Network Working Group
Request for Comments: 3203
Category: Standards Track

Y. T'Joens
C. Hublet
Alcatel
P. De Schrijver
Mind

December 2001

DHCP reconfigure extension

Status of this Memo

Copyright Notice

Abstract

This document defines extensions to DHCP (Dynamic Host Configuration Protocol) to allow dynamic reconfiguration of a single host triggered by the DHCP server (e.g., a new IP address and/or local configuration parameters). This is achieved by introducing a unicast FORCERENEW message which forces the client to the RENEW state. The behaviour for hosts using the DHCP INFORM message to obtain configuration information is also described.

1. Introduction

The procedures as described within this document allow the dynamic reconfiguration of individual hosts.

1.1 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. DHCP force renew

This section describes the FORCERENEW message extension.

2.1 Terminology

DHCP client : host to be reconfigured using DHCP.

DHCP server : server which configured the DHCP client.

2.2 Force renew procedures

The DHCP server sends a unicast FORCERENEW message to the client. Upon receipt of the unicast FORCERENEW message, the client will change its state to the RENEW state, and will then try to renew its lease according to normal DHCP procedures. If the server wants to assign a new IP address to the client, it will reply to the DHCP REQUEST with a DHCP NAK. The client will then go back to the init state and broadcast a DHCP DISCOVER message. The server can now assign a new IP address to the client by replying with a DHCP OFFER. If the FORCERENEW message is lost, the DHCP server will not receive a DHCP REQUEST from the client and it should retransmit the FORCERENEW message using an exponential backoff algorithm. Depending on the bandwidth of the network between server and client, the server should choose a delay. This delay grows exponentially as retransmissions fail. The amount of retransmissions should be limited.

The procedures described above assume the server to send a unicast FORCERENEW message to the client. Receipt of a multicast FORCERENEW message by the client should be silently discarded.

It can be that a client has obtained a network address through some other means (e.g., manual configuration) and has used a DHCP INFORM request to obtain other local configuration parameters. Such clients should respond to the receipt of a unicast FORCERENEW message with a new DHCP INFORM request so as to obtain a potential new set of local configuration parameters. Note that the usage of these procedures are limited to the set of options that are eligible for configuration by DHCP and should not override manually configured parameters.

Note further that usage of the FORCERENEW message to reconfigure a client address or local configuration parameters can lead to the interruption of active sessions, and that as such these procedures should be used in controlled circumstances.

2.3 Example usage

2.3.1 Embedded DHCP clients

The autoconfiguration of home gateways (more generically Network Termination equipment) for public networking purposes can be achieved through means of DHCP, as described in [DSL_autoconf]. In order to allow service changes or service interruption, the FORCERENEW message can trigger the home gateway to contact the DHCP server, prior to the expiry of the lease.

2.3.2 Hospitality service scenario

In self provisioned networks, e.g., hotel rooms, the hotel owned DHCP server can hand out limited use IP addresses, that allows the customer to consume local services or select external services from a web browser interface. In order to allow external services through other service providers, e.g., global internet services or enterprise VPN services, the DHCP server can trigger the client to ask for a new DHCP initialization session so as to obtain e.g., a globally routed IP address.

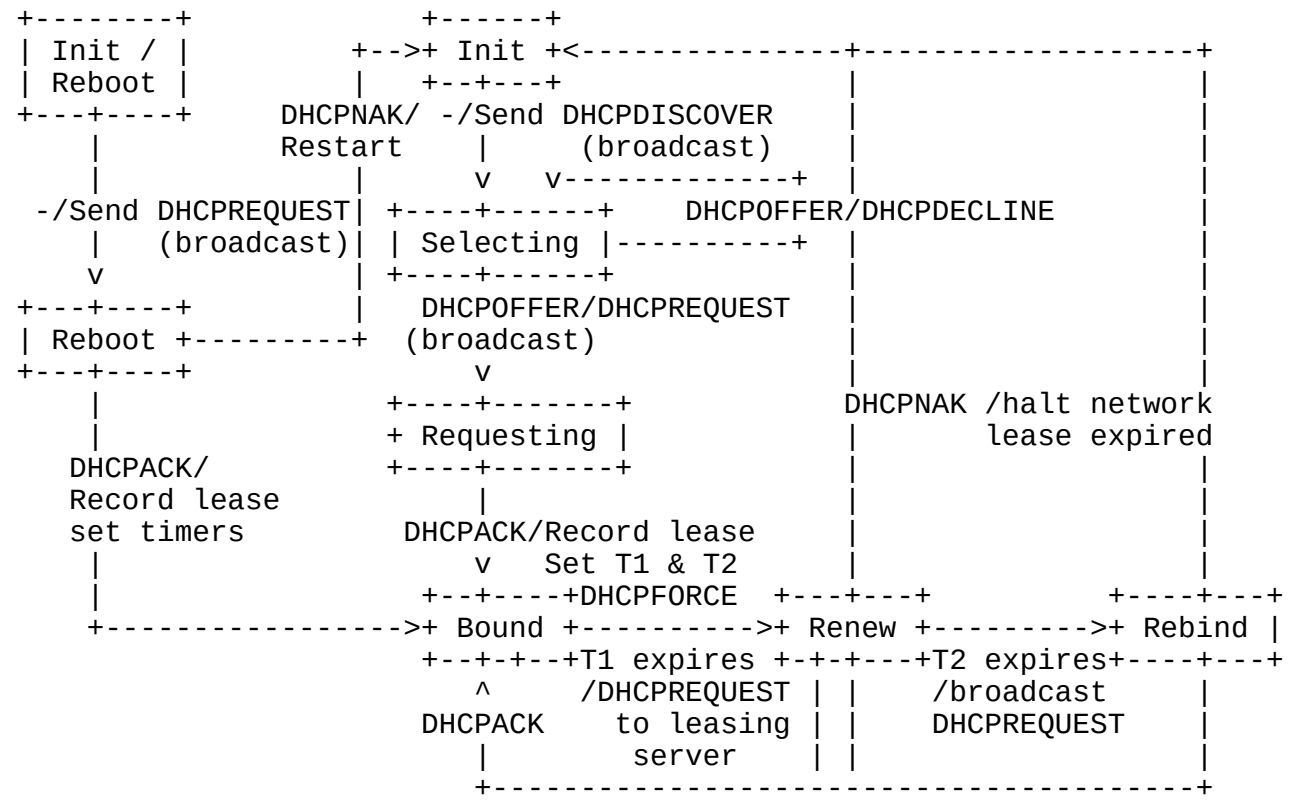
2.3.3 Network renumbering

Under tightly controlled conditions, the FORCERENEW procedures can be used to brute force the renumbering of entire subnets, client per client, under control of a DHCP server.

2.4 Rationale

The approach as described in this document has a number of advantages. It does not require new states to be added to the DHCP client implementation. This minimizes the amount of code to be changed. It also allows lease RENEWAL to be driven by the server, which can be used to optimize network usage or DHCP server load.

3. Extended DHCP state diagram



4. Message layout

The FORCERENEW message makes use of the normal DHCP message layout with the introduction of a new DHCP message type. DHCP option 53 (DHCP message type) is extended with a new value: DHCPFORCERENEW (9)

5. IANA Considerations

The new value for DHCP option 53 (DHCP message type) to indicate a DHCPFORCERENEW message is 9.

6. Security Considerations

As in some network environments FORCERENEW can be used to snoop and spoof traffic, the FORCERENEW message MUST be authenticated using the procedures as described in [DHCP-AUTH]. FORCERENEW messages failing the authentication should be silently discarded by the client.

6.1 Protocol vulnerabilities

The mechanism described in this document is vulnerable to a denial of service attack through flooding a client with bogus FORCERENEW messages. The calculations involved in authenticating the bogus FORECERENEW messages may overwhelm the device on which the client is running.

7. References

[DHCP] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[DHCP-AUTH] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[DSL_autoconf] Technical Report TR-044, "Auto-Configuration for Basic Internet (IP-based) Services", DSL Forum, November 2001

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8. Acknowledgements

The authors would like to thank David Allan, Nortel, for the constructive comments to these procedures.

9. Authors' Addresses

Yves T'joens
Alcatel Network Strategy Group
Francis Wellesplein 1, 2018 Antwerp, Belgium
Phone: +32 3 240 7890
EMail: yves.tjoens@alcatel.be

Peter De Schrijver
Mind NV
Vaartkom 11
3000 Leuven
EMail: p2@mind.be

Alcatel Broadband Networking Division
Veldkant 33b, 2550 Kontich, Belgium
Phone: +32 3 450 3322
EMail: Christian.Hublet@alcatel.be

10. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.