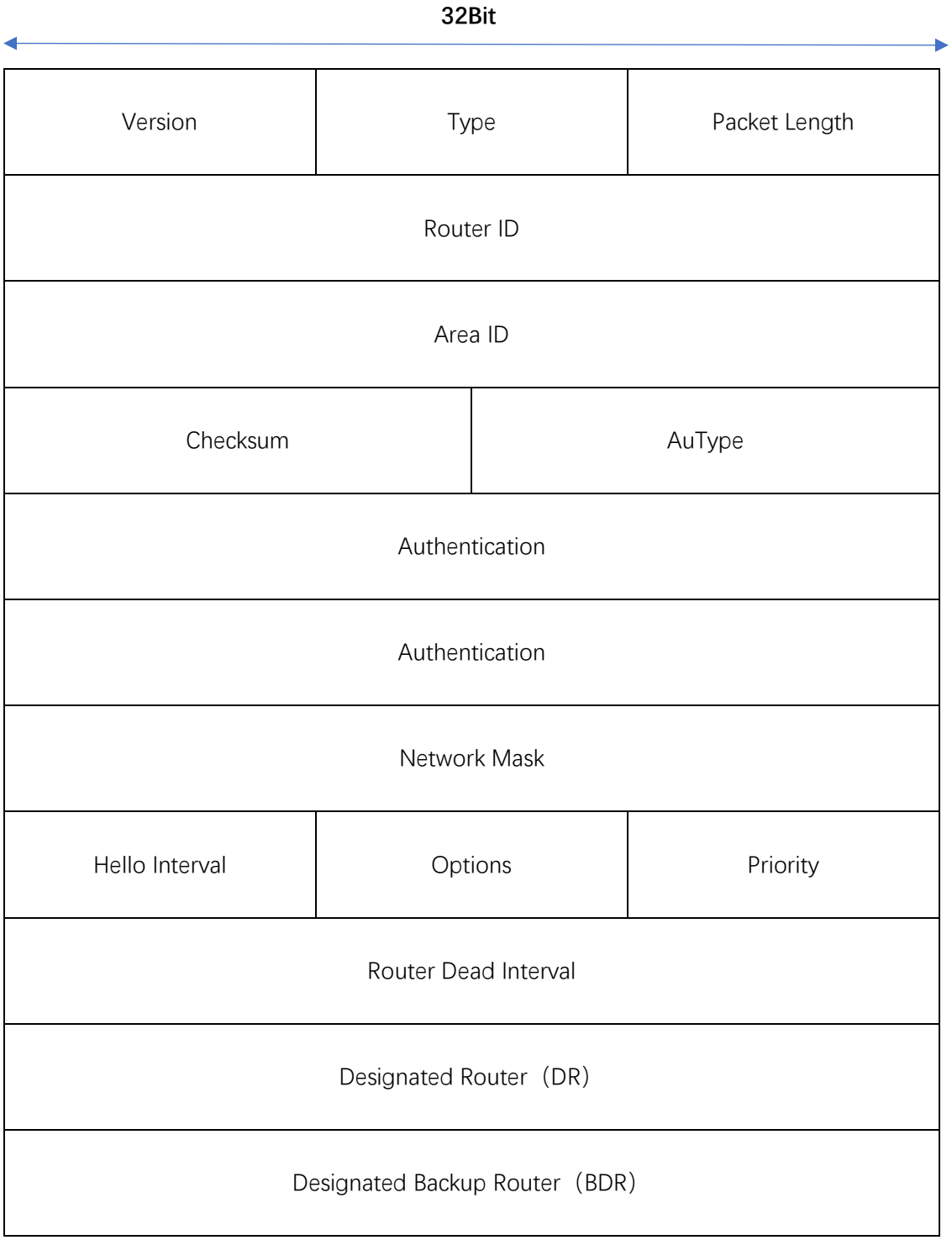


Figure 3: OSPF Format of OSPF message header and OSPF Hello packet picture

In Figure 3, the data packet of OSPF consists of a header and a body, where the header is used to identify and parse the type and information of the data packet. The OSPF message header mainly includes:

Version: 1 byte, indicating the version number of the OSPF protocol. The commonly used version number currently is 2.

Message type: 1 byte, identifying the type of data packet. Different packet types contain different information.

Packet Length: 2 bytes, representing the length of the entire data packet, including the number of bytes in the header and body.

Router ID: 4 bytes, indicating the unique identifier of the router that sent the packet.

Area ID: 4 bytes, representing the area ID of the router sending the packet.

Checksum: 2 bytes, used for integrity check of data packets. The receiver uses checksums and fields to verify whether the packet has experienced errors or losses during transmission.

Instance ID: 4 bytes, used to identify the instance to which the packet belongs in multi-instance OSPF.

Additional Data (Authentication Data): Variable length, used to store authentication information. In OSPF, different authentication mechanisms can be configured to ensure the legality and security of data packets, and this authentication information will be included in this field.

The OSPF packet header contains the necessary fields to identify and parse the type and information of the packet. By parsing the packet header, OSPF routers can determine the purpose of the packet and perform corresponding operations based on its content.

Hello messages are important control messages used for neighbor discovery and link state maintenance. The OSPF Hello message format mainly includes:

Version: 1 byte, indicating the version number of the OSPF protocol. The commonly used version number currently is 2.

Message type: 1 byte, identifying the Hello message type. The Hello message type is 1, indicating that it is a Hello message.

Packet Length: 2 bytes, representing the length of the entire Hello message, including the number of bytes in the message header and content.

Router ID: 4 bytes, indicating the unique identifier of the router that sent the Hello message.

Area ID: 4 bytes, representing the area ID of the router sending the Hello message.

Hello Interval: 4 bytes, representing the time interval between sending Hello messages. This value indicates the time interval between two consecutive Hello messages sent by the sender.

Priority: 4 bytes indicating the priority of the router sending the Hello message.

Router Dead Interval: 4 bytes, indicating the time interval between router failures.

Authentication Type: 4 bytes, indicating the authentication mechanism adopted by OSPF.

Designed Router (DR) IP: 4 bytes, indicating the IP address of the router selected as DR.

Backup Designed Router (BDR) IP: 4 bytes indicating the IP address of the router selected as BDR.

Neighbor List: Variable length, listing the Router ID and IP address of neighbors. This list is used to inform other routers of the current router's neighbor information.

4.3 OSPF Hello Package Construction and Defect Sending Principle

The OSPF Hello packet structure and OSPF router forming neighbors is a complex process, and routers running the OSPF routing protocol use periodic sending of Hello packets to establish and maintain neighbor relationships. On the network layer of the OSI reference model, Hello packets are also sent to multicast 224.0.0.5. This multicast is recognized by all routers running the OSPF routing protocol. The default router running the OSPF routing protocol sends Hello packets every 10 seconds, but in NBMA-type networks, the router sends Hello packets every 30 seconds [24].

The header of the OSPF Hello package is the header of the OSPF package. When the type part of the OSPF header is set to 1, the package becomes the Hello

package. The header of the Hello package contains the router's identification and area identification, which are essential information. The purpose of router identification is to enable other routers to recognize themselves. Two routers can only become neighbors if they have the same area identification. In addition, if neighbor verification is configured on a router running the OSPF routing protocol, the verified data will also be included in the header of the Hello packet. If the verification passwords do not match, the two routers cannot become neighbors. Hello Interval is the time interval between sending Hello packets and Dead Interval is the time when the neighbor relationship expires. That if no Hello packet is received within the time specified in Dead Interval, the neighbor relationship will expire. Two routers can only form a neighbor relationship if the Hello Interval and Dead Interval are the same [25]. Router Priority is the priority of the router. By exchanging Hello packets, routers can understand the priority of their neighbors and the size of their router ID, enabling them to select DR and BDR in the broadcast multi-access network.

There are some insecure issues in the construction process of the OSPF Hello package, including a lack of authentication mechanism, Hello flooding attack, neighbor disguise, and information exposure.

Firstly, due to the lack of a mandatory authentication mechanism during the construction process of OSPF Hello packets, attackers can send forged Hello

packets to deceive other routers into establishing neighbor relationships. The lack of authentication makes Hello packets susceptible to tampering during transmission, posing a potential threat to the network.

Secondly, OSPF Hello packets are transmitted through broadcast to the multicast address 224.0.0.5, which leads to the possibility of Hello flooding attacks. Attackers can utilize this feature to send a large number of forged Hello packets, consume network resources, cause network congestion, and even prevent legitimate Hello packets from reaching the target router, forming a denial-of-service attack, leading to a decrease in network performance and stability.

In addition, the OSPF Hello package contains the router's identity and neighbor information, which attackers can forge an attempt to deceive the target router into establishing adjacency relationships. Such disguises may cause malicious routers to enter the network and lead to incorrect data transmission.

Finally, the OSPF Hello package carries information about the router's identity, area identification, and other network topology. Attackers may obtain sensitive information about network structure and routers by intercepting Hello packets, providing favorable conditions for subsequent construction of false OSPF Hello packet attacks.

4.4 Parameter settings for OSPF Denial of Service attachment

Attackers use the Hello package flooding method to attack. The attacker forges a large number of Hello packets and sends these malicious Hello packets to the target network. These forged Hello packets may contain false router IDs, area identifiers, or authentication information, causing the OSPF router of the target network to handle a large number of invalid neighbor establishment and deletion operations, thereby depleting network resources and bandwidth, causing network congestion and service interruption.

To successfully send fake Hello data packets, the following key points are required to set appropriate parameters:

(1) When conducting OSPF Denial of Service attacks, attackers typically construct malicious Hello packets based on known information and default values to guess the Hello time interval, Dead time interval, and region ID of the target OSPF network. The purpose of doing this is to make the fake Hello package appear as legitimate as possible, to avoid the establishment of adjacency relationships failing due to parameter mismatches.

(2) If the attacker wants to continue maintaining the survival of the neighbor relationship, they can choose to send Hello packets at a time interval smaller than

the default Dead time interval, thereby deceiving the target router into believing that the neighbor router is still alive and continuing to maintain the neighbor relationship.

(3) Attackers usually do not preempt the original DR role to avoid being adjacent to other routers and reduce attack costs. Seizing the DR role requires establishing adjacency relationships with other routers in the region, which increases the exposure risk of attackers and increases attack costs. Therefore, attackers may be more inclined to become DROthers (routers other than DR and BDR), which do not require additional adjacency establishment and can affect DR's election and routing information dissemination. By becoming a DROther, attackers can broadcast forged LSA information to other routers, thereby affecting the routing tables in the network [25].

(4) When conducting OSPF Denial of Service attacks, attackers usually try to use fake Router-IDs to avoid being learned from real IP network segments by other routers. Attackers use false Router-ID to conceal the true IP network segment, increasing the concealment and deception of the attack.

(5) If the attacked area is configured with plaintext encryption authentication, the attacker needs to know the correct key to forge and decrypt OSPF-encrypted messages.

4.5 Defense of OSPF Denial of Service attacks

Based on the analysis of the principle of OSPF Denial of Service attachment in this chapter, the reason for producing OSPF Denial of Service attachment is that attackers forge a large number of fake Hello messages to send to the multicast address 224.0.0.5 that OSPF listens to the following proposes two defense methods for the security configuration of OSPF protocol.

(1) In terms of defending against OSPF Denial of Service attacks, security reinforcement methods that currently exist in the OSPF protocol can be used for defense. In terms of establishing adjacency relationships, the difficulty of establishing adjacency relationships can be increased by modifying the default Hello and Dead time intervals.

(2) In terms of encryption and authentication, it is recommended to use ciphertext message authentication, which encrypts the authentication information using encryption algorithms to ensure the security and reliability of communication. In addition, to increase the difficulty of explosive attacks, the strength of the key should also be strengthened, complex key algorithms and long key lengths should be adopted, which can greatly increase the difficulty of attackers in cracking the key.

4.6 Summary of this chapter

Firstly, a thorough analysis was conducted on the principles of OSPF Denial of Service attachment. Attackers exploit the characteristics of the OSPF protocol to forge OSPF Hello packets and disguise themselves as legitimate neighboring routers in the OSPF network. Sending fake Hello packets to multicast addresses.

Secondly, based on the above research on OSPF Denial of Service attaching, the reasons for the occurrence of OSPF Denial of Service attaching attacks and the steps for OSPF Denial of Service attaching have been clarified.

Finally, reliable defense measures were proposed against OSPF's Denial of Service attachment. Increasing the authenticity verification of adjacent objects and deploying encrypted links are two core measures to defend against false routing and false adjacency attacks.

Chapter 5 OSPF Other-LSA falsification

5.1 OSPF Other-LSA falsification Attacking Principle

With the widespread application of OSPF, some serious security issues are gradually emerging. The link state advertisement (LSA) forgery problem is one of the serious vulnerabilities that lead to routing information leakage and routing black holes. OSPF provides a counterattack mechanism, which is a method used by routers to prevent illegal routers from sending false LSAs on behalf of legitimate routers. When a router receives a false LSA notified by another router on its behalf, the router will immediately notify a newer instance of the LSA to eliminate the impact of the false LSA [26].

In network security, there is a type of attack that involves a combination of OSPF protocol and default routing, known as "OSPF default routing theft" or "Default Route Hijacking" attacks. The goal of this attack is to obtain default routing information and deceive other routers in the network, directing data traffic to the location controlled by the attacker, thereby conducting data traffic theft, tampering, or man-in-the-middle attacks.

5.2 The Counterattack Mechanism of OSPF Routing Protocol

This mechanism is a key security mechanism in the OSPF protocol. When a router

receives a flooded LSA, it determines whether the declared router is itself. If not, it continues to flood. On the contrary, compare the sequence number, checksum, and other parameters of its LSA with the corresponding ones in LSDB. If they are different or updated compared to LSDB, the router will generate the latest LSA based on the latest link state and flood it out. This mechanism can ensure the authenticity of LSA in each router. At the same time, attackers forge the identity of OSPF routers or send false router notifications, making them accepted as legitimate neighbors by other OSPF routers. This may allow attackers to gain greater control over the OSPF domain.

5.3 The Flooding Mechanism of OSPF Protocol

The flooding mechanism of OSPF protocol refers to a communication method used by OSPF routers to exchange link state information (LSA) [27]. The flooding mechanism ensures that all OSPF routers in the network can timely understand the topology information of the entire network, thereby constructing the optimal routing table.

When an OSPF router detects a change in network topology, it generates the corresponding LSA and broadcasts it to all OSPF neighbors directly connected to it. After these neighbors receive the LSA, they will continue to broadcast it to their neighbors, and so on, until all OSPF routers receive the LSA.

5.4 Verification and inspection

After receiving protocol packets, the OSPF protocol must undergo strict verification for the IP layer to receive data packets, which is mainly divided into three steps. The first step is mainly to verify the IP header. The IP checksum must be correct, and the destination address of the data packet must be the accepted IP address or multicast address. The IP protocol type must be OSPF 89, and the IP source address must be checked to prevent multicast packets sent by oneself from being accepted by oneself [28]. In the second step OSPF header, version, region ID, and authentication type must all be the same. The third step mainly targets specific protocol groups, and different types will undergo different verifications. The process of verification and inspection can ensure the normal use of the protocol and enhance its security.

5.5 Security threats to protocols

Although the OSPF protocol has security mechanisms such as a counterattack mechanism, protocol packet authentication, checksum checking, and flooding mechanism, there are still some vulnerabilities in the protocol itself that can be easily exploited by illegal attackers. The current method of OSPF Other LSA falsification attacks is route spoofing attacks.

5.5.1 Routing spoofing attacks

Route spoofing is an attack method that utilizes protocol vulnerabilities to forge LSA and tamper with routing information. Once an attacker implements a routing spoofing attack, it will seriously affect the security and quality of the network. Causing the leakage of routing information, routing loops, network paralysis, and other consequences [28]. And routing will choose a flooding mechanism, which will further enhance the destructive power of routing spoofing attacks.

5.6 Introduction to the default routing

The default route is usually used to indicate the next hop address to which packets should be forwarded when there are no matching routing entries in the routing table for the target network [29].

When a router receives a packet, it looks at the destination IP address and attempts to find a matching destination network in its routing table. If a matching routing entry is not found in the routing table, the router will forward the packet to the next hop address specified by the default route. The default route is usually used to handle situations where the target network is unreachable, serving as the "last resort" of the routing table, sending packets to the next suitable router for further attempts to forward.

5.6.1 OSPF declares default routes

In the OSPF protocol, "default routing" is a special routing term used to handle situations where the target IP address cannot match any known target network. When the router cannot find a specific routing item that matches the target IP address, it will forward the packet to the next hop address specified by the default route [30].

The default route can be declared in two ways in OSPF. Firstly, administrators can manually configure a static default route to forward packets to the specified next-hop address. This is very common when connecting to external networks or the Internet, as the OSPF domain may not contain specific routing items for external networks. Secondly, OSPF supports Default Information Origin, allowing an OSPF router to declare a default route to the entire OSPF domain. This default route will be propagated to all OSPF routers, allowing the entire OSPF domain to forward packets to the next hop address specified by the default route.

5.7 OSPF Passive Interface

In the OSPF protocol, passive interfaces refer to those interfaces that do not actively send Hello messages. When an interface is active, it actively sends Hello messages to detect neighboring routers. But some interfaces may not actively send Hello messages, and these interfaces are called passive interfaces [30].

In OSPF, passive interfaces typically refer to interfaces that do not have OSPF neighbors or are connected to non-OSPF networks. For passive interfaces, the router will not send Hello messages because it does not need to establish neighbor relationships.

By configuring certain interfaces as passive interfaces, network exposure and attack surface can be reduced. This can prevent OSPF routing information from being announced to external networks, protecting network privacy and security.

5.8 OSPF Other-LSA falsification Specific Steps of Attack

(1) Attackers forge OSPF routing information. The attacker sends false OSPF routing update messages, disguised as legitimate OSPF routers, to pass false routing information to other routers.

(2) Obtain the default route. The attacker's false routing information contains information about the default route, which is the route targeting 0.0.0.0/0.

(3) Spoofing routers. After receiving false routing updates, other OSPF routers may update their routing table and set the next hop address of the default route to the address controlled by the attacker.

(4) Data traffic redirection. Once the attacker successfully changes the router's routing, all data traffic will be sent to the target specified by the attacker, thereby achieving the goal of stealing traffic from the target router.

5.9 Specific defense measures

(1) Router authentication. Use encryption algorithms such as MD5 to authenticate and encrypt OSPF routing update messages, preventing unauthorized routers from sending false routing information.

(2) Router authentication: Use OSPF MD5 authentication or other similar mechanisms to ensure that only authorized routers can join the OSPF domain.

(3) Configure router interfaces that run the OSPF protocol as passive interfaces to prevent injection attacks from default routes.

5.10 Summary of this chapter

Firstly, a thorough analysis was conducted on the principle of OSPF Other LSA falsification. Attackers use the counterattack mechanism of the OSPF protocol and the flooding mechanism of OSPF to disguise themselves as legitimate neighboring routers in the OSPF network by declaring default routes externally. Establish

adjacency relationships with other genuine and legitimate routers.

Secondly, based on the above research on OSPF Other LSA failure, the reasons for the OSPF Other LSA failure attack and the security threats of the protocol have been clarified, as well as the steps for the OSPF Other LSA failure attack.

Finally, reliable defense measures were proposed against OSPF's Other LSA failures.

Chapter 6 Construction of a Virtualization Platform

6.Introduction to virtualization technology

Virtualization technology plays a crucial role in the fields of modern computing and data centers. It not only provides users with flexibility, efficiency, and reliability but also makes the management and maintenance of IT resources more convenient and economical, providing enterprises and organizations with a new mode of computing resource management and deployment.

6.1.1 The characteristics of virtualization technology

Virtualization technology is an important innovation in the fields of computer science and information technology. It abstracts and isolates computing resources, storage resources, and network resources by creating virtual machines or environments on physical hardware, providing users with a flexible, efficient, secure, and reliable computing environment.

The core idea of virtualization technology is to divide a physical server into multiple virtual machines and run independent operating systems and applications within each virtual machine. Each virtual machine is considered an independent computing resource with its CPU, memory, disks, and network

connections, which are isolated from each other and do not interfere with each other. This resource isolation and multi-tenant support make virtualization technology very suitable for cloud computing networks and data center environments, allowing multiple users to share the same physical server without affecting each other[31].

6.1.2 Application scenarios of virtualization technology

Virtualization technology has a wide range of application scenarios in the network field, providing flexible, efficient, and secure solutions for network architecture. In this paper, we explored the main application scenarios of virtualization technology in networks and elaborated on its advantages in network isolation and management, security assurance, load balancing, flexible routing, and other aspects [32].

Virtualization technology can deploy traffic managers in the network, automatically adjust network resource allocation according to the needs of network traffic, and ensure high availability and performance of the network. In addition, the implementation of virtual soft routing can virtualize ordinary servers into soft routing devices, achieving a flexible and scalable network architecture. This is very useful for building scenarios such as network function virtualization.

6.2 Building a network experimental platform based on the virtualization platform

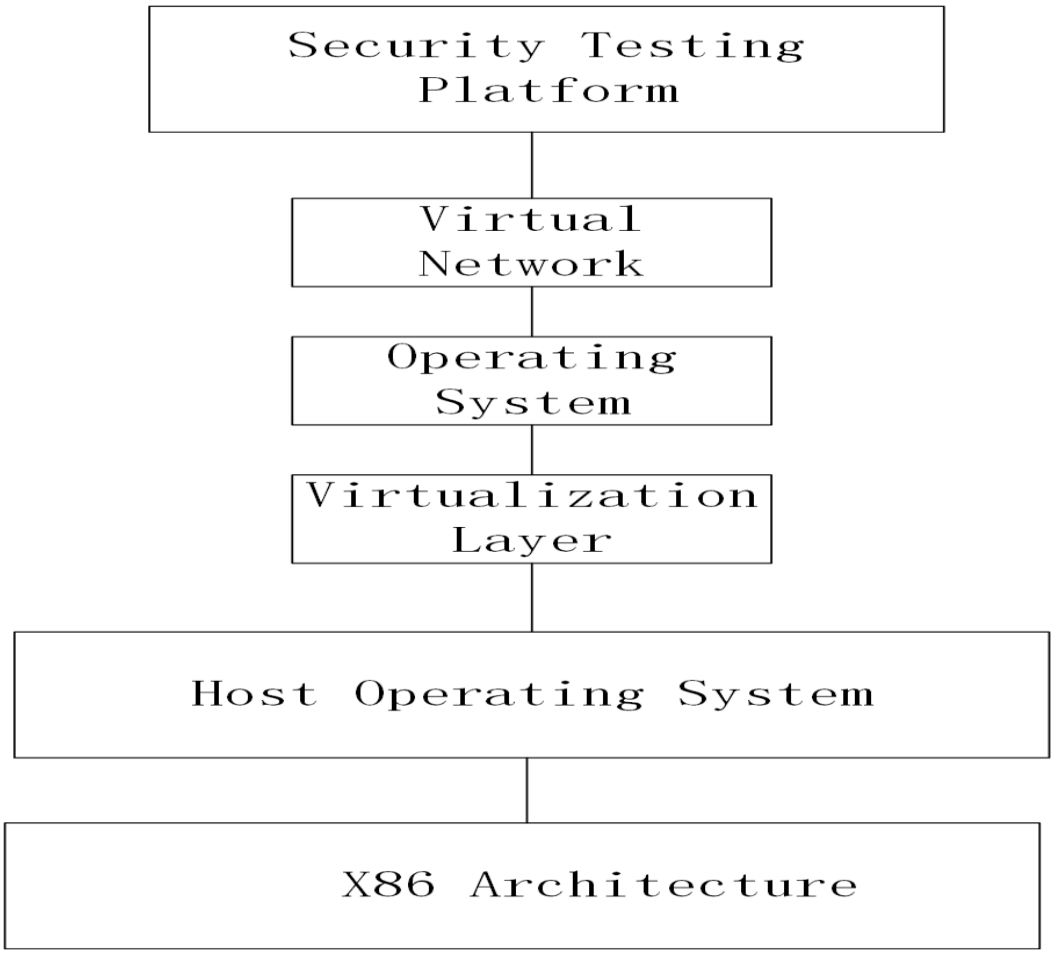


Figure 4: Hosted Architecture picture

As shown in Figure 4. A virtualization platform is a technology built on the X86 architecture, which utilizes the host's operating system as the foundation to build a virtualization layer on top of it. The virtualization layer of this layer plays a key role, allowing multiple independent operating system instances to run in the environment of the host operating system. These independent operating systems are called virtual machines and run in an isolated and mutually independent

manner on a virtualization platform.

The architecture of the virtualization platform is based on the host operating system, which is responsible for managing the allocation and scheduling of hardware resources. On top of the virtualization layer, each virtual machine is assigned an independent set of computing, memory, storage, and network resources, enabling them to run in a relatively isolated environment.

6.3 Hardware requirements for virtualization platforms

In terms of selecting virtual machines, VMware Workstation not only supports multiple operating systems, but also provides an intuitive user interface, allowing users to quickly create, configure, and manage virtual machines. Its high performance and stability ensure smooth operation when multiple virtual machines are running simultaneously on the host system, and the virtual machines are isolated from each other and will not interfere with each other [33]. Based on these advantages, VMware Workstation was chosen as the underlying virtualization platform. Based on network virtualization technology, run a virtual machine on a universal server to simulate a virtual router on a network testing platform.

The assets of the network security platform include:

(1) 1 host: model Lenovo XiaoXinPro 14ACH; Operating system Windows 11; Processor AMD Ryzen 7 5800H with Radeon Graphics 3.20 GHz; Memory 16.0 GB

(2) 1 virtual platform: named VMware Workstation 16 Pro; Version 16.2.4 build-20089737; Memory 14200 MB

(3) 2 servers: system version number CentOS7 (64 bit); Operating System Mirroring CentOS-7-x86_ 64-DVD-1708; Memory 1GB; 1 CPU quantity; Hard disk capacity 20GB

(4) 1 attack server: system version number Debian 10 (64 bit); Operating system mirror kali linux-2023.2a installer amd64.iso; Memory 2GB; CPU1 hard drive capacity 20GB

(5) The required software includes: the universal server needs to install Quagga; Attacking the server requires installing FRR.

6.4 Virtual Machine Generation and Configuration

When building a network topology, it is necessary to prepare three universal servers and import the same version of CentOS-7-x86_ 64-DVD-1708 mirror image. After starting the server, update the software in the system to the latest version by executing the 'sudo yum y update' command to ensure that the system

is in the latest state.

Next, configure the network connections of these three universal servers to Host-only mode through the virtual platform, which can ensure the authenticity of the experimental environment and ensure the integrity and reliability of the experimental data.

To ensure that the IP addresses of virtual devices in the security testing platform do not change, we have changed the DHCP function of the three universal servers to the Static function, so that the IP addresses remain fixed.

When building a network topology, an additional network card named ens36 needs to be added to the first universal server as the backbone core router. At the same time, we need to enable the IPv4 routing forwarding function to ensure that the two network cards of this router can access each other.

By following the above steps, a network topology with three universal servers can be successfully built and interconnected within the same local area network. This network setup will provide a foundation and guarantee for subsequent experiments and data collection.

Continue to generate a virtual machine with the operating system version number

Debian 10 (64 bit) on the virtual platform, and import the operating system image kali linux-2023.2a installer amd64.iso as the attack machine. Modify the network connection of the Kali attack machine to Host-only mode to ensure the authenticity of the experimental environment and the integrity and reliability of the experimental data. Similarly, change the DHCP function of the Kali attack machine to the Static function. Ensure that the IP address of virtual devices in the security testing platform does not jump.

6.5 Experimental Routing Topology diagram

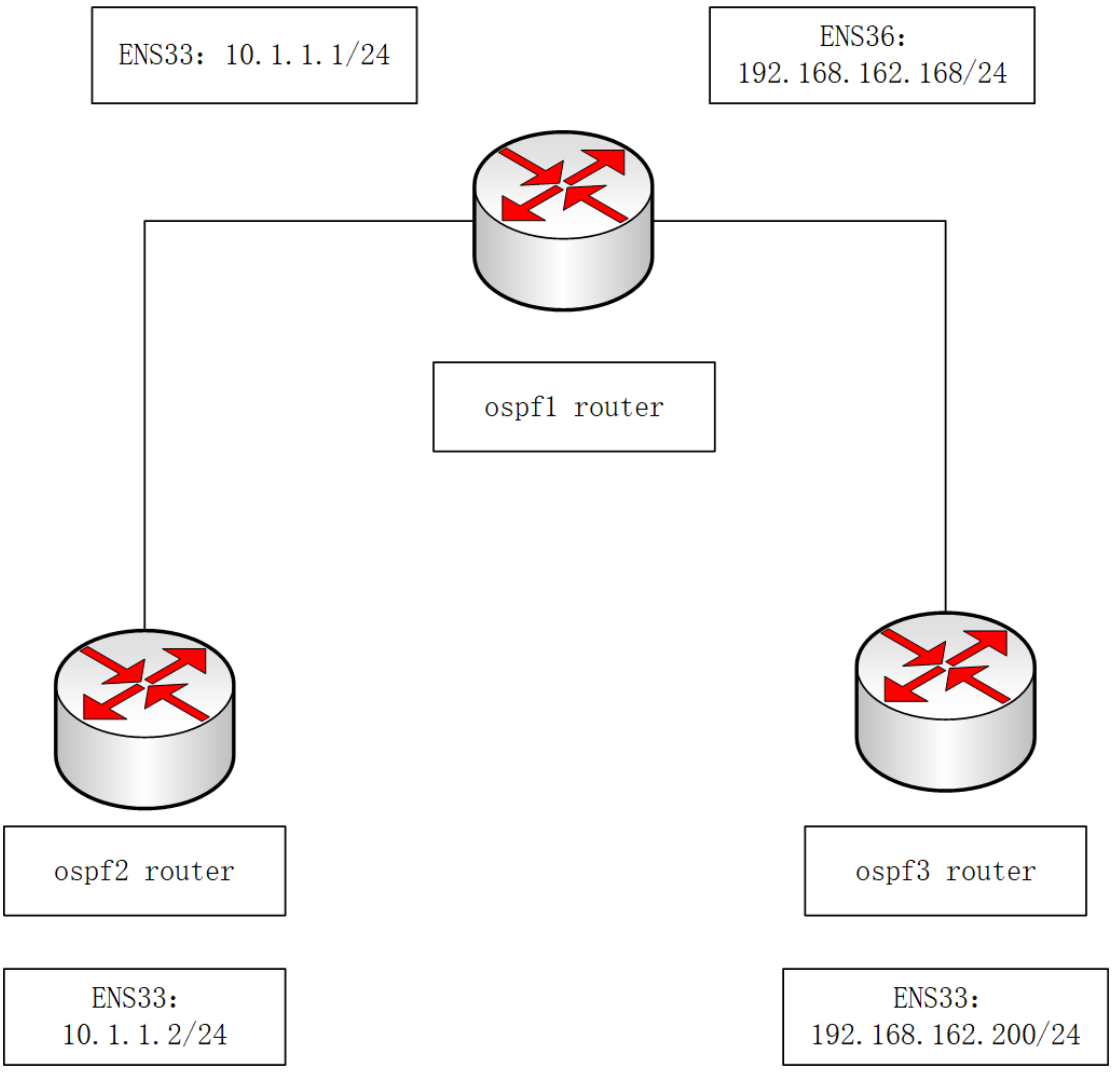


Figure 5: ospf basic topology picture

According to the figure 5, a total of 3 virtualization routers have been deployed on the virtualization platform. They are ospf1 router, ospf2 router, and ospf3 router。 ospf2 router and ospf3 router are edge routers. ospf1 router is the core router. The network card of two edge routers is ENS33 The IP addresses are 10.1.1.2 and 192.168.162.200, respectively. The subnet mask is 24 bits. The core router has a total of 2 network cards, namely ENS33 and ENS36 The IP addresses

are 10.1.1.1 and 192.168.162.168, respectively. The subnet mask is 24 bits.

6.6 Configuration of router protocols

The following content will mainly introduce the software and installation steps required for routers and attacking machines, and provide detailed instructions on how to configure the ospf routing protocol in routers and attacking machines. And how to use Scapy to construct fake ospf hello messages.

6.6.1 software introduction

(1) Quagga is an open-source network routing software suite that focuses on implementing various dynamic routing protocols. The design goal is to provide users with flexible, stable, and functionally rich routing solutions that enable efficient, reliable, and flexible packet forwarding and routing in complex network environments[34].

(2) The Quagga software suite consists of multiple independent network daemons, each responsible for implementing a specific routing protocol. Among them, zebra is the core component of Quagga, responsible for basic routing table management and synchronization of kernel routing information[35].These daemons communicate with each other through sockets to exchange and synchronize routing information, effectively maintaining network topology and routing strategies.

(3) FRR (Free Range Routing) is an open-source network routing software suite designed to implement various dynamic routing protocols[36]. In Linux systems, FRR provides a powerful routing solution that provides flexible, stable, and feature rich routing services for network administrators.

(4) MTR (My TraceRoute) is a network diagnostic tool designed to assist network administrators and users in quickly and accurately locating network faults and performance issues. It integrates ping and traceroute functions, providing more comprehensive and real-time network path and latency information [37].

(5) Scapy is a powerful network packet manipulation tool widely used for network packet sniffing, packet construction, and network protocol analysis[38]. It is written in Python language and can run on operating systems such as Kali Linux.

6.6.2 Software installation

Running Quagga open-source software on three universal servers can configure them as virtual routers.

（1）Download Quagga open-source software. Enter “sudo yum -y install quagga” on three universal servers[39].

（2）After the installation is completed, you need to edit Quagga's configuration

file. The configuration files for Quagga are located in the/etc/quagga/directory, and there are three main files. The important configuration files are daemons and ospfd. conf, and zebra. conf. The daemons file is used to specify which services Quagga runs, the zebra. conf file is used to specify the configuration of the routing table and the ospfd. conf file is used to specify the configuration of OSPF. Use the command "sudo cp/usr/share/doc/quagga 0.99.22.4/zebra. conf. sample/etc/quagga/zebra. Conf". Copy the zebra. conf. sample file from directory/usr/share/doc/quagga 0.99.22.4 to the/etc/quagga/directory and change the file name to zebra.conf[40].

(3) Use command "sudo cp /usr/share/doc/quagga0.99.22.4/ospfd.conf.sample /etc/quagga/ospfd.conf"[41]. Copy the ospfd. conf. sample file from the directory/usr/share/doc/quagga0.99.22.4/to the/etc/quagga/directory and change the file name to ospfd. conf

(4) Start the zebra daemon. Use the command "sudo systemctl start zebra" to start the zebra service and set sudo systemctl to enable zebra to automatically start the service on the next boot[42].

(5) Start the ospfd daemon. Use the command sudo systemctl start ospfd to start the ospfd service, and use the command "sudo systemctl enable ospfd" to automatically start the service on the next boot[43].

(6) After configuration is completed, use “sudo vtysh to start quagga”[44].

6.6.3 Configuration and Installation of Attack Machine Routing Protocol

(1) Download the FRR open-source software from the Kali attack machine and enter the command “sudo apt-get install FRR”[45].

(2) After the download is completed, enter the command “cd/etc/frr to enter” the frr folder. Modify the daemons file to activate the ospfd file[46].

(3) Restart FRR. Use the commands “systemctl restart frr” and “ systemctl enable frr” to restart frr and set the next boot frr software[47].

(4) Automatically enabled.

(5) After the configuration is completed, use "sudo vtysh" to enter the FRR routing configuration interface.

6.6.4 Configure Routing Protocol

(1) Log in to the quagga configuration interface of the universal router using 'sudo vtysh'. Afterwards, also use ‘sudo vtysh’ to log in to the FRR configuration interface of the Kali attack machine[48].

(2) Use commands similar to Cisco routers to configure virtual routers and routing modules for Kali attack machines.

6.6.5 Configuration of platform parameters

To make the research platform close to the real network environment, the research platform needs to test network traffic. MTR is a network performance testing tool. MTR can report bandwidth, latency jitter, and packet loss.

6.7 forged OSPF Hello Message Construction

6.7.1 Attack module generated through Kali attack machine

The attack module sends packet operation instructions to Scapy through a method called the Kali system, which supports common routing protocols such as OSPF, RIP, EIGRP, etc. Scapy encapsulates and forms packets based on the network parameters set by the attack module, and passes the packets into the security testing platform by calling the sendp function. The number and duration of data packets sent, as well as the interval between sending, are programmed by the attack module.

6.7.2 Scapy attack module

Scapy is a Python-based library that primarily includes flexible packet generation and processing, network sniffing, packet injection, packet parsing, traffic control, routing functionality, application protocol testing, and attack and defense. Through Scapy, users can customize and build various types of network data

packets, including IP layer protocols such as TCP and UDP, and flexibly set various fields of the data packet[49]. Finally, Scapy can also be used to test the protocol implementation of network applications and verify whether the application processes various packet types correctly.

Scapy main function call interface

from scapy.all import *	Import all Scapy function modules
load_contrib	Load Protocol Module
sendp	Sending packets
show	Display the structure of the data package

Figure 6: Scapy main function call interface picture

The implementation flowchart of the attack module.

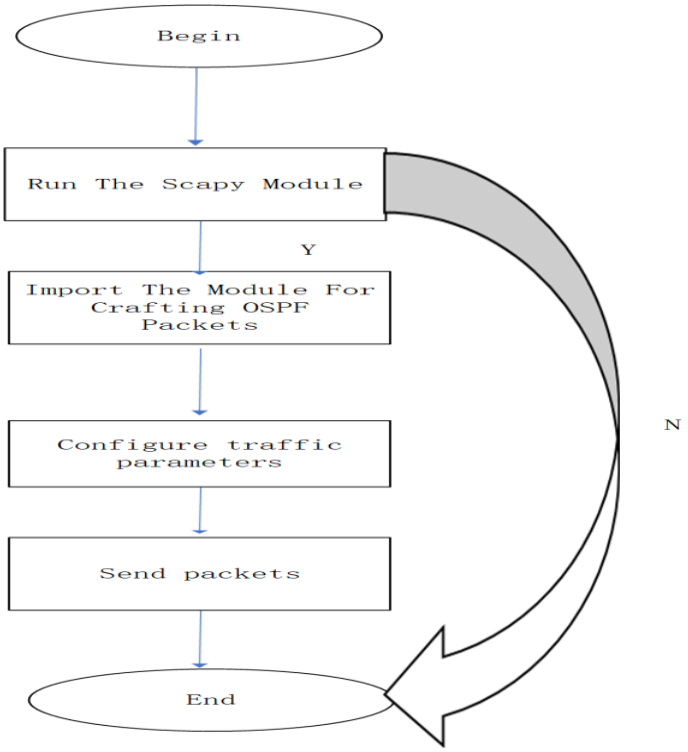


Figure 7: Scapy flowchart of the attack module picture

According to Figures 6 and 7, the attack steps are divided into 6 stages.

Specific steps:

（1）Start the Kali attack machine and open the Scapy module. Enter scapy on the terminal command line of the Kali attack machine.

（2）In the scapy module, enter the command from scapy. all import * to import all scapy function modules.

（3）Select the protocol type and set the key value of the protocol field. The attack module supports the simulation of multiple network protocol traffic through load_ The contrib function references the network protocol module, and here we introduce the OSPF protocol. The method of calling the function is load_ Contrib ("ospf").

（4）Create an OSPF protocol message, and set the function packet to Ether()/IP()/OSPF(). Finally, fill in the fields of the created protocol message.

（5）Set the rate at which data packets are sent. The regular protocol runs at specific time intervals. The Scapy module supports setting the sending time of attack streams. By dynamically passing a time value to the sleep () function and combining it with a while loop statement to control the sending rate

（6）Send data packets. Use the sendp() function in the Scapy module to send an attack stream.

OSPF Security Network Experimental Platform Based on Virtualization Platform

6.7.3 Router Protocol Configuration

Run open-source software Quagga on three virtual servers, configure OSPF routing protocol to make them accessible to each other and test connectivity between virtual servers.

6.7.4Configure quagga routing simulation software

According to the experimental phenomenon in Figure 8, it is shown that execute the command “cp /usr/share/doc/quagga0.99.22.4/zebra.conf.sample /etc/quagga/zebra. conf” on three virtual servers. The purpose of this command is to copy the zebra. conf. sample file of path/usr/share/doc/quagga 0.99.22.4/zebra. conf. sample to/etc/quagga, and change the name of zebra. conf. sample to/zebra. conf.

Enter “systemctl start zebra” to start the zebra service[50].

(2) To ensure that the service must be enabled, we once again use the “chkconfig zebra on” command to ensure that the zebra service is safely enabled[51].

```
[root@localhost ~]# cp /usr/share/doc/quagga-0.99.22.4/zebra.conf.sample /etc/quagga/zebra.conf
cp: overwrite '/etc/quagga/zebra.conf'? yes
[root@localhost ~]# systemctl start zebra
[root@localhost ~]# chkconfig zebra on
```

Figure 8: zebra configuration picture

(3) According to the experimental phenomenon in Figure 9, it is shown that execute commands on three virtual servers: "cp/usr/share/doc/quagga 0.99.22.4/ospfd.conf.sample /etc/quagga/ospf. conf". The purpose of this command is to copy the ospfd. conf. sample file from path/usr/share/doc/quagga 0.99.22.4/ospfd. conf. sample to/etc/quagga, and change the name of ospfd. conf. sample to ospfd. conf.

Enter "systemctl start ospfd" to start the ospfd service[52].

(5) To ensure that the service must be enabled, we once again use the "chkconfig ospfd on" command to ensure that the zebra service is safely enabled[53].

```
[root@localhost ~]# cp /usr//share/doc/quagga-0.99.22.4/ospfd.conf.sample  /etc/quagga/ospfd.conf
[root@localhost ~]# systemctl start ospfd
[root@localhost ~]# chkconfig ospfd on
```

Figure 9: ospfd configuration picture

(6) Start the quagga routing simulation software and configure the file directory for storing logs

(7) According to the experimental phenomenon in Figure 10, it is shown that

start quagga routing simulation software using the command vtysh.

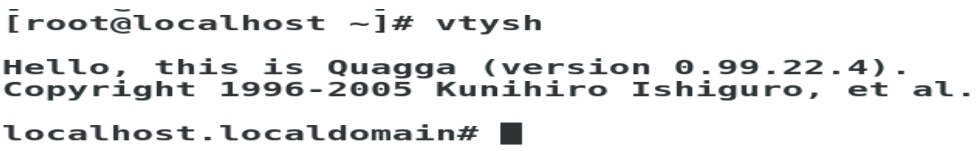


Figure 10: vtysh configuration picture

（8）According to the experimental phenomenon in Figure 11, it is shown that enter configure terminal to enter the global configuration mode of vtysh.

Figure 11: vtysh global configuration picture

(9) According to the experimental phenomenon in Figure 12, it is shown that enter log file/var/log/quagga/quagga. log to specify the location of the log file, and then exit mode。

Figure 12: log configuration picture

（10）According to the experimental phenomenon in Figure 13, it is shown that enter the write command to permanently save the configuration。

Figure 13: configuration save picture

6.8 Summary of this chapter

The purpose of this chapter is to establish the foundational framework for an in-depth exploration of attacks and defenses within the OSPF routing protocol. Employing a methodology that involves leveraging virtualization technology to design an experimental platform, Specifically, this chapter mainly contributes to the following key aspects:

1. Establishment of Virtualization Testing Platform.

2.Software Installation and Configuration.

3. Construction of Deceptive OSPF Data Packets.

With the successful establishment of the virtualization testing platform and the adept configuration of routing software, we are well-prepared for the ensuing chapters.

Chapter 7

Simulation Experiment of OSPF Network Attack Based on Virtualization Platform

7.1 OSPF network environment construction

According to the experimental topology scenario designed and built on the virtualization testing platform in Chapter 6. There are a total of three virtual routers in the experimental topology, namely ospf1 router, ospf2 router, ospf3 router, and kali attack machine. There are a total of two network segments, namely the 10.1.1.0 network segment and the 192.168.162.200 network segment. Firstly, all network devices are located within the same autonomous system, and a local area network is designed. It can more directly observe the phenomenon of ospf network being attacked. Generate a Kali Linux system host in a virtualization platform to simulate the attacker's host. Secondly. The attack module containing Scapy in the attack machine generated through the virtualization platform supports the generation and sending of forged ospf packets. Support functions such as timed sending and interval sending, as this method does not require the installation of other virtual machines or operating systems, saving hardware and CPU resources, and also has the ability to easily send fake ospf data packets.

7.1.1 OSPF basic network construction process

In the global configuration, use the hostname command to modify the default name of the three virtual routers, Respectively is ospf1, ospf2, ospf3。Changing the default names of the three virtual routers is to better distinguish between virtual routers. Let readers distinguish as soon as possible. Figure14, Figure15 and Figure16 are the results of changes made to three routers installed on a virtualization platform.

```
localhost.localdomain(config)# hostname ospf1
```

Figure 14: configuration hostname ospf1 picture

```
localhost.localdomain(config)# hostname  ospf2
```

Figure 15: configuration hostname ospf2 picture

```
localhost.localdomain(config)# hostname  ospf3
```

Figure 16: configuration hostname ospf3 picture

7.1.2 Configure the IP addresses and subnet masks separately.

(1) The IP address of the ens33 interface in the ospf1 router is 10.1.1.1. The IP address of the ENS36 interface is 192.168.162.128. The subnet masks are all 255.255.255.0. Use the IP address command to configure the above IP address and subnet mask. Check if the configuration is complete through the show

interface command[54]. Checking the IP address of an interface is crucial. This step is to prevent network congestion caused by DHCP jumps within the system. Reasonable configuration of IP addresses is the first step for the normal operation of OSPF protocol. Figure 17 checks the interface address of the ospf1 virtual router.

```
ospf1# show interface
Interface ens33 is up, line protocol detection is disabled
  index 2 metric 1 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:0c:29:f2:a6:7e
  inet 10.1.1.1/24 broadcast 10.1.1.255
  inet6 fe80::20c:29ff:fef2:a67e/64
Interface ens36 is up, line protocol detection is disabled
  index 5 metric 1 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:0c:29:f2:a6:88
  inet 192.168.162.128/24 broadcast 192.168.162.255
  inet6 fe80::2966:4d6a:100b:5dfe/64
```

Figure 17: show ospf1 interfaces picture

(2) The IP address of the ens33 interface in the ospf2 router is 10.1.1.2, and the subnet mask is 255.255.255.0. Use the show interface command to check if the configuration is complete. Figure 18 checks the interface address of the ospf2 virtual router.

```
ospf2# show interface
Interface ens33 is up, line protocol detection is disabled
  index 2 metric 1 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:0c:29:d5:94:a6
  inet 10.1.1.2/24 broadcast 10.1.1.255
  inet6 fe80::20c:29ff:fed5:94a6/64
```

Figure 18: show ospf2 interfaces picture

(3) The IP address of the ens33 interface in the ospf3 router is 192.168.162.200, and the subnet mask is 255.255.255.0. Use the show interface command to check if the configuration is complete. Figure 19 is to check the interface address of the

ospf3 virtual router.

```
ospf3# show interface
Interface ens33 is up, line protocol detection is disabled
  index 2 metric 1 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:0c:29:6a:10:30
  inet 192.168.162.200/24 broadcast 192.168.162.255
  inet6 fe80::20c:29ff:fe6a:1030/64
```

Figure 19: show ospf3 interfaces picture

7.2 Configure OSPF protocol in three virtual routers separately

Explanation of experimental steps. Firstly, start the ospf protocol process in different ospf routers. Secondly, configure 'router id' to identify the device used as a dedicated device for OSPF routers. Finally, the network segments with different interface configurations are notified to the planned area through network commands.

(1) In the ospf1 router, first enter the command router ospf to create the ospf process. Secondly, configure the router id to 1.1.1.1 to identify this virtual router, and finally use the network command to announce the network segment it is on.

```
router ospf
 ospf router-id 1.1.1.1
 network 10.1.1.0/24 area 0.0.0.0
 network 192.168.162.0/24 area 0.0.0.0
!
```

Figure 20: router1 ospf configuration picture

Explanation of Figure 20 configuration commands:

Start OSPF protocol process

router ospf

Set the router id 1.1.1.1 running this OSPF protocol router

ospf router-id 1.1.1.1

Publish 10.1.1.0/24 network segments to OSPF network backbone area 0

network 10.1.1.0/24 area 0.0.0.0

Publish 192.168.162.0/2 network segment to OSPF network backbone area 0

network 192.168.162.0/24 area 0.0.0.0

（2）In the ospf2 router, first enter the command router ospf to create the ospf process. Secondly, configure the router id to 2.2.2.2 to identify this virtual router, and finally use the network command to announce the network segment it is on.

```
router ospf
 ospf router-id 2.2.2.2
 network 10.1.1.0/24 area 0.0.0.0
```

Figure 21: router2 ospf configuration picture

Explanation of Figure 21 configuration commands:

Start OSPF protocol process

router ospf

Set the router id running this OSPF protocol router to 2.2.2.2

ospf router-id 2.2.2.2

Publish 10.1.1.0/24 network segments to OSPF network backbone area 0

network 10.1.1.0/24 area 0.0.0.0

（3）In the ospf3 router, first enter the command router ospf to create the ospf process. Secondly, configure the router id to 3.3.3.3 to identify this virtual router, and finally use the network command to announce the network segment it is on.

```
router ospf
 ospf router-id 3.3.3.3
 network 192.168.162.0/24 area 0.0.0.0
!
```

Figure 22: router3 ospf configuration picture

Explanation of Figure 22 configuration commands:

Start OSPF protocol process

router ospf

Set the router id for running this OSPF protocol router to 3.3.3.3

ospf router-id 3.3.3.3

Publish 192.168.162.0/24 network segment to OSPF network backbone area 0

network 192.168.162.0/24 area 0.0.0.0

7.3 experimental result

Testing router connectivity through ping command

（1）ospf2 router accessing ospf3 router using ping command[55]. According to Figure 23, the ospf2 router can successfully access the ospf3 router.

Figure 23: ospf2 accessing test picture

（2）ospf3 router accessing ospf2 router using ping command. According to Figure 24, the ospf3 router can successfully access the ospf2 router.

```
ospf3# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
64 bytes from 10.1.1.2: icmp_seq=1 ttl=63 time=0.967 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=63 time=0.775 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=63 time=0.741 ms
64 bytes from 10.1.1.2: icmp_seq=4 ttl=63 time=1.10 ms
64 bytes from 10.1.1.2: icmp_seq=5 ttl=63 time=0.676 ms
64 bytes from 10.1.1.2: icmp_seq=6 ttl=63 time=0.634 ms
64 bytes from 10.1.1.2: icmp_seq=7 ttl=63 time=0.835 ms
64 bytes from 10.1.1.2: icmp_seq=8 ttl=63 time=0.743 ms
64 bytes from 10.1.1.2: icmp_seq=9 ttl=63 time=0.874 ms
64 bytes from 10.1.1.2: icmp_seq=10 ttl=63 time=0.609 ms
```

Figure 24: ospf3 accessing test picture

7.4 View the neighbor status and link status databases and the resulting route

View ospf1 Router experiment results:

（1） According to Figure 25， ospf1 router: Use “show ip ospf neighbor” command to check the neighbor status [56], and it is determined that ospf1 router has formed a stable neighbor status with the ospf2 router and ospf3 router.

```
ospf1# show ip ospf  neighbor

    Neighbor ID Pri State          Dead Time Address         Interface            RXmtL RqstL DBsmL
2.2.2.2           1 Full/DR          30.420s 10.1.1.2        ens33:10.1.1.1           0     0     0
3.3.3.3_          1 Full/DR          34.278s 192.168.162.200 ens36:192.168.162.128     0     0     0
```

Figure 25: show ospf neighbor picture

（2） According to Figure 26， ospf1 router Use the command “show ip ospf database” to inspect the link state database and verify that the link state database of the ospf1 router has learnt the link state notification information of the other two routers.

```
ospf1# show ip ospf  database

       OSPF Router with ID (1.1.1.1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1          13 0x80000015 0xa2f5 2
2.2.2.2         2.2.2.2         190 0x8000000a 0xd440 1
3.3.3.3         3.3.3.3         345 0x8000000a 0x017e 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.1.1.2        2.2.2.2         330 0x80000008 0x1021
192.168.162.200 3.3.3.3         195 0x80000008 0x4b17
```

Figure 26: show ospf database picture

（3） According to Figure 27， ospf1 router: Use the show IP ospf router to view

the routes and determine that ospf1 router has learned the routing information for ospf2 router and ospf3 router.

```
ospf1# show ip ospf  route
============ OSPF network routing table ============
N    10.1.1.0/24           [10] area: 0.0.0.0
                           directly attached to ens33
N    192.168.162.0/24      [10] area: 0.0.0.0
                           directly attached to ens36

============ OSPF router routing table =============

============ OSPF external routing table ===========
```

Figure 27: show ospf routing picture

View ospf2 Router experiment results:

（1）According to Figure 28，ospf2 router: Use Show IP ospf neighbor to check the status of neighbors and determine that the ospf2 router has formed a stable neighbor state with the ospf1 router.

```
ospf2# show ip ospf  neighbor

   Neighbor ID Pri State          Dead Time Address         Interface           RXmtL RqstL DBsmL
1.1.1.1_         1 Full/Backup       34.434s 10.1.1.1        ens33:10.1.1.2          0     0     0
```

Figure 28: show ospf neighbor picture

（2）According to Figure 29, ospf2 router: Use the show IP ospf database to view the link state database and obtain that the link state database of the ospf2 router has learned the link state notification information of the other two routers.

```
ospf2# show ip ospf  database

       OSPF Router with ID (2.2.2.2)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1          478 0x80000015 0xa2f5 2
2.2.2.2         2.2.2.2          652 0x8000000a 0xd440 1
3.3.3.3         3.3.3.3          809 0x8000000a 0x017e 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.1.1.2        2.2.2.2          792 0x80000008 0x1021
192.168.162.200 3.3.3.3          659 0x80000008 0x4b17
```

Figure 29: show ospf database picture

（3）According to Figure 30, ospf2 router: Use the show IP ospf router to view the routes and determine that ospf1 router has learned the routing information for ospf2 router and ospf3 router.

```
ospf2# show ip ospf  route
============ OSPF network routing table ============
N    10.1.1.0/24           [10] area: 0.0.0.0
                           directly attached to ens33
N    192.168.162.0/24      [20] area: 0.0.0.0
                           via 10.1.1.1, ens33

============ OSPF router routing table =============

============ OSPF external routing table ===========
```

Figure 30: show ospf routing picture

View ospf3 Router experiment results:

（1）According to Figure 31, ospf3 router: Use Show IP OSPF neighbor to check the status of neighbors and determine that the OSPF3 router has formed a stable neighbor state with the OSPF1 router.

```
ospf3# show ip ospf neighbor

    Neighbor ID Pri State          Dead Time Address         Interface            RXmtL RqstL DBsmL
1.1.1.1           1 Full/Backup       35.409s 192.168.162.128 ens33:192.168.162.200     0     0     0
```

Figure 31: show ospf neighbor picture

(2) According to Figure 32, ospf3 router: Use the "show ip ospf database" to view the link status database and obtain that the link status database of the ospf3 router has learned the link status notification information of the other two routers.

```
ospf3# show ip ospf  database

       OSPF Router with ID (3.3.3.3)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1          296 0x80000014 0xa4f4 2
2.2.2.2         2.2.2.2          542 0x80000009 0xd63f 1
3.3.3.3         3.3.3.3          635 0x80000009 0x037d 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.1.1.2        2.2.2.2          662 0x80000007 0x1220
192.168.162.200 3.3.3.3          515 0x80000007 0x4d16
```

Figure 32: show ospf database picture

(3) According to Figure 33, ospf3 router: Use the "show ip ospf router" to view the route and determine that the ospf3 router has learned the routing information of the ospf2 router.

```
ospf3# show ip ospf  route
============ OSPF network routing table ============
N    10.1.1.0/24           [20] area: 0.0.0.0
                           via 192.168.162.128, ens33
N    192.168.162.0/24      [10] area: 0.0.0.0
                           directly attached to ens33

============ OSPF router routing table =============

============ OSPF external routing table ===========
```

Figure 33: show ospf routing picture

Summary: Three routers can access each other. The OSPF2 router and OSPF3 router can form stable neighbor relationships with the OSPF1 router. The link status database information of the three routers is synchronized and consistent. All three routers can learn the routing information of the other party.

7.5 Attack machine selection

(1) Select Debian as the basic system and install Kali image about kali-linux-2023.2a-installer-amd64.iso

(2) Use the ifconfig command to check the attacker's IP address[57]. The experimental results in Figure 34 show that the IP address of the eth0 interface is 192.168.162.129 Checking the IP address of the attacker's host prevents DHCP protocol sending jumps in the virtual testing platform, ensuring the accuracy and integrity of data traffic.

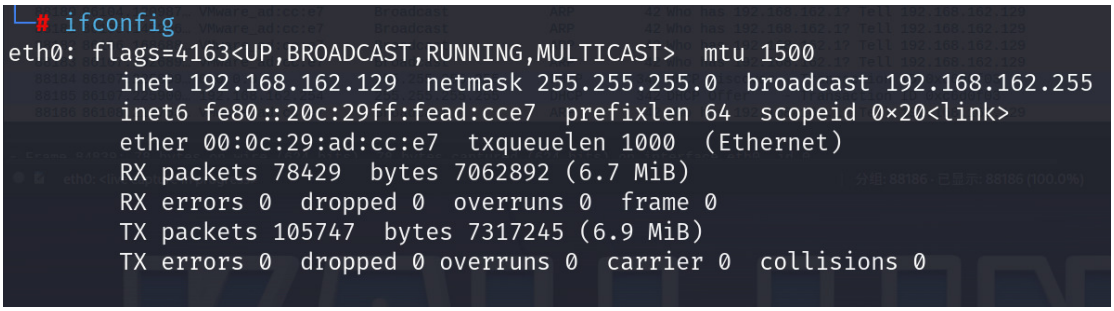


Figure 34: show kali attacker's interface address picture

(3) Use the Nmap tool to scan the surviving routers or hosts on the same LAN [58]. Nmap（Network Mapper）It is a tool used for network detection and security scanning, which can scan specified IP address ranges, as well as port and service

information of specific hosts. The advantage of Nmap scanning IP addresses is that it can provide detailed information about network topology, port status, service information, and security. Figure 35 Experimental results show that found that besides myself, 2 target hosts are surviving. The IP addresses are 192.168.162.128 and 192.168.162.200 respectively.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.162.1-254
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-05 16:39 CST
Nmap scan report for 192.168.162.128
Host is up (0.00078s latency).
Nmap scan report for 192.168.162.129
Host is up (0.000095s latency).
Nmap scan report for 192.168.162.200
Host is up (0.0031s latency).
Nmap done: 254 IP addresses (3 hosts up) scanned in 19.90 seconds
```

Figure 35: Scan survival address picture

(4) Use "Ping" command to check the connectivity between the IP addresses 192.168.162.128 and 192.168.162.200. The experimental results of Figure 36 and Figure 37 show that the attacker can successfully access the surviving IP address.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.162.128
PING 192.168.162.128 (192.168.162.128) 56(84) bytes of data.
64 bytes from 192.168.162.128: icmp_seq=1 ttl=64 time=0.394 ms
64 bytes from 192.168.162.128: icmp_seq=2 ttl=64 time=0.327 ms
64 bytes from 192.168.162.128: icmp_seq=3 ttl=64 time=0.315 ms
64 bytes from 192.168.162.128: icmp_seq=4 ttl=64 time=0.357 ms
^C
── 192.168.162.128 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3036ms
rtt min/avg/max/mdev = 0.315/0.348/0.394/0.030 ms
```

Indicates that the attacker is in the same network segment as one of the routers.

Figure 36: ping survival address picture

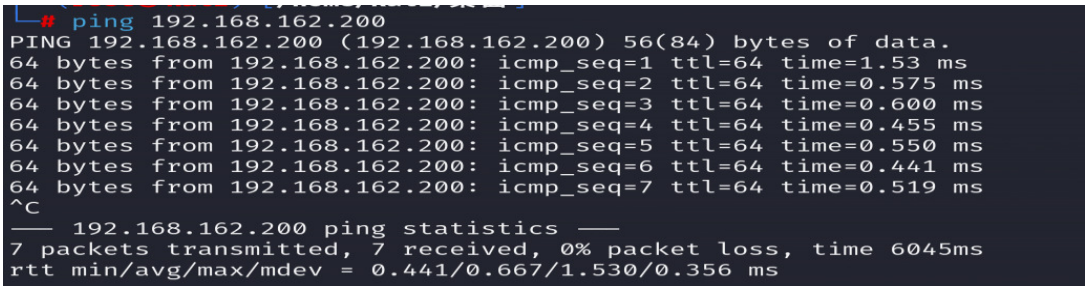
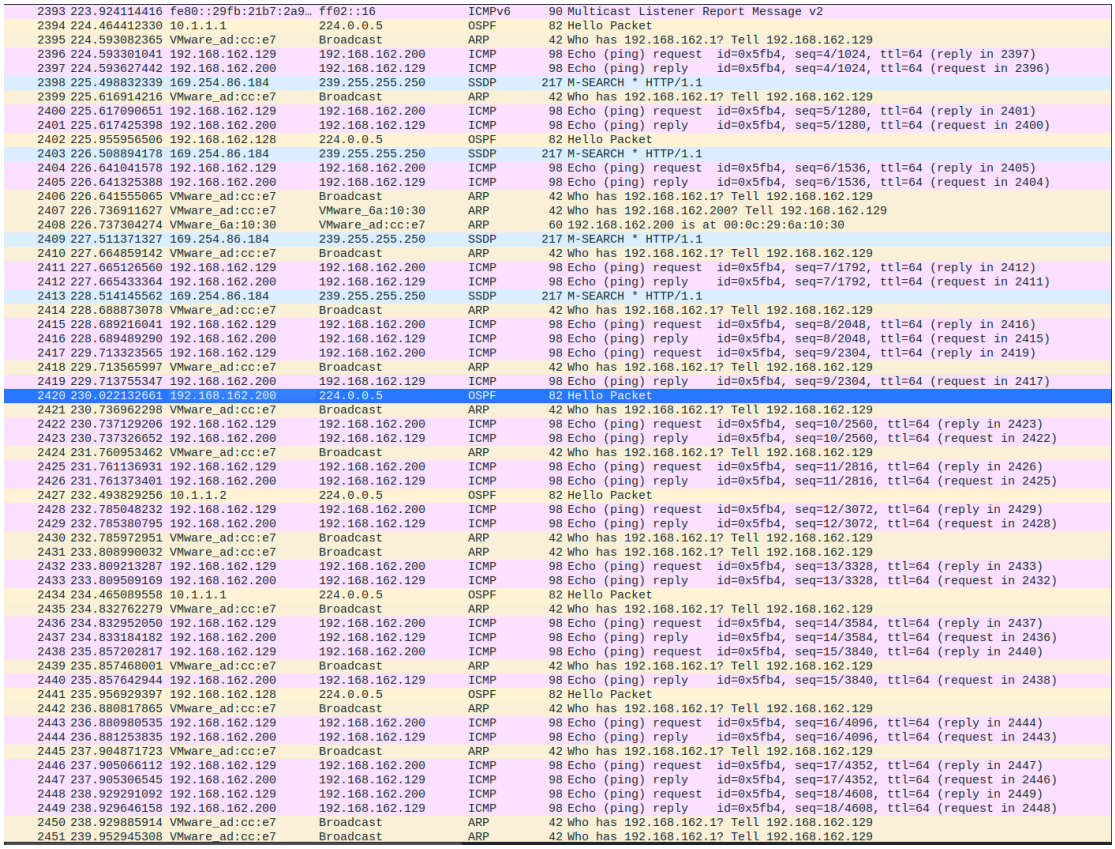


Figure 37: ping survival address picture

(1) View specific packet information through Wireshark software [59]. We obtained the Kali attack machine and the interaction with the target machine of 192.168.162.200 that generated ICMP protocol packets[60]

(2) In addition, based on the analysis of experimental data obtained from Figure 38 a large number of OSPF packets interacting with the target machine. So, it is generally believed that the target machine is a router.



2393	223.924114416	fe80::29fb:21b7:2a9…	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
2394	224.464412330	10.1.1.1	224.0.0.5	OSPF	82 Hello Packet
2395	224.593082365	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2396	224.593301041	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=4/1024, ttl=64 (reply in 2397)
2397	224.593627442	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=4/1024, ttl=64 (request in 2396)
2398	225.498832339	169.254.86.184	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
2399	225.616914216	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2400	225.617090651	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=5/1280, ttl=64 (reply in 2401)
2401	225.617425398	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=5/1280, ttl=64 (request in 2400)
2402	225.955956506	192.168.162.128	224.0.0.5	OSPF	82 Hello Packet
2403	226.508894178	169.254.86.184	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
2404	226.641041578	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=6/1536, ttl=64 (reply in 2405)
2405	226.641325388	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=6/1536, ttl=64 (request in 2404)
2406	226.641555065	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2407	226.736911627	VMware_ad:cc:e7	VMware_6a:10:30	ARP	42 Who has 192.168.162.200? Tell 192.168.162.129
2408	226.737304274	VMware_6a:10:30	VMware_ad:cc:e7	ARP	60 192.168.162.200 is at 00:0c:29:6a:10:30
2409	227.511371327	169.254.86.184	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
2410	227.664859142	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2411	227.665126560	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=7/1792, ttl=64 (reply in 2412)
2412	227.665433364	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=7/1792, ttl=64 (request in 2411)
2413	228.514145562	169.254.86.184	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
2414	228.688873078	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2415	228.689216041	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=8/2048, ttl=64 (reply in 2416)
2416	228.689489290	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=8/2048, ttl=64 (request in 2415)
2417	229.713323565	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=9/2304, ttl=64 (reply in 2419)
2418	229.713565997	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2419	229.713755347	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=9/2304, ttl=64 (request in 2417)
2420	230.022132661	192.168.162.200	224.0.0.5	OSPF	82 Hello Packet
2421	230.736962298	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2422	230.737129206	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=10/2560, ttl=64 (reply in 2423)
2423	230.737326652	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=10/2560, ttl=64 (request in 2422)
2424	231.760953462	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2425	231.761136931	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=11/2816, ttl=64 (reply in 2426)
2426	231.761373401	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=11/2816, ttl=64 (request in 2425)
2427	232.493829256	10.1.1.2	224.0.0.5	OSPF	82 Hello Packet
2428	232.785048232	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=12/3072, ttl=64 (reply in 2429)
2429	232.785380795	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=12/3072, ttl=64 (request in 2428)
2430	232.785972951	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2431	233.808990032	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2432	233.809213287	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=13/3328, ttl=64 (reply in 2433)
2433	233.809509169	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=13/3328, ttl=64 (request in 2432)
2434	234.465089558	10.1.1.1	224.0.0.5	OSPF	82 Hello Packet
2435	234.832762279	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2436	234.832952050	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=14/3584, ttl=64 (reply in 2437)
2437	234.833184182	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=14/3584, ttl=64 (request in 2436)
2438	235.857202817	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=15/3840, ttl=64 (reply in 2440)
2439	235.857468001	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2440	235.857642944	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=15/3840, ttl=64 (request in 2438)
2441	235.956929397	192.168.162.128	224.0.0.5	OSPF	82 Hello Packet
2442	236.880817865	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2443	236.880980535	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=16/4096, ttl=64 (reply in 2444)
2444	236.881253835	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=16/4096, ttl=64 (request in 2443)
2445	237.904871723	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2446	237.905066112	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=17/4352, ttl=64 (reply in 2447)
2447	237.905306545	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=17/4352, ttl=64 (request in 2446)
2448	238.929291092	192.168.162.129	192.168.162.200	ICMP	98 Echo (ping) request id=0x5fb4, seq=18/4608, ttl=64 (reply in 2449)
2449	238.929646158	192.168.162.200	192.168.162.129	ICMP	98 Echo (ping) reply id=0x5fb4, seq=18/4608, ttl=64 (request in 2448)
2450	238.929885914	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129
2451	239.952945308	VMware_ad:cc:e7	Broadcast	ARP	42 Who has 192.168.162.1? Tell 192.168.162.129

Figure 38: Show ICMP and OSPF data packet picture

(3) Falsifying false data packets requires obtaining the structure of the actual data packet that has already been obtained. An IP packet typically has a data link layer encapsulation protocol. IP layer encapsulation protocol, including protocol type, packet size, etc. According to the experimental data obtained from Figure 39 looking at the IP data packet with a real IP address of 192.168.162.200, we obtained that the source MAC address of this packet is 00:0c: 29:6a: 10:30, and the destination MAC address is 01:00:5e: 00:00:05. The OSPF header contains the source ospf Router ID of 3.3.3.3 and the IP address of the Designed Router of 192.168.162.200 The IP address of the Backup Designed Router is 192.168.162.128 and other basic information. With this basic information, we can

further forge it.

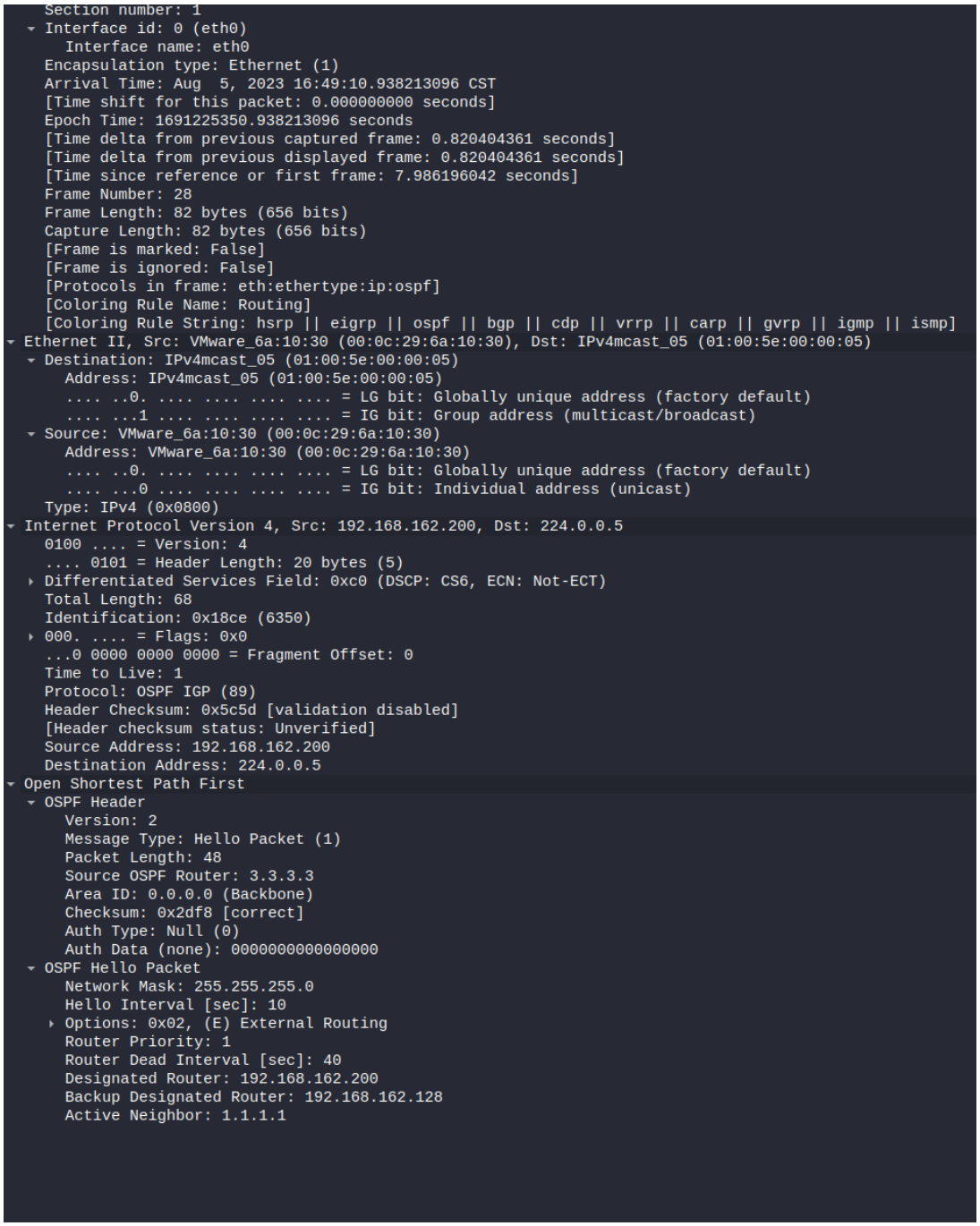


Figure 39: Show OSPF data packet message picture

(4) OSPF Router Spoofing Message Construction

To study the attacks and prevention of OSPF routing spoofing, firstly, we need to

construct the attack source, construct OSPF routing spoofing packets, and send them to the virtual research platform. Then, we can further study their attack characteristics and propose defense methods, which is the fundamental condition of this paper's research.

Due to the relatively complex nature of the OSPF protocol, both message types and data formats are very diverse, which poses a huge challenge to constructing data packets. But Scapy perfectly solves this problem.

```
>>> from scapy.all import *
>>> load_contrib("ospf")
>>> ethe = Ether(dst="01:00:5e:00:00:05",src="00:0c:29:f2:a6:88")
>>> packet = ethe/IP(src='192.168.162.128',dst='224.0.0.5',proto="ospf")
>>> packet = packet/OSPF_Hdr()
>>> packet = packet/OSPF_Hello(router='192.168.162.200',backup='192.168.162.128',neighbors='3.3.3.3')
>>> num_packets = 1000
>>> success_count = 0
>>> for i in range(num_packets):
...     try:
...         sendp(packet,iface='eth0',verbose=False)
...         success_count +=1
...     except:
...         pass
... print(f"successfully sent { success_count } data packets")

successfully sent 1000 data packets
>>>
>>>
```

Figure 40: Show Scapy code picture

Experimental attack code based on Figure 40 to forge 192.168.162.128, firstly in the Scapy software, enter from Scapy. all import * to import all modules of Scapy.

Secondly, enter load_ Contrib ("ospf") loads the functional module of OSPF.

Thirdly, enter ether (dst="01:00:5e:00:00:05", src="00:0c: 29: f2: a6:88"). The meaning of this command is to define the MAC address of a data link layer. To the destination of "01:00:5e:00:00:05", the forged MAC address is "00:0c: 29: f2: a6:88".

Fourthly, the meaning of the instruction 'packet=the/IP' (src='192.168.162.200 ', dst='224.0.0.5', proto="ospf") is to forge a network layer data packet, with the forged source IP address being 192.168.162.200 and going to the OSPF multicast address with IP address 224.0.5, using the OSPF protocol as the encapsulation.

Fifth, Packet=packet/OSPF_ The meaning of the Hdr() instruction is to add the encapsulation format of the OSPF head to the outer layer of the defined packet data package.

Sixth, packet=packet/OSPF The meaning of this command, Hello (router='172.168.162.200 ', backup='172.168.162.128', neighbors='3.3.3.3 '), is to continue forging the Hello message of OSPF based on the previous forgery. Router='172.168.162.200' indicates that the IP address of the forged DR router is 172.168.162.200, backup='172.168.162.128' indicates that the forged BDR router, neighbors='172.168.162.130' indicates that the forged neighbor IP address is 3.3.3.3

Seventh, the setting requires sending 1000 data packets.

Eighth, use the for-loop function to output the execution result on the screen.

(5) Through Wireshark packet capture, we have successfully sent a forged packet to the multicast address 224.0.0.5 of OSPF.

According to the experimental data analysis obtained from Figure 41, it is concluded that a large number of fake OSPF packets have been sent to the multicast addresses monitored by the OSPF protocol, achieving the experimental goal of OSPF DOS attack.

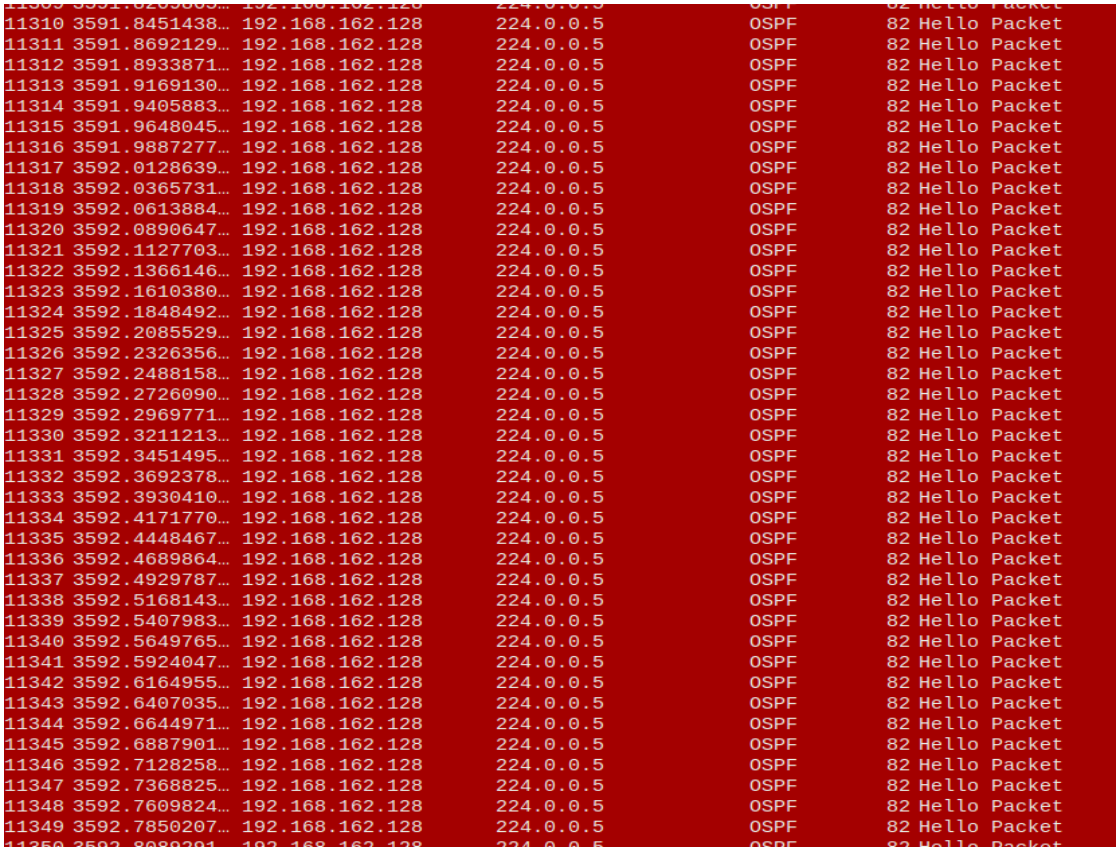


Figure 41: Show inject fake ospf data packet picture

Analysis of experimental results:

According to the experimental results in Figures42 and Figure43, the specific structure of the fake OSPF packet is consistent with the OSPF packet with a real address of 192.168.162.200. According to Figure41 and Figure42, the structure of fake data packets is obtained. The encapsulation from the data link layer to the IP layer, as well as the encapsulation of OSPF protocol packets and OSPF Hello packets in the IP layer, is consistent with the structure of real OSPF data packets. The protocol configuration parameters of fake OSPF packets, such as Hello time, death time, OSPF region type, etc., are consistent with the real OSPF packet. Through experimental results, it is found that false OSPF packets behave similarly to real packets in the network, which may deceive network devices. Attackers can generate fake OSPF packets by forging these parameters for OSPF Hello Flooding attacks, resulting in network latency and delayed packet arrival.

Through experimental results, it has been proven that false OSPF packets can successfully disguise themselves as real packets, with structures and protocol parameters similar to real packets. This experimental phenomenon illustrates an important issue in network security, where attackers can deceive network devices by forging protocol packets, posing a threat to the stability and reliability of the network.

Figure 42: using scapy module to show ospf data packet construction picture

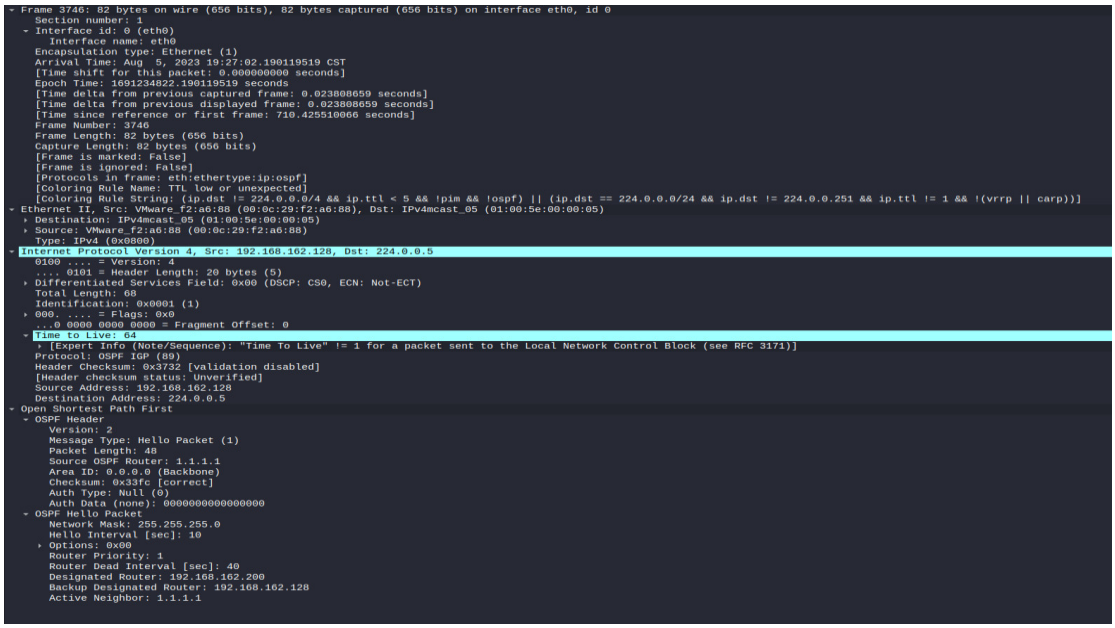


Figure 43: show ospf data packet specific construction picture

（6）Test the load status of the network:

MTR can be used to some extent to test the load status of a network, especially for intermediate routers and hosts in the network. Due to the continuous transmission of data packets and real-time display of response time by MTR, the response delay of each router on the network path can be observed to understand the network load status. In the output of MTR, Snt, Last, Avg, Best, Worst, and StDev are statistical information about network connection performance. These statistics represent the situation of sending packets and receiving responses.

The meaning of parameter representation:

1.Snt (Sent): Indicates the number of data packets sent, that is, the number of times the data packets were sent.

2.Last: Indicates the round-trip time (RTT) of the last packet. It indicates the round-trip time of the most recent packet, in milliseconds.

3.Avg (Average): represents the average round-trip time of all data packets. It is the arithmetic mean of all packet RTTs.

4.Best: represents the minimum round-trip time of all data packets. It is the

shortest time among all packet RTTs.

5.Wrst (Worst): represents the maximum round-trip time of all data packets. It is the longest time among all packet RTTs.

6.StDev (Standard Deviation): represents the standard deviation of round-trip time for all data packets. It is a measure of the degree of variation of all packet RTTs.

（7） Before testing:

According to Figure 44 The experimental results show that the IP address 10.1.1.1 belongs to the 10.1.1.0 network segment of the OSPF protocol area 0. 318 packets have been sent, and the round-trip time for the last packet is 0.4 milliseconds. The average value is 0.9. The minimum round-trip time for data packets is 0.3, while The IP address 192.168.162.200 belongs to the 192.168.162.0 network segment of the OSPF protocol area 0 region. 317 packets have been sent, and the round-trip time for the last packet is 0.8 milliseconds. The average value is 0.9. The minimum round-trip size for data packets is 0.4

Figure 44: Before data traffic testing picture

(8) After testing:

According to Figure 45 the experimental results show that the IP address 10.1.1.1 belongs to the 10.1.1.0 network segment of the OSPF protocol area 0 region. 426 packets have been sent, and the round-trip time for the last packet is 0.4 milliseconds. The average value is 0.8. The minimum round-trip time for data packets is 0.3, while The IP address 192.168.162.200 belongs to the 192.168.162.0 network segment of the OSPF protocol area 0 region. 426 packets have been sent, and the round-trip time for the last packet is 0.7 milliseconds. The average value is 0.9. The minimum round-trip size for data packets is 0.4

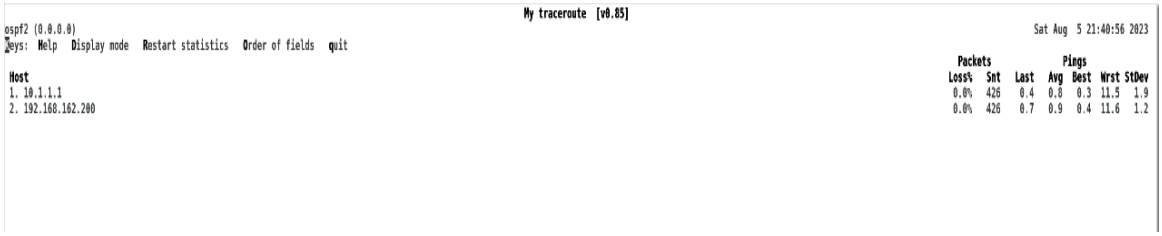


Figure 45: After data traffic testing picture

(9) Analysis of test results:

The Kali attack machine forged the source address 192.168.162.200 and sent 1000 fake OSPF Hello packets. During the transmission of these 1000 packets, the average load of the 192.168.162.0 network segment in the OSPF protocol was higher than that of the 10.1.1.0 network segment, with an average load value higher than 0.1. The conclusion is that the fake OSPF Hello data packets forged

by the Kali attacker successfully consumed link bandwidth and reduced the quality of the network.

(10) The attacker simulates a fake OSPF router. Install the attack machine with routing general software to simulate a fake OSPF router, with the aim of stealing routing information from the target router by connecting to the target OSPF network through configuring the OSPF protocol on the attack machine. Use the command “sudo apt-get install FRR” on the Kali attack machine to download FRR software FRR (Free Range Routing) an open-source routing software suite designed to provide advanced network routing functionality and support for various routing protocols for UNIX operating systems.

(11) The detailed process of configuring the OSPF protocol of the attacker is achieved by combining illegal default route injection to steal route information to the target router. Enter the vtysh command to enter the global configuration interface of FRR, and enter configure terminal to enter the terminal configuration interface. Firstly, configure the IP address of the eth0 interface to 192.168.162.129 with a mask of 24 and use no shutdown

Open the interface and exit. Secondly, use the command route ospf to start the process of the OSPF protocol. Finally, use the network command to declare a default route of 0.0.0.0/0 and exit.

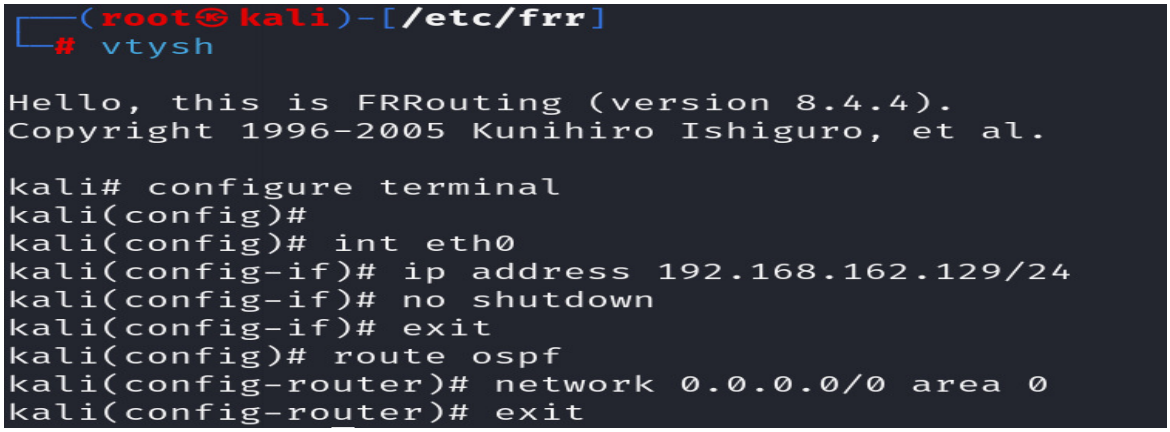


Figure 46: Show attacking machine's ospf configuration picture

Explanation of figure 46 experimental configuration parameters:

Enter eth0 interface

Int eth0

Configure IP address of the eth0 interface to 192.168.162.129 and the subnet

mask to 24

ip address 192.168.162.129/24

Start OSPF protocol process

router ospf

Publish a default route to OSPF network backbone area 0

network 0.0.0.0 area 0

Configuration completed, exit

Exit

(12) Figure 47 experimental results show that in the Kali attack machine, to though "show ip ospf route" command it have learned the routing information of the 10.1.1.0/24 network segment and the 192.168.162.0/24 network segment by showing the IP ospf route.

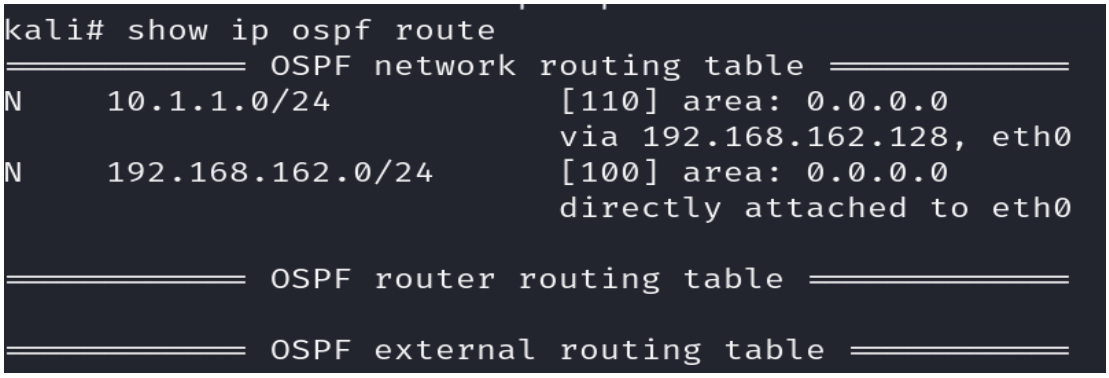


Figure 47: Show attacking machine's ospf route counts picture

(13) Figure 48 experimental results show that in the Kali attack machine, by showing the IP ospf neighbor and checking the neighbor status of the OSPF protocol, we have established a stable neighbor relationship with two routers.

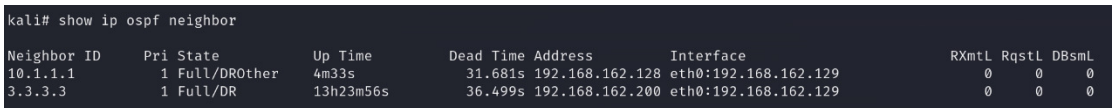


Figure 48: Show attacking machine's ospf neighbor picture

(14) Figure 49 experimental results show that in the Kali attack machine, by showing the IP ospf database to view the link state database of the OSPF protocol, it can be concluded that the Kali attack machine has synchronized with the link state database of other routers.

```
kali# show ip ospf database

       OSPF Router with ID (192.168.119.128)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1        1.1.1.1          635 0×8000007d 0×0628 2
2.2.2.2        2.2.2.2         1036 0×8000006c 0×10a2 1
3.3.3.3        3.3.3.3          645 0×8000006e 0×38e2 1
192.168.119.128192.168.119.128 1064 0×80000021 0×ffaa 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.1.1.2       2.2.2.2         1316 0×8000006a 0×4b83
192.168.162.2003.3.3.3          715 0×8000006b 0×8f0a
```

Figure 49: Show attacking machine's ospf database picture

(15) Figure 50 Experimental results show that the Kali attacker has successfully learned hidden network segments in the target network. By examining the ospf routing in the Kali attack machine, it was found that the Kali attack machine learned a route of 10.1.1.0/24 and 192.168.162.0/24. Use the commands nmap -SP 10.1.1.1-254 and nmap - SP 192.168.162.1-254 to scan the specific IP addresses as 10.1.1.1 and 10.1.1.2.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 10.1.1.1-254
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-05 21:21 CST
Nmap scan report for 10.1.1.1
Host is up (0.011s latency).
Nmap scan report for 10.1.1.2
Host is up (0.024s latency).
Nmap done: 254 IP addresses (2 hosts up) scanned in 16.10 seconds
```

Figure 50: Show the attacking machine detect ospf routing network segment picture

(16) Figure 51 experimental results show that in addition to the IP addresses of the Kali attack machine itself, the important IP addresses in this network segment are 192.168.162.128 and 192.168.162.200

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.162.1-254
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-05 21:23 CST
Nmap scan report for 192.168.162.128
Host is up (0.00055s latency).
Nmap scan report for 192.168.162.129
Host is up (0.00011s latency).
Nmap scan report for 192.168.162.200
Host is up (0.00091s latency).
Nmap done: 254 IP addresses (3 hosts up) scanned in 19.93 seconds
```

Figure 51: Show network segments detected by the attack machine picture

(17) Figure 52 experimental results show that view detailed routing information by using the commands show IP route 10.1.1.1, show IP route 10.1.1.2, show IP route 192.168.162.130, and show IP route 192.168.162.200 in the Kali attack machine. The direct route of the Kali attack machine is 192.168.162.200, and the OSPF neighbor of this direct route is 192.168.162.128 The next hop address

obtained from this address is 10.1.1.1, and the direct routing for this address is 10.1.1.2

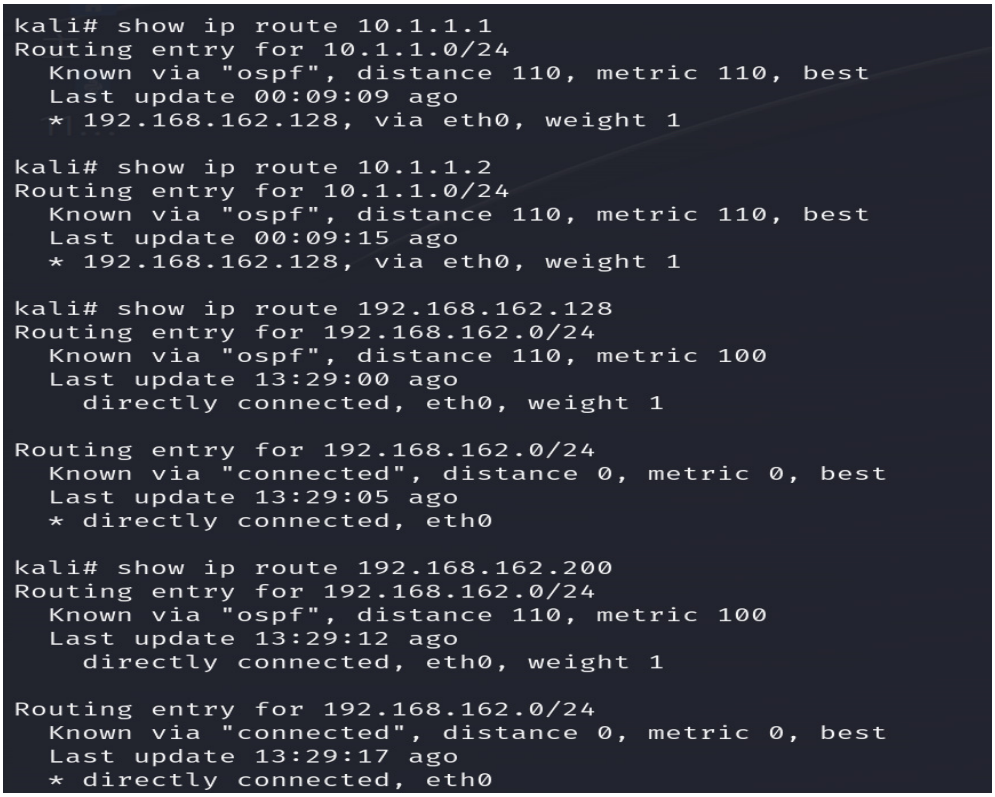


Figure 52: Show the routing details detected by the attack machine picture

(18) Based on the above routing information and OSPF neighbor status information, the network TOPO diagram can be ultimately inferred。Figure 53 is the final inferred logical topology diagram.

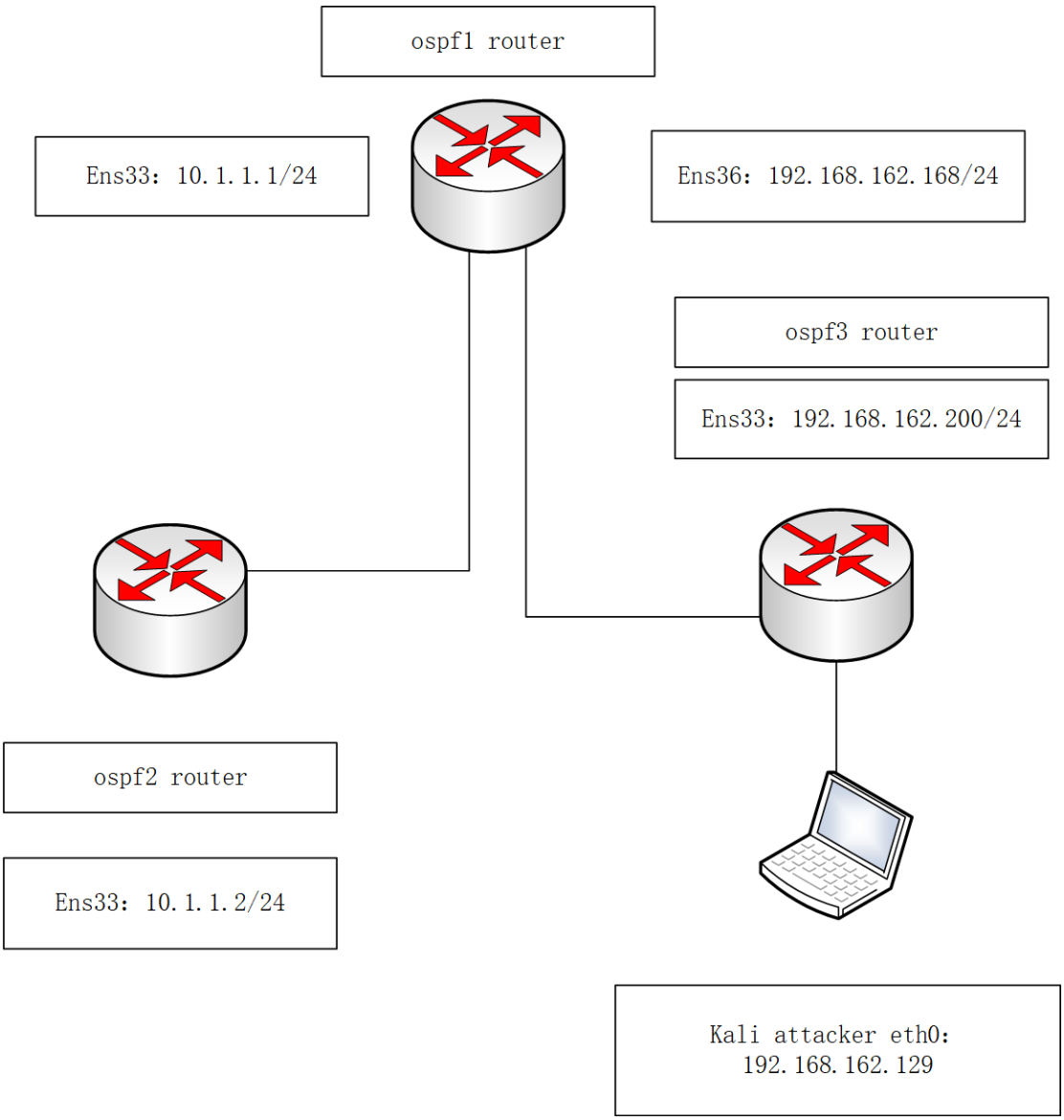


Figure 53: Show a network topology diagram inferred through the attack machines

7.6 Summary of this chapter

This chapter conducts in-depth research on the construction and security of OSPF network environment. Firstly, we provided a detailed introduction to the basic network construction process of OSPF, covering the configuration of IP addresses and subnet masks, as well as the detailed steps to configure the OSPF protocol in three virtual routers. Through these configurations, we have established a reliable

experimental environment that provides a foundation for subsequent experimental data.

In the experiment, we selected suitable attack machines and used nmap scanning tools to identify potential targets. Furthermore, we use the Scapy tool to construct fake OSPF packets and simulate attack scenarios. Through experimental analysis, we have verified the potential harm of false data packets and emphasized the security of OSPF networks.

During the experiment, we conducted a performance evaluation to evaluate the performance of the network under load. We observed indicators such as network throughput, latency, and response time, providing data support for network planning and defense.

Finally, by impersonating the Kali attack machine into a fake OSPF router, and combining the characteristics of default routes, the illegal default routes are notified to the target router through the OSPF protocol. Finally, the Kali attack machine successfully stole the routing information of the target router. NMAP scanning detects and constructs fake data packets to verify vulnerabilities in OSPF networks. The load testing of OSPF networks evaluates network performance and provides support for the effectiveness of attack behavior. These works have made contributions in the fields of network security, attack and defense, experimental

verification, and performance optimization. At the same time, this also provides a substantive reference for the defense strategy of the OSPF protocol in Chapter 8.

Chapter 8 Defense Mechanism Based on OSPF Protocol

8.1 Introduction to Regional Certification

When configuring regional authentication, a series of steps need to be followed to implement it. Firstly, select different OSPF area types based on network requirements. Then, configure these generated keys as passwords for regional authentication and implement configuration on routers in each region. By verifying and monitoring commands, it is possible to confirm the key matching of each region and verify that the authentication status of the region is "message digest".

The introduction of regional authentication mechanisms has significant significance and significant advantages. Firstly, it ensures the integrity of communication data by signing communication messages using digest algorithms, avoiding the risk of data tampering. Secondly, it ensures that only legitimate routers with the correct key configuration can join a specific area, preventing unauthorized routers from impersonating legitimate devices. Finally, routers that are not configured with the correct key will be rejected from joining the zone, effectively resisting the threat of unauthorized routers joining the

network.

8.1.1 Defense Configuration for OSPF Regional Authentication

(1) Configure authentication on 3 OSPF routers:

```
ospf1# show running-config
Building configuration...

Current configuration:
!
hostname ospfd
log file /var/log/quagga/quagga.log
log stdout
hostname ospf1
!
password zebra
!
interface ens33
 ip address 10.1.1.1/24
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 ipv6 nd suppress-ra
 link-detect
!
interface ens36
 ip address 192.168.162.128/24
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 ipv6 nd suppress-ra
 link-detect
!
interface eth0
 ipv6 nd suppress-ra
!
interface lo
!
interface virbr0
 ipv6 nd suppress-ra
!
interface virbr0-nic
 ipv6 nd suppress-ra
!
router ospf
 network 10.1.1.0/24 area 0.0.0.0
 network 192.168.162.0/24 area 0.0.0.0
 area 0 authentication message-digest
!
ip forwarding
!
line vty
!
end
```

Figure 54: Show ospf1 Global Configuration picture

（2）Explanation of Figure 54 configuration commands for OSPF1 virtual router in experimental operation:

Enable OSPF message digest authentication in ens33 and ens36

ip ospf authentication message digest

Sets the authentication key for OSPF messages on this interface, with a key that uses the md5 hash algorithm and a password of cisco in ens33 and ens36

ip ospf message digest key 1 md5 cisco

Start ospf protocol process

router ospf

Identify this router running the OSPF protocol as 1.1.1.1

ospf router-id 1.1.1.1

Publish a network segment with a 10.1.1.0 subnet mask of 255.255.255.0 in area 0

network 10.1.1.0/24 area 0.0.0.0

Publish a network segment with a 192.168.162.0 subnet mask of 255.255.255.0 in area 0

network 192.168.162.0/24 area 0.0.0.0

Associate the md5 key configured by the interface with area0 in the OSPF protocol.

area0 authentication message-digest

!

（3）Explanation of Figure 55 configuration commands for OSPF2 virtual router in experimental operation:

```
ospf2# show running-config
Building configuration...

Current configuration:
!
hostname ospfd
log file /var/log/quagga/quagga.log
log stdout
hostname ospf2
!
password zebra
!
interface ens33
 ip address 10.1.1.2/24
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 ipv6 nd suppress-ra
!
interface lo
!
interface virbr0
 ipv6 nd suppress-ra
!
interface virbr0-nic
 ipv6 nd suppress-ra
!
router ospf
 network 10.1.1.0/24 area 0.0.0.0
 area 0 authentication message-digest
!
ip forwarding
!
line vty
!
end
```

Figure 55: Show ospf2 Global Configuration picture

（4）Explanation of Figure 55 configuration commands:

Enable OSPF message digest authentication in ens33

ip ospf authentication message-digest

Sets the authentication key for OSPF messages on this interface, with a key that uses the md5 hash algorithm and a password of cisco

ip ospf message digest key 1 md5 cisco

Start ospf protocol process

router ospf

Publish a network segment with a 10.1.1.0 mask of 255.255.255.0 in area 0

network 10.1.1.0/24 area 0.0.0.0

Associate the md5 key configured by the interface with area0 in the OSPF protocol.

area0 authentication message-digest

!

（5）Explanation of Figure 56 configuration commands for OSPF3 virtual router in experimental operation:

```
ospf3# show running-config
Building configuration...

Current configuration:
!
hostname ospfd
log file /var/log/quagga/quagga.log
log stdout
hostname ospf3
!
password zebra
!
interface ens33
 ip address 192.168.162.200/24
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 ipv6 nd suppress-ra
!
interface lo
!
interface virbr0
 ipv6 nd suppress-ra
!
interface virbr0-nic
 ipv6 nd suppress-ra
!
router ospf
 network 192.168.162.0/24 area 0.0.0.0
 area 0 authentication message-digest
!
ip forwarding
!
line vty
!
end
```

Figure 56: Show ospf3 Global Configuration picture

（6）Explanation of Figure 56 configuration commands:

Enable OSPF message digest authentication in ens33

ip ospf authentication message-digest

Sets the authentication key for OSPF messages on this interface, with a key that uses the md5 hash algorithm and a password of cisco

ip ospf message digest key 1 md5 cisco

Start ospf protocol process

router ospf

Publish a network segment with a 192.168.162.0 mask of 255.255.255.0 in area 0

network 192.168.162.0/24 area 0.0.0.0

Associate the md5 key configured by the interface with area0 in the OSPF protocol.

area0 authentication message-digest

!

8.1.2 The experimental results show that:

(1) According to Figure 57, the experimental results show that the OSPF3 router can access the OSPF2 router. This indicates that routers within the OSPF network can access each other.

```
ospf3# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
64 bytes from 10.1.1.2: icmp_seq=1 ttl=63 time=0.812 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=63 time=0.706 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=63 time=0.453 ms
64 bytes from 10.1.1.2: icmp_seq=4 ttl=63 time=0.818 ms
64 bytes from 10.1.1.2: icmp_seq=5 ttl=63 time=0.708 ms
64 bytes from 10.1.1.2: icmp_seq=6 ttl=63 time=0.534 ms
64 bytes from 10.1.1.2: icmp_seq=7 ttl=63 time=0.859 ms
```

Figure 57: Show ospf3 router accessing texting picture

（2）We have pinged and verified on the Kali attack machine that it is no longer able to access three routers normally。 According to Figure 58, the experimental results show that the Kali attacker is no longer able to successfully access network segments in the OSPF network, resulting in the phenomenon of unreachable routing.

```
kali# ping 10.1.1.1
ping: connect: Network is unreachable
kali# ping 10.1.1.2
ping: connect: Network is unreachable
kali# ping 192.168.200
ping: connect: Network is unreachable
```

Figure 58: Show OSPF3 router accessing texting picture

（3）According to the experimental results shown in Figure 59, Figure 60, and Figure 61， check the routing of OSPF on the Kali co-attack machine, and determine the neighbor status and link status databases of OSPF. The Kali attack machine is no longer able to view the neighbor status of the three routers and receive routing information from the three routers. Finally, the link database cannot be synchronized.

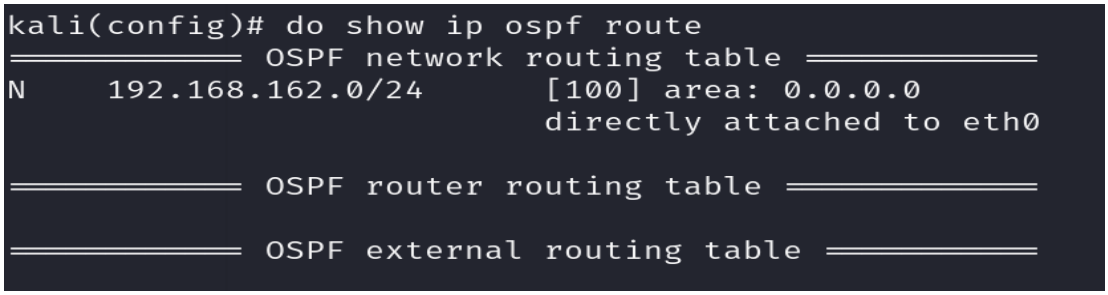


Figure 59: Show Kali attacking machine's route count picture

Figure 60: Show ospf neighbor picture

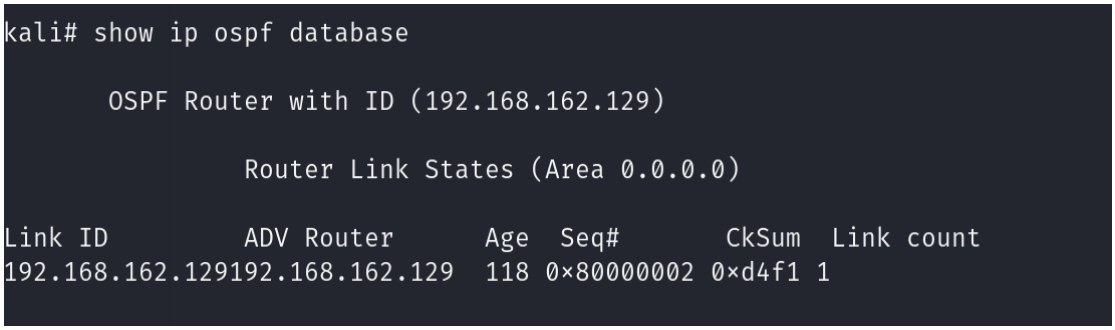


Figure 61: Show kali attacking machine's ospf database picture

8.2 Introduction to Passive Interface Protection Mechanism

The working principle of the Passive Interface protection mechanism is to set certain OSPF interfaces as "passive", thereby preventing these interfaces from actively sending OSPF Hello messages and link status update information. Through this setting, the mechanism effectively reduces the number of possible attacks on the entry points, thereby reducing the probability of abnormal behavior

on the network.

The advantages of this mechanism are obvious. Firstly, it effectively reduces the attack surface of the network by reducing the active participation of interfaces, thereby improving the security of the network. Secondly, by reducing unnecessary protocol communication, the Passive Interface mechanism reduces the consumption of network resources and optimizes network performance. In addition, this mechanism can also prevent malicious nodes from spoofing attacks by forging Hello messages, maintaining the stable operation of the network.

8.2.1 Defense Configuration for OSPF Regional Authentication

（1）Configure passive interfaces to prevent the injection of illegal routes in ospf1 router:

```
ospf1# show running-config
Building configuration...

Current configuration:
!
hostname ospfd
log file /var/log/quagga/quagga.log
log stdout
hostname ospf1
!
password zebra
!
interface ens33
 ip address 10.1.1.1/24
 ipv6 nd suppress-ra
 link-detect
!
interface ens36
 ip address 192.168.162.128/24
 ipv6 nd suppress-ra
 link-detect
!
interface eth0
 ipv6 nd suppress-ra
!
interface lo
!
interface virbr0
 ipv6 nd suppress-ra
!
interface virbr0-nic
 ipv6 nd suppress-ra
!
router ospf
 ospf router-id 1.1.1.1
 passive-interface default
 network 10.1.1.0/24 area 0.0.0.0
 network 192.168.162.0/24 area 0.0.0.0
!
ip forwarding
!
line vty
!
end
```

Figure 62: Show ospf1 passive interface of global Configuration picture

Explanation of Figure 62 passive interface configuration commands for OSPF1 virtual router in experimental operation:

#Start ospf protocol process

router ospf

Identify this router running the OSPF protocol as 1.1.1.1

ospf router-id 1.1.1.1

Configure the interface declared in this region as a passive interface

passive-interface default

Publish a network segment with a 10.1.1.0 mask of 255.255.255.0 in area 0

network 10.1.1.0/24 area 0.0.0.0

Publish a 192.168.162.0 network segment with a mask of 255.255.255.0 in area 0

network 192.168.162.0/24 area 0.0.0.0

!

（2）Configure passive interfaces to prevent the injection of illegal routes in ospf2 router:

```
ospf2# show running-config
Building configuration...

Current configuration:
!
hostname ospfd
log file /var/log/quagga/quagga.log
log stdout
hostname ospf2
!
password zebra
!
interface ens33
 ip address 10.1.1.2/24
 ipv6 nd suppress-ra
!
interface lo
!
interface virbr0
 ipv6 nd suppress-ra
!
interface virbr0-nic
 ipv6 nd suppress-ra
!
router ospf
 ospf router-id 2.2.2.2
 passive-interface default
 network 10.1.1.0/24 area 0.0.0.0
!
ip forwarding
!
line vty
!
end
```

Figure 63: Show ospf2 passive interface of global Configuration picture

Explanation of Figure 63 passive interface configuration commands for OSPF2 virtual router in experimental operation:

Start ospf protocol process

router ospf

Identify this router running the OSPF protocol as 2.2.2.2

ospf router-id 2.2.2.2

Configure the interface declared in this region as a passive interface

passive-interface default

Publish a network segment with a 10.1.1.0 mask of 255.255.255.0 in area 0

network 10.1.1.0/24 area 0.0.0.0

（3）Configure passive interfaces to prevent the injection of illegal routes in ospf3 router:

```
ospf3# show running-config
Building configuration...

Current configuration:
!
hostname ospfd
log file /var/log/quagga/quagga.log
log stdout
hostname ospf3
!
password zebra
!
interface ens33
 ip address 192.168.162.200/24
 ipv6 nd suppress-ra
!
interface lo
!
interface virbr0
 ipv6 nd suppress-ra
!
interface virbr0-nic
 ipv6 nd suppress-ra
!
router ospf
 passive-interface default
 network 192.168.162.0/24 area 0.0.0.0
!
ip forwarding
!
line vty
!
end
```

Figure 64: Show ospf3 passive interface of global Configuration picture

Explanation of Figure 64 passive interface configuration commands for OSPF3 virtual router in experimental operation:

Start ospf protocol process

router ospf

Identify this router running the OSPF protocol as 3.3.3.3

ospf router-id 3.3.3.3

Configure the interface declared in this region as a passive interface

passive-interface default

Publish a 192.168.162.0 network segment with a mask of 255.255.255.0 in area 0

network 192.168.162.0/24 area 0.0.0.0

Experimental results:

18. According to the experimental results of Figure 65, it is shown that test the connectivity of OSPF3 router accessing OSPF2 router on OSPF3 router. It is concluded that the OSPF3 router can access the OSPF2 router.

```
ospf3# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
64 bytes from 10.1.1.2: icmp_seq=1 ttl=63 time=0.812 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=63 time=0.706 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=63 time=0.453 ms
64 bytes from 10.1.1.2: icmp_seq=4 ttl=63 time=0.818 ms
64 bytes from 10.1.1.2: icmp_seq=5 ttl=63 time=0.708 ms
64 bytes from 10.1.1.2: icmp_seq=6 ttl=63 time=0.534 ms
64 bytes from 10.1.1.2: icmp_seq=7 ttl=63 time=0.859 ms
```

Figure 65: Show ospf3 router accessing ospf2 router's accessing texting picture

19. According to the experimental results of Figure 66, Figure 67, and Figure 68, it is shown that, check the routing of OSPF on the Kali co-attack machine, and obtain the OSPF neighbor status and link status database. The Kali attack machine is no longer able to view the neighbor status of the three routers and receive routing information from the three routers. Finally, the link database cannot be synchronized.

```
kali(config)# do show ip ospf route
============ OSPF network routing table ============
N    192.168.162.0/24      [100] area: 0.0.0.0
                           directly attached to eth0

============ OSPF router routing table =============

============ OSPF external routing table ===========
```

Figure 66: Show kali attacking machine's ospf route count picture

```
kali# show ip ospf neighbor

Neighbor ID     Pri State         Up Time       Dead Time Address       Interface                RXmtL RqstL DBsmL
```

Figure 67: Show kali attacking machine's ospf neighbor picture

```
kali# show ip ospf database

       OSPF Router with ID (192.168.162.129)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
192.168.162.129192.168.162.129  118 0×80000002 0×d4f1 1
```

Figure 68: Show kali attacking machine's ospf database picture

8.3 Summary of this chapter:

In this chapter, we delve into security enhancement measures for OSPF networks, with a focus on the implementation and significance of OSPF regional authentication and passive interface protection mechanisms. Firstly, this section provides a detailed introduction to the importance of OSPF region authentication. This mechanism prevents illegal routers from joining by requiring all routers in the region to use the same authentication password, thereby maintaining the integrity and stability of the network. This chapter emphasizes the important role of regional authentication in preventing malicious router intrusion and protecting the network from unauthorized configuration changes.

On the other hand, the application of passive interface protection mechanism in OSPF networks was emphasized. The passive interface protection mechanism can detect and block unauthorized OSPF Hello messages, thereby reducing the risk of DDoS attacks on the network. We emphasized how this mechanism can help the network effectively respond to malicious attacks and maintain the availability and stability of the network.

Chapter 9 Work Summary and Prospects

9.1 Work Summary

Against the backdrop of frequent security flaws in the OSPF routing protocol, this article first provides a clear introduction to the basic principles of OSPF. Secondly, a thorough analysis was conducted on the principles of OSPF Denial of Service attachment and OSPF Other LSA false attachment, and the setting of attack parameters and specific attack processes were summarized and summarized. Afterwards, we studied the existing virtualization simulation platforms and designed and implemented a virtualization network simulation platform for routing protocol security research. Finally, a multi-perspective attack method was studied on the network interruption scenario caused by the false adjacency of virtual routes.

Therefore, the main work of this article is as follows:

（1）Based on a network attack against OSPF - OSPF Denial of Service attacks, and proposed a specific attack method. Firstly, the security flaws in the adjacency process of the OSPF protocol were studied, and the principles and attack parameters of OSPF Denial of Service attacking were analyzed, with specific attack steps clarified. Secondly, a method was developed to construct fake OSPF Hello

packets through the Scapy module to attack the target router in the local area network. Finally, this attack method resulted in a high network load.

（2）Based on a network attack against OSPF - OSPF Other LSA false attachment, a specific attack method is proposed. OSPF Other LSA false attachment causes the theft of target routing information in the local area network through default route injection. Firstly, based on the area where the victim router is located, an experimental network attack scenario was designed and constructed, and methods for stealing routing information in the experimental network were studied. A stealing idea by injecting default routes was proposed. Secondly, based on the virtualization network simulation platform, simulation experiments were conducted to verify the attack scenarios and methods, as well as to obtain attack parameters.

（1）Designed and implemented a virtual network security simulation platform. Firstly, this simulation platform utilizes virtualization technology to simulate real network devices. Secondly, an attack module has been designed and implemented in this simulation platform for routing protocol security analysis. Finally, this simulation platform adopts a distributed C/S architecture, which is more conducive to network device resource sharing and saves hardware resources.

（2）A defense method against Denial-of-Service attachment and OSPF Other LSA false attachment was proposed for the research in Job 1 and Job 2. Specific solutions were provided in terms of the OSPF protocol stack and OSPF security configuration.

9.2 Future Work

Future work will start from the following three aspects:

Firstly, the defense method proposed in this article mainly relies on manually configuring the security of the OSPF protocol, which requires administrator intervention. Future research can consider developing automated security configuration functions based on the OSPF protocol to reduce configuration complexity and improve system security.

Secondly, this article focuses on the prevention of routing spoofing in broadcast OSPF protocol networks. However, the actual network covers multiple types, and there are differences in its operating mechanisms, which may affect the accuracy of detection. Future research can detect and prevent different types of network attacks while developing corresponding routing protocol security detection systems to improve security performance.

Finally, although this article focuses on IP attacks and defences in local area networks, with the rapid development of wireless IP networks, the risk of attacks

they face is also increasing. Future research can expand its focus to wireless IP networks, exploring attack detection and prevention technologies to ensure the security of wireless networks.

References：

[1] M. Bishop, "What is computer security?," *IEEE Security & Privacy,* vol. 1, no. 1, pp. 67-69, 2003.

[2] W. Ming-Hao, "The security analysis and attacks detection of OSPF routing protocol," in *2014 7th International Conference on Intelligent Computation Technology and Automation*, 2014: IEEE, pp. 836-839.

[3] K. Pahlavan and P. Krishnamurthy, *Networking fundamentals: Wide, local and personal area communications*. John Wiley & Sons, 2009.

[4] L. Lum and P. A. Beachy, "The Hedgehog response network: sensors, switches, and routers," *science,* vol. 304, no. 5678, pp. 1755-1759, 2004.

[5] M. A. Sportack and J. Fairweather, *IP routing fundamentals*. Cisco Press, 1999.

[6] U. D. Black, *IP routing protocols: RIP, OSPF, BGP, PNNI, and Cisco routing protocols*. Prentice Hall Professional, 2000.

[7] D. Mitra, S. Sarkar, and D. Hati, "A comparative study of routing protocols," *Engineering and Science,* vol. 2, no. 1, pp. 46-50, 2016.

[8] G. Ash, R. H. Cardwell, and R. Murray, "Design and optimization of networks with dynamic routing," *Bell System Technical Journal,* vol. 60, no. 8, pp. 1787-1820, 1981.

[9] J. Moy, "OSPF version 2," 2070-1721, 1997.

[10] G. Malkin, "RIP version 2," 2070-1721, 1998.

[11] J. Moy, "RFC2328: OSPF Version 2," ed: RFC Editor, 1998.

[12] A. Shaikh, C. Isett, A. Greenberg, M. Roughan, and J. Gottlieb, "A case study of OSPF behavior in a large enterprise network," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*, 2002, pp. 217-230.

[13] M. Goyal *et al.*, "Improving convergence speed and scalability in OSPF: A survey," *IEEE Communications Surveys & Tutorials,* vol. 14, no. 2, pp. 443-463, 2011.

[14] H. Nurwarsito and A. R. Sindunata, "Optimization of Hello Interval in OSPF Routing Protocol Performance on Mesh Network Topology," in *2020 10th Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)*, 26-28 Aug. 2020 2020, pp. 222-225, doi: 10.1109/EECCIS49483.2020.9263434.

[15] A. Cianfrani, V. Eramo, M. Listanti, M. Marazza, and E. Vittorini, "An energy saving routing algorithm for a green OSPF protocol," in *2010 INFOCOM IEEE Conference on Computer Communications Workshops*, 2010: IEEE, pp. 1-5.

[16] K. Manousakis, T. McAuley, R. Morera, and J. Baras, "Using multi-objective domain optimization for routing in hierarchical networks," in *2005 International Conference on Wireless Networks, Communications and Mobile Computing*, 13-16 June 2005 2005, vol. 2, pp. 1460-1465 vol.2, doi: 10.1109/WIRLES.2005.1549628.

[17] J. Moy, "OSPF standardization report," 2070-1721, 1998.

[18] K. Holter, A. Hafslund, F. Y. Li, and K. Øvsthus, "Design and implementation of wireless OSPF for mobile ad hoc networks," in *Scandinavian Workshop on Wireless Ad-hoc Networks (ADHOC 06)*, 2005.

[19] M. Bhatia *et al.*, "OSPFv2 HMAC-SHA cryptographic authentication," 2070-1721, 2009.
[20] H.-Y. Chang, S. F. Wu, and Y. F. Jou, "Real-time protocol analysis for detecting link-state routing protocol attacks," *ACM Transactions on Information and System Security (TISSEC),* vol. 4, no. 1, pp. 1-36, 2001.
[21] G. Nakibly, A. Kirshon, D. Gonikman, and D. Boneh, "Persistent OSPF Attacks," in *NDSS*, 2012.
[22] B. Al-Musawi, P. Branch, M. F. Hassan, and S. R. Pokhrel, "Identifying OSPF LSA falsification attacks through non-linear analysis," *Computer Networks,* vol. 167, p. 107031, 2020.
[23] R. Rivest, "The MD5 message-digest algorithm," 2070-1721, 1992.
[24] D. Zhao, C. Wu, X. Hu, X. Wang, and B. Zhao, "Characterization of ospf convergence with correlated failures," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2013: IEEE, pp. 1351-1356.
[25] P. Gundalwar and V. Chavan, "Area Configuration and Link Failure Effect in IP Networks using OSPF Protocol," *International Journal of Scientific and Research Publications,* vol. 3, no. 4, 2013.
[26] A. Kirshon, D. Gonikman, and G. Nakibly, "Owning the Routing Table New OSPF Attacks," *BlackHat Briefings and Trainings USA,* vol. 2011, pp. 1-18, 2011.
[27] Y. N. Krishnan and G. Shobha, "Performance analysis of OSPF and EIGRP routing protocols for greener internetworking," in *2013 International Conference on Green High Performance Computing (ICGHPC)*, 2013: IEEE, pp. 1-4.
[28] Y. Song, S. Gao, A. Hu, and B. Xiao, "Novel attacks in OSPF networks to poison routing table," in *2017 IEEE International Conference on Communications (ICC)*, 2017: IEEE, pp. 1-6.
[29] C. L. Hedrick, "Routing information protocol," 2070-1721, 1988.
[30] W. R. Parkhurst, *Cisco OSPF command and configuration handbook*. Cisco Press, 2002.
[31] S. N. T.-c. Chiueh and S. Brook, "A survey on virtualization technologies," *Rpe Report,* vol. 142, 2005.
[32] R. Kumar and S. Charu, "An importance of using virtualization technology in cloud computing," *Global Journal of Computers & Technology,* vol. 1, no. 2, 2015.
[33] D. T. Vojnak, B. S. Đorđević, V. V. Timčenko, and S. M. Štrbac, "Performance Comparison of the type-2 hypervisor VirtualBox and VMWare Workstation," in *2019 27th Telecommunications Forum (TELFOR)*, 2019: IEEE, pp. 1-4.
[34] P. Jakma and D. Lamparter, "Introduction to the quagga routing suite," *IEEE Network,* vol. 28, no. 2, pp. 42-48, 2014.
[35] A. Ramanath, "A Study of the interaction of BGP/OSPF in Zebra/ZebOS/Quagga," *Computer Science Department, State University of New York at Stony Brook, Tech. Rep,* 2000.
[36] M. Ogul, N. Akçam, and N. Erkan, "Measurement of OSPF-MPLS-TE-FRR line transitions and data losses," *Balkan Journal of Electrical and Computer Engineering,* vol. 2, no. 2, pp. 46-50, 2014.
[37] W. B. Kihuya, C. Otieno, and R. Rimiru, "Fuzzy Logic Model for Analysis of Computer Network Quality of Experience."
[38] P. Biondi, "Packet generation and network based attacks with scapy," *CanSecWest/core05,* 2005.

[39] E. Sagas, "Deploying an Open Source Router: Quagga," 2013.
[40] P. Martin, "IPv4 Anycast with Linux and Quagga," *Linux Journal,* vol. 2009, no. 187, p. 4, 2009.
[41] С. ЯРЕМЧУК, "Маршрутизация с Quagga," *Системный администратор,* no. 5, pp. 40-43, 2010.
[42] G. Howser and G. Howser, "Route Interchange Protocol," *Computer Networks and the Internet: A Hands-On Approach,* pp. 245-269, 2020.
[43] G. Howser and G. Howser, "Open shortest path first," *Computer Networks and the Internet: A Hands-On Approach,* pp. 271-297, 2020.
[44] M. Kontšek and P. Segeč, "Testing of the current open-source EIGRP implementations," in *2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2018: IEEE, pp. 291-296.
[45] N. G.-S. Góngora, "Taller de Sistemas Ciberfísicos."
[46] W. Shotts, *The Linux command line: a complete introduction*. No Starch Press, 2019.
[47] R. Simola, "Data Centre Network Design and Development: Collapsed Leaf-Design," 2020.
[48] G. Howser and G. Howser, "Service Provider Protocols," *Computer Networks and the Internet: A Hands-On Approach,* pp. 299-319, 2020.
[49] R. Rohith, M. Moharir, and G. Shobha, "SCAPY-A powerful interactive packet manipulation program," in *2018 international conference on networking, embedded and wireless systems (ICNEWS)*, 2018: IEEE, pp. 1-5.
[50] J.-E. Luukkonen, "Integrated services access node with Linux," 2016.
[51] S. Sirohi and A. Gupta, *Koha 3 Library Management System*. Packt Publishing Ltd, 2010.
[52] S. H. B. Brito, *Serviços de Redes em Servidores Linux*. Novatec Editora, 2017.
[53] E. Siever, A. Weber, S. Figgins, R. Love, and A. Robbins, *Linux in a Nutshell*." O'Reilly Media, Inc.", 2005.
[54] A. Cianfrani, V. Eramo, M. Listanti, and M. Polverini, "An OSPF enhancement for energy saving in IP networks," in *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2011: IEEE, pp. 325-330.
[55] M. Bogdanoski and A. Risteski, "Wireless network behavior under icmp ping flooddos attack and mitigation techniques," *International Journal of Communication Networks and Information Security (IJCNIS),* vol. 3, no. 1, 2011.
[56] M. Navarro, J. C. Rangel, and E. Cruz, "Automatic OSPF Topology map generation using information of the OSPF database," *KnE Engineering,* pp. 853-861, 2018.
[57] L. Spitzner, "Configuring Network Interface Cards," ed: Aug, 1999.
[58] A. Orebaugh and B. Pinkard, *Nmap in the enterprise: your guide to network scanning*. Elsevier, 2011.
[59] U. Lamping and E. Warnicke, "Wireshark user's guide," *Interface,* vol. 4, no. 6, p. 1, 2004.
[60] S. M. Bellovin, M. Leech, and T. Taylor, "ICMP traceback messages," 2003.