

Simulation and Analysis of OSPFv2 Neighbor Authentication Based on GNS

Xiaohua Li^{1, a}, Xiangang Zhao², Renlong Zhang¹, Shuyan Xu¹ and Li Yang¹

¹ School of Computer and Information Engineering, Beijing University of Agriculture, Beijing, China

² National Satellite Meteorological Center, Beijing, China

^a lixiaohuabj@gmail.com

Keywords: OSPFv2; neighbor authentication; GNS; MD5

Abstract. Routing information release is a kind of promise from the router for network reachability. Illegal routing information may have disastrous effects on the normal work of the network. Open Shortest Path First (OSPF) protocol provides authentication methods to protect the authenticity and integrity of the routing traffic. This paper describes two authentication types of OSPFv2, analyzes the realization mechanism and packet header format of each authentication respectively. Based on GNS3, a typical network topology was designed, and with the aid of it we carried out functional verification and security analysis. The simulation can provide a reference for building an OSPF network. Experimental results show that the configuration of OSPFv2 routing authentication can effectively prevent the router from receiving unauthorized or malicious routing updates, thereby improving network safety.

Introduction

To feasibly protect the authenticity and integrity of the routing traffic and provide the means to verify the authority of the participating routers, Open Shortest Path First protocol version 2 [1-3] (OSPFv2) supports two types of authentication. In this paper, we focus on the simulation and analysis of OSPFv2 routing authentication. We discuss the two authentication types of OSPFv2 in section 2, and carry out GNS-based simulation and analysis in section 3. Finally we give conclusions in section 4.

OSPFv2 Authentication

OSPFv2 supports two types of authentication [4-6]: one is simple password authentication and the other is MD5 cryptographic authentication. The authentication type is configurable on a per-interface basis and the 2-byte authentication type field (*AuthType*) in the OSPFv2 packet header should be set accordingly. Different type of authentication has different packet header format and realization principle. We will discuss it in the following.

Simple Password Authentication

In simple password authentication, the *AuthType* field in the OSPFv2 packet header (shown in Fig. 1) should be set to 1. At the same time, a 64-bit clear text password can be configured and all packets sent on a particular network must have this configured value in their OSPFv2 header. The received OSPFv2 packets will be authenticated according to the following rules. Packets which fail authentication will be discarded.

- The *AuthType* field in the received OSPFv2 packet header should match the setting of *AuthType* for the receiving OSPFv2 interface.
- The 64-bit *authentication* field in the received OSPFv2 packet header must be equal to the 64-bit password (i.e., *authentication* key) that has been configured for the interface.

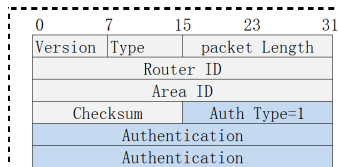


Figure 1. OSPF packet header in simple password authentication.

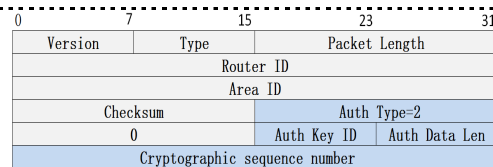


Figure 2. OSPF packet header in MD5 authentication.

MD5 Cryptographic Authentication

In MD5 cryptographic authentication, the *AuthType* field in the OSPFv2 packet header should be set to 2. In addition, the 64-bit *Authentication* field in the standard OSPFv2 packet header is redefined as shown in Fig. 2 and a 64-byte *crypto authentication TLV* (message digest) will be appended to the OSPFv2 packet as well. The new field definitions are as follows:

- *Key ID*: This field identifies the algorithm and secret key used to create the message digest appended to the OSPFv2 packet. Key Identifiers are unique per-interface (or equivalently, per-subnet).
- *Auth Data Len*: The length in bytes of the message digest appended to the OSPFv2 packet.
- *Cryptographic sequence number*: An unsigned 32-bit non-decreasing sequence number. Used to guard against replay attacks.

The received OSPFv2 packets will be authenticated according to the following rules. Packets which fail authentication will be discarded.

- Locate the receiving interface's configured key having *Key ID* equal to that specified in the received OSPFv2 packet. If the key is not found, or if the key is not valid for reception, the OSPFv2 packet is discarded.
- If the *cryptographic sequence number* found in the OSPFv2 header is less than the *cryptographic sequence number* recorded in the sending neighbor's data structure, the OSPFv2 packet is discarded.
- Verify the appended message digest. Calculate a new digest and let it compare with the received one. If they do not match, the OSPFv2 packet is discarded. If they do match, the OSPFv2 protocol packet is accepted as authentic.

Simulations and Analysis

In this section, a typical network topology is designed and with the aid of GNS3, we carry out simulation and analysis. GNS (Graphical Network Simulator) is a very good graphical network simulator that can simulate the real IOS and complex networks. It is visual and accurate, with friendly interface, convenient operation, and strong interactivity. It can be said to be one of the most popular network simulators. It is also an excellent complementary tool to real labs for network engineers, administrators etc. It is an open source, free program that may be used on multiple operating systems, including Windows, Linux, and MacOS X.

Experimental Network Topology and Configurations

We design such a network topology as shown in Fig. 3, which is a two-level hierarchical routing scheme. It consists of three areas and 10 C7200 routers. Through serial and fastEthernet connections the routers are connected and compose a typical LAN network. In this topology, R3 and R2 are *Area Border Routers*: through R3 area 0 and area 2 is connected, whereas area 0 and area 1 is connected through R2. The *router ID* and other corresponding configurations for each router are set and marked in the figure.

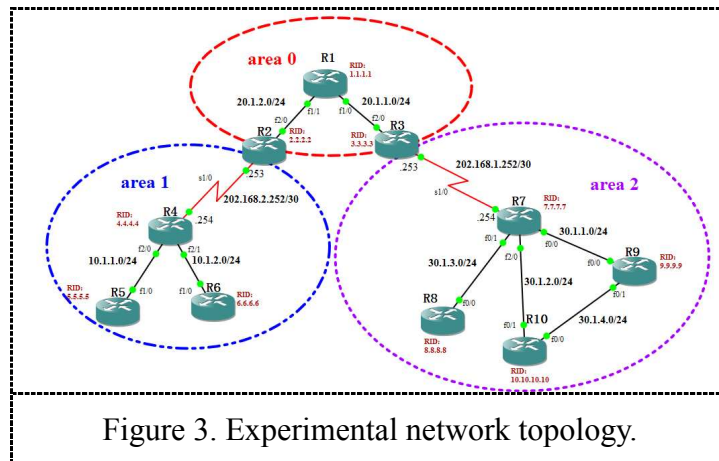


Figure 3. Experimental network topology.

Simulation and Analysis of Simple Password Authentication

Router R3 and R7 are connected through serial connection. We will enable simple password authentication to this connection and capture the data packets on this route using Wireshark software. We will unpack and analyze the captured packets to discuss the behaviour of OSPFv2 and analyze the security of OSPFv2 authentication.

By default, OSPFv2 employs *Null* authentication, meaning that all the routing exchanges over the network/subnet are not authenticated. In this case, when R3 and R7 runs, after sending *hello* messages periodically in the network, they can find each other as their neighboring router, establish full adjacency and synchronization with each other. Fig. 4 demonstrates the packet series for database synchronization in OSPFv2 *Null* authentication. From this series of operation, R3 can learn the routes in area 2 from R7, thus, all the routers in the topology can *Ping* and communicate with each other. When simple password authentication is configured on R7, as for the mismatch authentication type, the neighbor relationship between R3 and R7 is broken. Examine the neighbor list of R3, we find that only R1 is the neighbor of R3. The topology at this time becomes isolated and routers in area 2 cannot communicate with other routers in area 0 and area 1. But if we set the same password and enable simple password authentication on R3, we can see the full adjacency between R3 and R7 is established again (shown in Fig. 5).

Figure 4. Database synchronization in OSPF Null authentication.

Figure 5. Database synchronization in OSPF simple password authentication.

Examine the neighbor list and route table of R3 (shown in Fig. 6), we can see R7 becomes its full adjacent neighbor and R3's route table is complete and convergent.

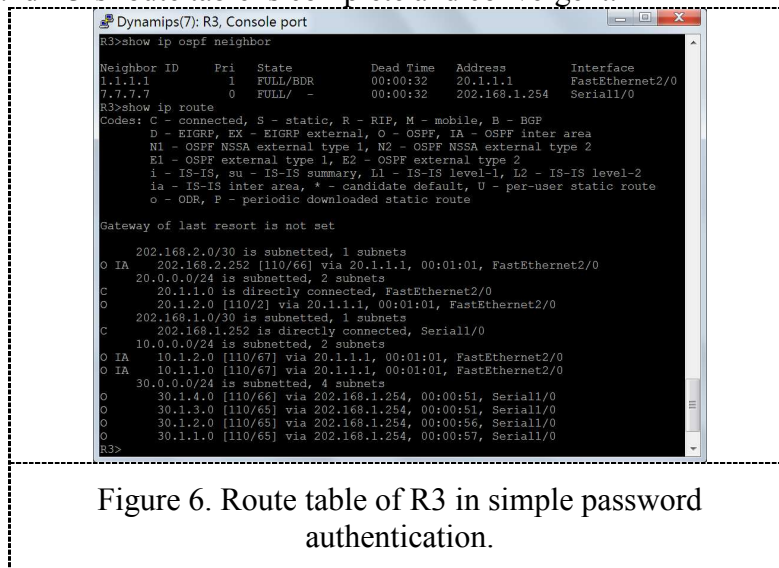


Figure 6. Route table of R3 in simple password authentication.

Simulation and Analysis of MD5 Cryptographic Authentication

We will enable *MD5 cryptographic authentication* to the serial connection between R2 and R4. By default, OSPFv2 employs *Null authentication*. In this case, after sending *hello* messages periodically in the network, R2 and R4 can find each other as their neighboring router. After the establishment of full adjacency, their link state databases are synchronized. When *MD5 cryptographic authentication* is configured on R2, packet series captured using *Wireshark* (shown in Fig.7) demonstrate that the neighbor relationship between the two routers is broken due to the mismatch of authentication type, but when we enable MD5 cryptographic authentication on R4, full adjacency and synchronization between the two routers is established again (shown in Fig. 8).

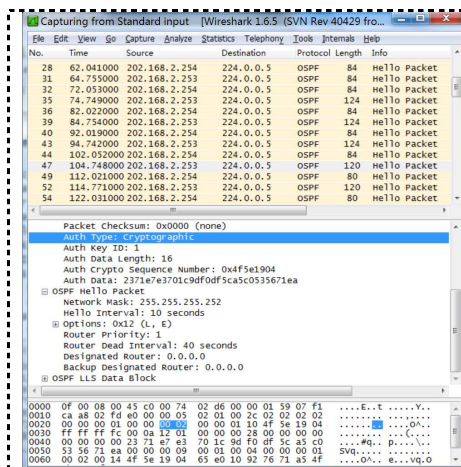


Figure 7. Neighbor relationship breaks in MD5 cryptographic authentication.

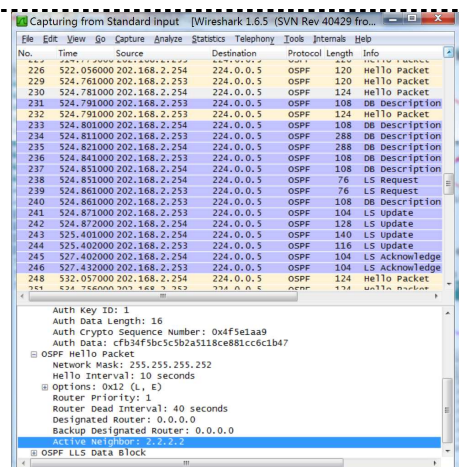
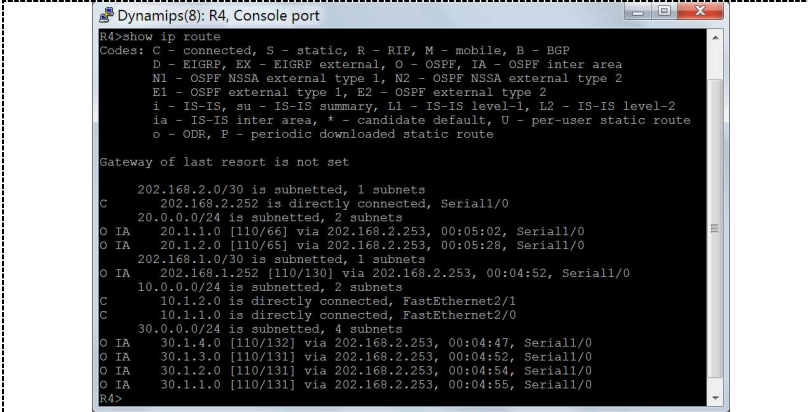


Figure 8. Establishment of full adjacency in MD5 cryptographic authentication.

Examine the route tables of R4 (shown in Fig. 9), we can see it is complete and convergent.



```

Dynamips(8): R4, Console port
R4>show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, LL - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    202.168.2.0/30 is subnetted, 1 subnets
    C      202.168.2.252 is directly connected, Serial1/0
    20.0.0.0/24 is subnetted, 2 subnets
    O IA   20.1.1.0 [110/66] via 202.168.2.253, 00:05:02, Serial1/0
    O IA   20.1.2.0 [110/65] via 202.168.2.253, 00:05:28, Serial1/0
    202.168.1.0/30 is subnetted, 1 subnets
    O IA   202.168.1.252 [110/130] via 202.168.2.253, 00:04:52, Serial1/0
    10.0.0.0/24 is subnetted, 2 subnets
    C      10.1.2.0 is directly connected, FastEthernet2/1
    C      10.1.1.0 is directly connected, FastEthernet2/0
    30.0.0.0/24 is subnetted, 4 subnets
    O IA   30.1.4.0 [110/132] via 202.168.2.253, 00:04:47, Serial1/0
    O IA   30.1.3.0 [110/131] via 202.168.2.253, 00:04:52, Serial1/0
    O IA   30.1.2.0 [110/131] via 202.168.2.253, 00:04:54, Serial1/0
    O IA   30.1.1.0 [110/131] via 202.168.2.253, 00:04:55, Serial1/0
R4>

```

Figure 9. R4's Route table in MD5 authentication.

Summary

This paper makes a study of OSPFv2 neighbor routing authentication, analyzes the realization mechanisms and packet header formats of the simple password and MD5 cryptographic authentication. Based on GNS, simulation and analysis are carried out. Experimental results show that the configuration of the OSPFv2 neighbor routing authentication can prevent the router from receiving unauthorized or malicious routing updates, thereby improving network safety. Using Wireshark to capture OSPFv2 packets and analyze the security of OSPFv2 authentication, we can see simple password authentication can guard against routers inadvertently joining the routing domain, but it is vulnerable to passive attacks. Anyone with physical access to the network can learn the password. MD5 cryptographic authentication is much safer than simple password authentication. It can prevent eavesdropping on the line to obtain the authentication key phenomenon effectively. However, since the whole OSPFv2 packet (encapsulated in IP packet) are exposed in clear text security in the segment, if the IP header are modified, it will be very difficult to detect and it may have disastrous effects on the normal work of the network, thus we must explore new security enhancements to OSPFv2, which is the emphasis of our future work.

Acknowledgment

This work is sponsored by the project of Beijing Committee of Education (KM201210020004). Renlong Zhang is the corresponding author. We thank the authors involved in our reference for sharing data and beneficial inspirations with us. We also thank the peer review experts for their guidance and advice. Many references had to be deleted due to limited space, and I apologize to authors and readers for work that could not be cited.

References

- [1] K. Manousakis and A. J. McAuley 2008 6th Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, Wiopt 2008, April 1, 2008 - April 3, 2008 (Berlin, Germany, 2008) pp 394-402
- [2] R. Rastogi, Y. Breitbart, M. Garofalakis, and A. Kumar 2002 IEEE Infocom 2002, June 23, 2002 - June 27, 2002 (New York, NY, United states, 2002) pp 874-882
- [3] P. A. Spagnolo and T. R. Henderson 2007 Military Communications Conference, MILCOM 2007, October 29, 2007 - October 31, 2007 (Orlando, FL, United states, 2007)

-
- [4] M. Yu 2006 IEEE international Conference on Systems,Man, and Cybernetics (Taipei, Taiwan, October 8-11 2006) pp 1891-1896
 - [5] J. Goold and M. Clement 2007 2nd International Conference on Internet Monitoring and Protection, ICIMP 2007, July 1, 2007 - July 5, 2007 (San Jose, CA, United states, 2007)
 - [6] P. Li, S.-D. Wang, R.-C. Wang, and D.-Y. Zhang 2005 Research on security of OSPF routing protocol with digital signature Nanjing Youdian Xueyuan Xuebao/Journal of Nanjing Institute of Posts and Telecommunications 25 86-90.