L-005

MTU Analysis for Integrated Wireless Authentication System

Zulong Zhang‡　Eiji Takimoto‡　Toshikazu Nishimura‡

1. Introduction

For security purposes, access restrictions are often set in Wireless LAN, such as data encryption. It is not a good idea to directly open a hotspot to the public because users who do malicious acts might be hard to be tracked. Integrated Wireless Authentication System [1] (IWAS, Japan Patent No. 4332000) is invented for securely sharing Wi-Fi to the public. For non-local users, IWAS can redirect them to external authentication servers through a virtual private network (VPN) and users can securely access the Internet through shared open Wi-Fi.

The Maximum Transmission Unit (MTU) is the largest number of bytes an individual packet can have, while a wrong MTU may cause persistent application issues. IP fragmentation will occur when trying to send an IP packet larger than its MTU. This paper studies MTU for IWAS under various circumstances by analyzing different headers in the transmitted data.

2. Integrated Wireless Authentication System

2.1 System Architecture

IWAS is a system that integrates multiple authentication services and allows the users from different organizations to connect to the Access Point (AP) for Internet access. Figure 1 shows the architecture of IWAS implementation for two organizations that use Point-to-Point Protocol over Ethernet [2] (PPPoE). PPPoE is one of a network protocol that encapsulates Point-to-Point Protocol [3] (PPP) frames inside Ethernet frames and supports Authentication, Authorization, and Accounting (AAA). Each organization has a PPPoE server for authentication which can forward packets for authenticated clients. Unauthenticated clients cannot send or receive anything even if they stay connected. The three individual LANs (called chopped LANs) are connected through Layer 2 VPN (L2-VPN).

Here “L2” stands for data link layer in the Open System Interconnection (OSI) model. In L2-VPN, a VPN server can relate to multiple clients, and Ethernet frames can be transmitted through any connected node, regardless of server or client. Moreover, each node can branch out the Ethernet frame to other devices such as LAN switches, WLAN APs or even other L2-VPNs through Ethernet bridges. So, any client (or organization) can join and expand the large-scale L2-VPN network by implementing a VPN client and creating Ethernet bridges.

2.2 Distributed Authentication

Since Ethernet frames can be transmitted through any connected node, an authentication server can be set up anywhere on the large-scale network. One PPPoE server can be connected by multiple clients and is enough for all members in an organization, and multiple PPPoE servers can co-exist without conflicts by specifying service tag of PPPoE for each server.

‡College of Information Science and Engineering,
Ritsumeikan University

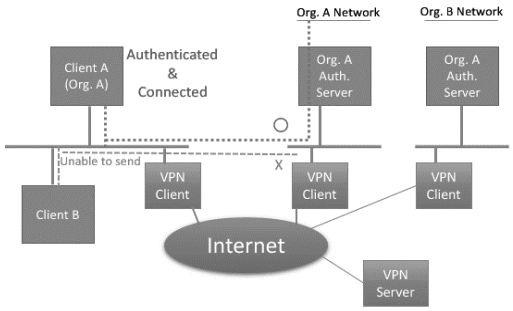

Fig. 1　IWAS Architecture

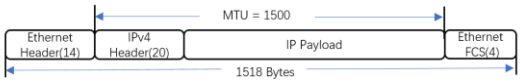

Fig. 2　Ethernet Frame in IP Network

Despite PPPoE, Layer 3 (L3, network layer in OSI model) protocols can also be used for authentication. Point-to-Point Tunneling Protocol [4] (PPTP), which can create a tunnel over IP network and supports AAA, can be used for authentication purposes. Like PPPoE, multiple PPTP servers can also co-exist if correct IP addresses are allocated. In the meanwhile, a Secure Sockets Layer VPN (SSL-VPN) like Cisco AnyConnect can also be used for more security and reliability.

3. MTU Analysis

In this implementation of the IWAS, there are three types of interface, the interface that connects to the Internet (here called the real network interface), the L2-VPN network interface, and the interface created by different authentication protocols. Thus, the MTUs must be considered separately.

Here we take the Ethernet II as our real network, and a Network Interface Card (NIC) is used to connect the Internet. Figure 2 shows an Ethernet frame in IP network.

3.1 Real Network Interface

By IEEE 802.3, the maximum length of an Ethernet frame is limited to 1518 bytes. The Ethernet header takes 14 bytes, including destination and source MAC addresses (6 bytes each), and two-octet EtherType field. Ethernet frame also has a tail called frame check sequence (FCS), which takes 4 bytes.

So, the Ethernet itself takes 18 bytes in total of the frame. The available space for IP packet will be 1518-18=1500 bytes, and the IP MTU set for real network interface should be 1500.

3.2 L2-VPN Network Using OpenVPN-UDP

OpenVPN [5] is an open-source software that implements VPN techniques to create point-to-point (L3) or site-to-site (L2) connections in routed or bridged configurations. It can encapsulate its payload into a TCP or UDP unit (often called OpenVPN-TCP or OpenVPN-UDP respectfully).

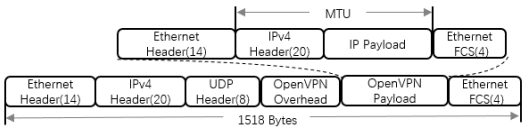

Fig. 3 OpenVPN-UDP Circumstances

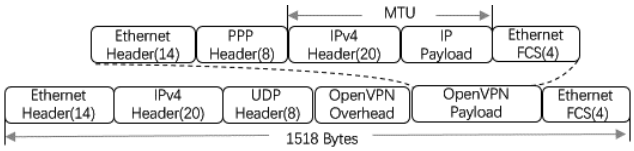

Fig. 4 PPPoE over OpenVPN-UDP

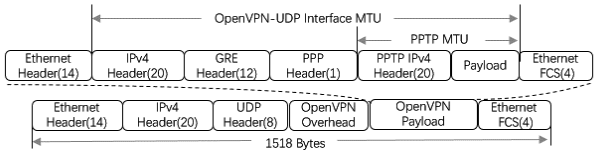

Fig. 5 PPTP over OpenVPN-UDP

In IWAS, a bridged configuration is used to create the large-scale L2 network, and the interface to the L2-VPN network is called a TAP interface. Figure 3 shows the packet structure for OpenVPN-UDP circumstances. The whole OpenVPN data is transferred in a UDP datagram, including the overhead and payload. Since a bridged configuration is used, the payload part will consist of a whole Ethernet frame (as shown in Fig. 2).

When OpenVPN runs without cipher or compression, using SHA1 as the digest algorithm (default), it takes 24 bytes of overhead (1 byte of packet tag, 3 bytes of peer id, and 20 bytes of the SHA1 signature). Now, it leaves 1448 bytes for OpenVPN payload. Since the payload consists of a whole Ethernet frame with a maximum size of 1448 bytes, the MTU for this interface will be 1430.

3.3 PPPoE Interface

As described in section 2.2 and Fig. 4, PPPoE uses PPP protocols to deliver IP packets. PPP header takes 8 bytes in PPPoE. Since the maximum PPPoE frame size is 1448 bytes, the space left for IP packet is 1422 bytes. MTU should be 1422.

3.4 PPTP Interface

Figure 5 shows the structure of a PPTP packet over OpenVPN-UDP. A PPTP tunnel should be built on an existing IPv4-capable network. Generic Routing Encapsulation (GRE) is used in PPTP to encapsulate PPP packets which include a PPTP-Tunnel IP packet. The GRE protocol takes 12 bytes while PPP header takes 1 byte in PPTP. Thus, since the frame size is up to 1448 bytes, the MTU for PPTP interface should be 1397.

4. Performance Analysis

iPerf [6] is a tool for active measurements of the maximum achievable bandwidth on IP networks which supports tuning of various parameters related to timing, buffers, and protocols (TCP, UDP, SCTP). We set up an OpenVPN server and a PPPoE server, both running CentOS 7. Cipher is disabled and SHA1 is used at the OpenVPN server. CHAP is used at the PPPoE server for authentication. A client is set up running Ubuntu 16.04. We limit the bandwidth from VPN client to VPN server to 30Mbps with 1% loss rate to simulate real network circumstances by configuring the firewall, and measure the TCP throughputs by varying the PPPoE interface MTU, and the result is as follows. TCP congestion control is cubic and the window size is 85.3 Kbytes as default. We take the average rate in 7 times test for each MTU, 10 seconds for each test. The OpenVPN internal fragmentation function is enabled only for MTU over 1422.

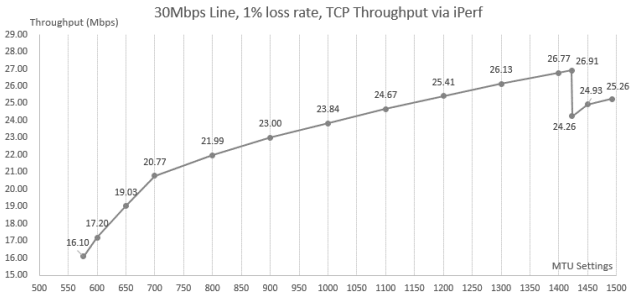

Fig. 6 TCP Throughput by varying MTU

In a 30Mbps link for the real network, theoretically, the maximum throughput for TCP is 27.3Mbps, while the maximum TCP payload is 1382 bytes. With 1% loss rate, the theoretical rate comes down to 27.04Mbps (99% of 27.3Mbps). The test starts MTU from 576 since IPv4 requires that hosts must be able to process IP datagrams of at least 576 bytes, and the throughput is 16.10Mbps. When the MTU is increased, the throughput gradually grows. The rising gets slower as MTU increases.

The maximum throughput gets 26.91Mbps when the MTU is set to 1422 as described in section 3.3. A sharp decrease occurs when MTU is 1 byte over that value (1423), with a throughput of 24.26Mbps. The throughput comes to 25.26Mbps at the maximum MTU of PPPoE, which is 1492. It is worth mentioning that, when the fragmentation function is disabled, almost no data can be sent when MTU is set over 1422.

5. Conclusions

As a summary, for IWAS, the best MTU can be decided by calculating overheads for each layer in every related interface. A correct MTU setting is significant for getting the best performance on a specific network, while oversized MTU settings might cause lower performance and application issues.

References

[1] NISHIMURA Toshikazu, “A Distributed Authentication Mechanism for Sharing an Overlay Network among Multiple Organizations”, Proceedings of IIWAS 2010, pp. 813-817, 2010.
[2] L. Mamakos, K. Lidl, J. Evarts, D. Carrel,D. Simone and R. Wheeler, “A Method for Transmitting PPP Over Ethernet(PPPoE),” RFC2516, 1999.
[3] W. Simpson, “The Point-to-Point Protocol (PPP),” RFC1661, 1994.
[4] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little and G. Zorn, “Point-to-Point Tunneling Protocol (PPTP),” RFC2637, 1999.
[5] “OpenVPN Community Software”, Available: https://openvpn.net
[6] “iPerf - The ultimate speed test tool for TCP, UDP and SCTP” Available: https://iperf.fr/.