The Role of DHCP and RADIUS in Lawful Interception

Ana M. Pavlicic, Phillip A. Branch, Grenville Armitage
Centre for Advanced Internet Architectures. Technical Report 040105A
Swinburne University of Technology
Melbourne, Australia
apavlicic@swin.edu.au, pbranch@swin.edu.au, garmitage@swin.edu.au

***Abstract* – This paper deals with the problem of identifying IP traffic to or from a user for the purposes of Lawful Interception (LI). Systems used for LI of IP traffic monitor Dynamic Host Configuration Protocol (DHCP) and Remote Authentication Dial-In User Service (RADIUS) messages to identify the IP address of packets to be intercepted. This paper identifies the key information flows between the Network Access Server (NAS) and the RADIUS and DHCP servers. It ends by suggesting directions for LI research related to user identification.**

***Keywords* –** *RADIUS, DHCP, Lawful Interception.*

I. INTRODUCTION

Lawful Interception is the process of intercepting within a network, communications between parties of interest to Law Enforcement Agencies. The interception is legally authorised and is conducted without the intercepted parties being aware of it. Law Enforcement Agencies include state and federal police, intelligence agencies and independent commissions against corruption. Lawful Interception is often referred to as 'wiretapping' or 'phone-tapping'[1].

It is little appreciated how important Lawful Interception is to the Law Enforcement Agencies. Lawful Interception is a powerful tool in criminal and security investigations. Governments throughout the world insist that before a telecommunications company can receive its operating license, it must have in place an adequate Lawful Interception system. Governments can and have delayed or cancelled the rollout of new services by telecommunications companies because they were unable to meet their Lawful Interception obligations.

Until a few years ago, Lawful Interception was the sole responsibility of the telecommunications companies. However, with the increasing popularity of the Internet and with the increasingly diverse ways that it can be accessed, interception within public access networks has become much less effective than it was. Internet cafes, public libraries, Internet kiosks and, to a lesser extent corporations and universities, all provide access to Internet services that is not easily intercepted within the access networks. Consequently, Law Enforcement Agencies have started to turn their attention towards interception of Internet services.

Internet Lawful Interception presents many technical challenges to Internet Service Providers (ISPs). One of the most fundamental and most difficult is linking identity to user traffic. Typically IP packets contain no identification, other than a dynamically allocated IP address. How can IP packets be linked to particular users?

Solutions to this problem have been developed based on sniffer systems intercepting RADIUS and DHCP traffic. RADIUS is a protocol used to authenticate username-password combinations when a client attempts to log on to the network. DHCP is a dynamic method network administrators can employ in their network architecture to simplify the allocation of IP addresses. In medium to large-scale networks, assigning IP addresses to each client computer manually is a long process, wasting valuable human and time resources. DHCP allows clients to boot up and obtain an IP address and other configuration information such as the subnet mask and default gateway in order to access resources in a network.

DHCP and RADIUS can be used in LI systems to identify a specific user that a legal warrant has been issued for. If the username-password combination being sent to the RADIUS server for validation matches that of a certain individual or group under surveillance, the LI device is able to record the IP address allocated to that client. From thereon the LI device collects all traffic to and from the identified IP address.

This paper describes a simple cable ISP configuration, using RADIUS and DHCP to illustrate typical information flows. Its purpose is to describe it in sufficient detail to enable future work to be carried out, where the robustness of current solutions can be investigated and perhaps to form a base for investigation of the whole issue of identity in the Internet.

The paper begins with an overview of RADIUS and DHCP. It then describes how the protocols are used in LI before discussing future research areas.

II. Basics Of Radius

A. *Remote Authentication Dial-In User Service*

RADIUS is a protocol used to both validate username-password combinations and keep a record of user accounting information for ISPs.

When a client attempts to log onto an ISP's network they are typically prompted for a username and password combination to establish their identity and right to use the network. A Network Access Server (NAS) must determine if the user is allowed to access the network resources. To do this it consults the RADIUS server as to whether the username and password are currently valid. The RADIUS server, with a database of users and their accounts, either validates or rejects the username-password combination and sends this information back to the NAS.

Communication between the NAS and RADIUS server occurs using UDP packets. The NAS and RADIUS server share a secret key that is used to identify and validate one to each other for communication. RADIUS supports Point-to-Point Protocol (PPP), Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) or other authentication mechanisms [2].

There is also a proxy RADIUS server mechanism. A RADIUS server is placed within a pool of servers acting as a proxy client to send username-password authorization requests to other RADIUS servers. Other authentication servers can also be used in the network to aid the RADIUS server. However, Proxy RADIUS is not covered in this paper.

B. *RADIUS Accounting*

One feature of RADIUS is its ability to keep track of user caps (amount of data users are allowed to download from the ISP network if the user is on a download plan) and billing information. This enables the ISP to identify its allocation of resources and revenue. The NAS sends the RADIUS server an Accounting-Request and the RADIUS server, if the account is valid, sends back an Accounting-Response. The time and resources used by the client are then recorded and stored in the RADIUS database at the end of a user session. Authentication and accounting can be separately employed and are not always run on the same RADIUS server.

III. Radius Message Exchange

A. *RADIUS message exchange protocol for user authentication*

When a user initialises a session on an ISP network, it is prompted by the NAS for a username-password combination. The username-password is either sent in plain text format using PAP or encrypted format using CHAP. The NAS sends an Access-Request to the RADIUS server, and if the username-password combination (and other information) is valid, the RADIUS server replies with an Access-Accept message. If the RADIUS server rejects the request it sends an Access-Reject message back to the NAS and network access is denied to the user.

The RADIUS server may choose to challenge the user at any time to reaffirm their identity and their right to use network resources by sending an Access-Challenge to the NAS. The NAS may then again prompt the user for their username-password with which the user must respond in order to retain network access. The NAS sends a new Access-Request to the RADIUS server upon the user re-submitting their username-password combination. The RADIUS server may then send another Access-Challenge, an Access-Accept or Access-Reject message to the client [3].

Any challenge messages forwarded from the NAS to the user during the session contain a random number the user machine must encrypt. The encryption is conducted by a smart card or software and requires a secret key known only by an authorised machine. The response is sent to the RADIUS server (via the NAS). The result of the encryption sent to the RADIUS server determines whether or not the user is authorized. For information on RADIUS packet fields and authentication algorithms see Appendix A.

Figure 1 shows the messages sent between the user, the NAS and RADIUS server to authenticate a user.

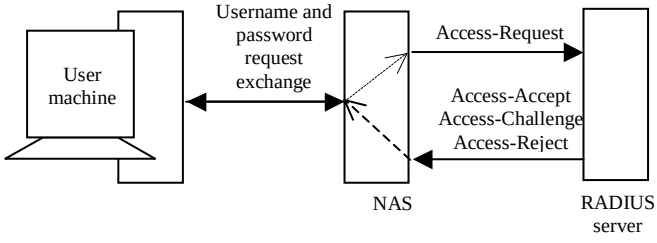

Figure 1: RADIUS user validation message flow

The RADIUS server may, in an Access-Accept message, send the user IP configuration information (including the IP address to be assigned to the end user's

machine, avoiding the need for DHCP). This usually occurs with PPP and Serial Line Internet Protocol (SLIP) connections.

IV. Basics Of DHCP

A. *Dynamic Host Configuration Protocol*

DHCP is defined in RFC 2131 [4]. This protocol was designed to be compatible with existing Bootstrap Protocol (BOOTP) systems, thus it shares much of the same packet format. DHCP is also capable of supporting BOOTP clients without any modification to these clients. UDP port 67 is reserved for DHCP servers and port 68 for clients.

DHCP provides network administrators with an easy way to distribute IP addresses and other network configuration information quickly and easily. DHCP also gives network administrators flexibility in that the pool of IP addresses may simply be a range of addresses and every time a client logs into the network a random unused address can be assigned to the client (dynamic). It can also distribute specific addresses to specific clients for permanent use (static), or allocate a random unused permanent address to a client (automatic). Other options are also available to the network administrator.

V. DHCP Message Exchange

A. *DHCP message exchange protocol for user authentication*

When a client boots up or attempts a network connection by dial-in, it must obtain a unique IP address to communicate with other nodes on the network. The first step a client takes to obtain an IP address is to broadcast a DHCPDISCOVER message using its Media Access Control (MAC) address, sometimes known as the "link layer address", as its identifier. These broadcast packets are then received by one or more DHCP servers and ignored by all other devices on the network. The DHCP server or servers reply to the DHCPDISCOVER message with a DHCPOFFER message containing the IP address it is offering to the client. The client may choose any of these offers, either based on the first offer to arrive or other factors such as the offer that has the longest IP address lease time. The client may also perform an ARP request to check that the IP address is not already in use on the network [5]. If it finds the IP address is in use, the client will send the server a DHCPDECLINE message and the server will mark the address as bad.

In reply to a DHCPOFFER a client responds directly to the DHCP server with a DHCPREQUEST acknowledging its agreement to the server's offer, again using the MAC address as its identifier. The server then either sends the client a DHCPACK containing all configuration parameters including the IP address or a DHCPNACK to deny lease (DHCPNACK may occur if a client is attempting to renew an address they previously owned and for any reason the server cannot issue them with that particular address again).

The dynamic allocation of IP addresses is on a first-come-first served basis. The first client to accept a particular configuration offer from the server where multiple packets of the same offer may be on the network will be allocated that address. Figure 2 below shows the basic flow of DHCP packets between a server and client initiating a lease on the same subnet.

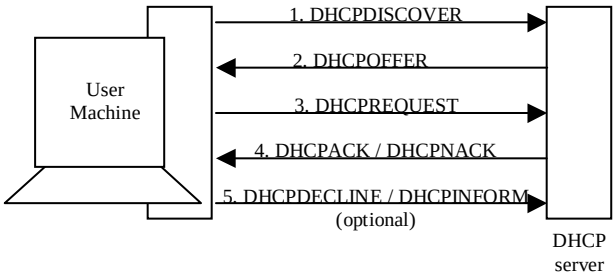

Figure 2: Basic DHCP packet flow

In the case that the DHCP server is on another subnet, the DHCPDISCOVER broadcast packet a client sends is received by a proxy device (most commonly a router) and forwarded to the DHCP server. The proxy device inserts its own IP address corresponding to the interface on which it received the DHCPDISCOVER as the source address. As the packet passes through the proxy device it increments the hop count from 0 to 1 so that the DHCP server knows the client resides on another subnet. In this way the DHCP server can send DHCPOFFER packets to the proxy device and they will not be discarded, but forwarded on to the client. This process is repeated for the DHCPREQUEST and response.

To renew a dynamic lease the client sends a DHCPDISCOVER message and the process repeats. The client will usually (but not always) request the allocation of the same IP address. If a graceful shutdown of the client is performed it sends the DHCP server a DHCPRELEASE packet to indicate the server should release the IP address so that other clients may obtain it. If the shutdown was not graceful, the IP address is released once the lease time has expired. The DHCP server does not send packets to the client to acknowledge the release of an IP address, since it assumes the client has already shutdown.

At any time a client may send the server a DHCPINFORM packet to request information regarding local configuration parameters [6].

The DHCP server keeps a list of all IP addresses that are available to be offered to potential clients. It also keeps a list of IP addresses it has assigned to computer interfaces and an identifier such as their MAC address. The DHCP server may or may not have a registered list of MAC addresses of computers for which it is to allocate IP addresses. For information on DHCP packet fields see Appendix B.

VI. RADIUS AND DHCP IN LAWFUL INTERCEPTION

A. *Incorporating RADIUS and DHCP with an interception device.*

There is currently no standard specifying where LI devices are placed within a network to monitor traffic. Each ISP or enterprise has a different physical and logical structure and uses IP protocols and communications technologies in different ways. There are many models that could be implemented for LI, each with its own advantages and disadvantages. This paper will describe a typical model for cable modem traffic interception.

RADIUS and DHCP are used in LI since they deal with the identities of network users. RADIUS 'knows' who is using the network (and possibly their allocated IP address if it has assigned it to user) and DHCP 'knows' the IP addresses it has allocated. Authorities can pinpoint their target then collect all packets associated with the user based on the IP address allocated to that user via either RADIUS or DHCP. Note that other variables such as MAC address, NT username, 802.1Q VLAN tag or a combination of these may also be used to monitor traffic [6].

When a warrant is issued by an authority to intercept the traffic of a particular user or group of users, an ISP is required to provide resources to fulfil that warrant. All ISPs have records containing personal information of their customers such as their name, address, phone number and can naturally access the particular user's username.

A schematic diagram of a theoretical cable interception model utilising both RADIUS and DHCP that is analysed in this paper is shown in Figure 3. Other protocols may be used for this task but this paper focuses only on RADIUS and DHCP. The authentication protocol used between the user and the NAS is either standard, such as PAP and CHAP, or proprietary.

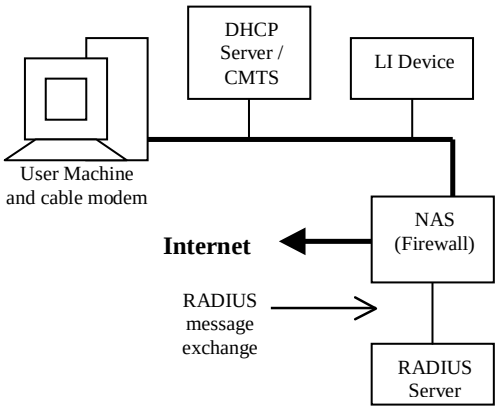

Figure 3: LI in a simplified ISP network architecture

When a user's computer boots up it broadcasts a DHCPDISCOVER packet onto the network and obtains an IP address from a DHCP server. The user is unable to access network resources beyond the NAS at this time since the firewall will not permit packets with this IP address to pass through. It could, however, communicate with local devices. The NAS consults the RADIUS server with the username-password combination of this user and either allows or denies them access based upon the authorisation results. If the user is granted access, the Firewall allows the IP address to pass onto the network.

An LI device placed between the DHCP server and NAS reads all usernames sent to the NAS for authentication and the IP address their computers have obtained. The LI device needs to have the ability to read the username and password in the authentication protocol transmitted between the user and the NAS. It would also need to have all encryption keys in order to decrypt the packets. The type of authentication protocol used depends on the ISP's particular preference. When the LI device detects packets belonging to the specific user whose packets it is to intercept, the LI device records their IP address and begins monitoring all communications to and from this IP address.

Note that if PPP is used the IP address is allocated by RADIUS, whereas with cable modem connections a DHCP server may have allocated it before authentication occurred. In the case of PPP, the LI device would detect and record the IP address allocated to the user via the RADIUS server as it reads authentication messages between the user and the NAS. It would then proceed to monitor the user.

The cable access process is described in Figure 4.

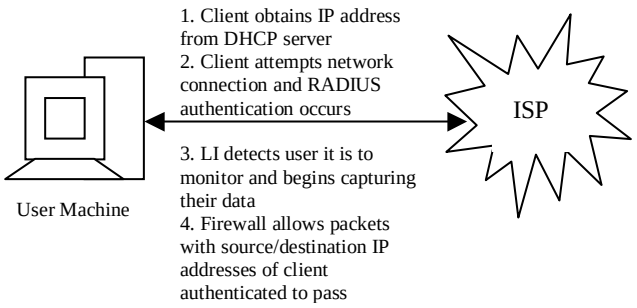

Figure 4: Basic system operation flow

The RADIUS server regularly sends challenges to the user via the NAS and in doing so the LI device can keep track of the IP address the user is associated with. In the event that the user has disconnected and another user has obtained their IP address, the LI device detects that, during the authentication, this IP address no longer belongs to the target user and stops intercepting packets associated with the IP address.

When the target user obtains another IP address, the LI device detects this when a username-password authentication takes place. The LI device registers a new IP address with the user it is monitoring and begins intercepting packets with this new IP address. The LI device stops tracking the user's packets once the warrant has expired.

The LI device may store all intercepted data in its memory cache to be downloaded to the authorities or the data may be sent directly to the law enforcement agency. The user is never aware they are being monitored. A good LI device merely copies all target packets as they pass along the network, so that no packets are ever lost due to its interaction.

It is possible that a user machine may have two or more IP addresses or that a user may be connected to the network on two or more machines. As a result, the LI device continue searching for the username-password combination of the user being sent to the NAS, even while monitoring that same user's traffic.

The RADIUS server may contain scripts that can be edited to monitor traffic. A script running on the server reads all usernames that require authentication. Once the target username is found in an Access-Request message all packets to and from this user to the RADIUS server are copied.

VIII. Conclusion

RADIUS and DHCP are established protocols that are used by current LI systems. Their role in ISP user validation and configuration distribution has been taken advantage of and incorporated into LI. The messages exchanged between the user, DHCP server, NAS and RADIUS server enable law enforcement agencies to identify a target user and their configuration information. In this manner they are able to monitor network users for whose traffic they have a legal warrant.

This paper is intended to provide a foundation for research into LI. Further work following on from this paper will involve investigating the robustness or otherwise of the use of RADIUS and DHCP in LI. In particular, investigations will be carried out into identifying under what circumstances the mechanism can fail, how easy it is to subvert it and how it can be made more robust. Different ISP architectures and different RADIUS and DHCP configurations will be investigated.

Lawful Interception has often attracted negative publicity because of public suspicion of the way in which it has the potential to be carried out. It is quite simple to place a device in a network and monitor packets, but another matter to ensure the packets that are intercepted belong only to an individual or group for which there is a legal basis to monitor. One of the many challenges for Internet LI is to ensure that only those packets for which there is a legal warrant, and no others, are obtained and used by authorities. We intend that this work will further that goal.

References

[1] Phillip A. Branch, "Lawful Interception of the Internet", Centre for Advanced Internet Architectures Technical Report 030606A, Swinburne University of Technology, June, 2003

[2] How does RADIUS work? Cisco Systems, Inc.

http://www.cisco.com/warp/public/707/32.html, February 13, 2003

[3] Carl Rigney, Allan C. Rubens, William Allen Simpson, Steve Willens, RFC 2865, "RFC 2865 - Remote Authentication Dial In User Service (RADIUS)", Internet RFC/STD/FYI/BCP Archives, http://www.faqs.org/rfcs/rfc2865.html, June, 2000

[4] Ralph Droms, "RFC 2131 – Dynamic Host Configuration Protocol", Internet RFC/STD/FYI/BCP Archives, http://www.faqs.org/rfcs/rfc2131.html, March, 1997

[5] Eric A. Hall, "How DHCP Works", http://www.ehsco.com/reading/19960515ncw3.html,

May 15, 2003

[6] CITADEL Interception Technologies, "White Paper on Xaminer IP", http://www.citadelsecurix.com/pdf/xaminer/Xaminer_whitepaper.pdf, (as of December, 2003)

[7] Joshua Hill, "An Analysis of the RADIUS Authentication Protocol", InfoGard Laboratories, http://www.untruth.org/~josh/security/radius/radius-auth.html, November 24, 2001

[8] Ralph Droms, Ph.D., and Ted Lemon, "The DHCP Handbook, Understanding, Deploying, and Managing Automated Configuration Services", Macmillan Technical Publishing, 1999

APPENDIX A – RADIUS MESSAGE FORMAT

The following Figure represents the RADIUS data format:

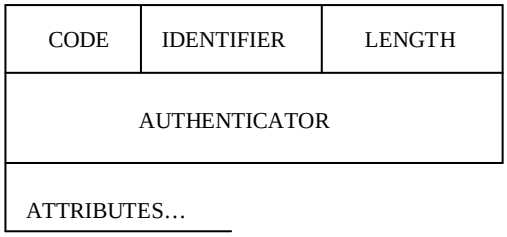

Figure 1: RADIUS packet data

The 'Code' field (8 bits) determines the type of message being sent. The value in this field is set to one of the following:

Code	Message
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Table 1: RADIUS packet codes

The 'Identifier' field (8 bits) is a way of keeping track of the specific conversation between the client and the server. The 'Length' field (16 bits) is simply the length of the packet that must be within a certain range to be valid. The 'Attributes' field contains all data such as the username and password of the user.

The 'Authenticator' field (16 bytes) contents depend on whether the packet is being sent by the client or the server. In Access-Request packets (also know as the Request Authenticator) sent by the client, the Authenticator field contains a secret value (S) shared by both the RADIUS server and NAS client that is added to a pseudo-random 128-bit Request Authenticator number (RA). The resulting value is then hashed using MD5. The first 16 bytes of the user password (P1) are XOR-ed with the MD5 hash result. If the password is longer than the 16 bytes, the remaining part(s) of the password are broken down into 16 byte blocks (Pn) and undergo the same process as shown in the following formulae [7]:

C1 = P1 XOR MD5(S + RA) first 16 bytes

C2 = P2 XOR MD5(S + C1) next 16 bytes

and so on so that

Cn = Pn XOR MD5(S + Cn-1)

In Access-Accept, Access-Challenge and Access-Reject (these packets are collectively known as the Response Authenticators) sent by the RADIUS server, the result of the following calculation is found in the Authenticator field:

MD5(Code + Identifier + Length + Request Authenticator + Attributes + Secret)

Upon reception of a Response Authenticator, the client (NAS) compares the value in the Identifier field with any requests pending. If the Identifier field value in the Response Authenticator packet matches that of a Request Authenticator it sent, the client checks the Authenticator value of that packet with its own calculation of the Authenticator field to determine the validity of the packet. If at any stage the client finds a mis-match it discards the packet and does not inform the RADIUS server. If the packet checks out and the message is an Access-Accept, the NAS allows the user to access network resources.

Figure 2 shows the Request and Response Authenticator packet flow:

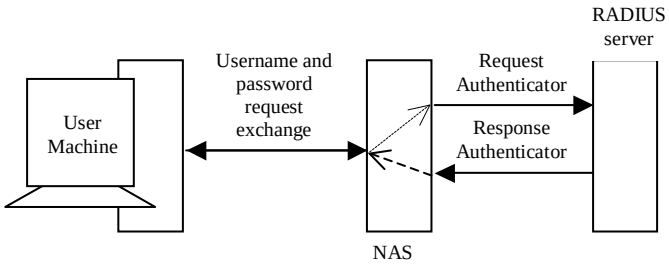

Figure 2: Request and Response Authenticator

APPENDIX B – DHCP MESSAGE FORMAT

The following Figure illustrates DHCP packet fields:

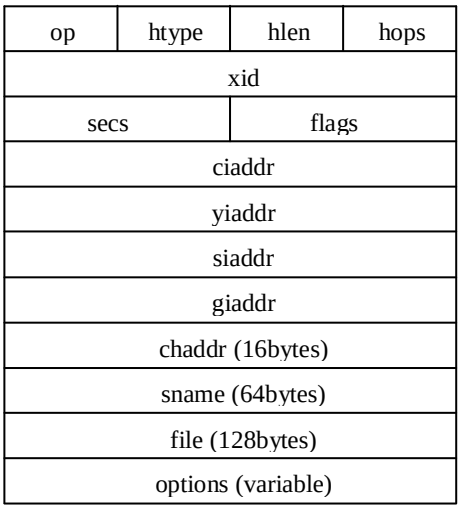

Figure 1: DHCP fields

Table 2 explains the role of the fields in a DHCP packet.

Field	Bytes	Description
op	1	1=BOOTREQUEST 2=BOOTREPLY message
hype	1	Hardware address type
hlen	1	Hardware address length
hops	1	Client=0, used by proxy devices
xid	4	Transaction ID – random number to identify a conversation
secs	2	Seconds since client initiated contact
flags	2	Flags
ciaddr	4	Client IP address when in BOUND, RENEW or REBINDING state
yiaddr	4	Client IP address
siaddr	4	IP address of next server
giaddr	4	Proxy device IP address
chaddr	16	Client hardware address
sname	64	Optional server host name
file	128	Boot file name
options	var	Optional parameters

Table 1: DHCP fields

The 'option' field determines the type of message that is being sent. Each Option contains an 'option code', 'option length' and 'option data' sub field. The option code sub field determines the Option field format. The option length sub field specifies the length of the option data that is to be received by either the client or server. This value is set between 312 bytes to 576 bytes and can be negotiated. The option data is the actual information being sent by the packet. This includes the 'message type' Option that specifies to the receiver the type of message. Table 3 shows the message type and values that are found in the 'option data' field for the message type Option [8]. This Option is used in every DHCP message as it identifies to the receiver the purpose of the message. Other Options include the 'subnet mask' option, 'router' option, and 'end' option.

Message Type	Option Value
DHCPDISCOVER	1
DHCPOFFER	2
DHCPREQUEST	3
DHCPDECLINE	4
DHCPACK	5
DHCPNACK	6
DHCPRELEASE	7
DHCPINFORM	8

Table 2: Message type option data values