Network Working Group
Request for Comments: 3495
Category: Standards Track

B. Beser
Juniper Networks
P. Duffy, Ed.
Cisco Systems

March 2003

Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration

Status of this Memo

Copyright Notice

Abstract

This document defines a Dynamic Host Configuration Protocol (DHCP) option that will be used to configure various devices deployed within CableLabs architectures. Specifically, the document describes DHCP option content that will be used to configure one class of CableLabs client device: a PacketCable Media Terminal Adapter (MTA). The option content defined within this document will be extended as future CableLabs client devices are developed.

Table of Contents

1. Conventions used in this document

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 BCP 14, RFC 2119 [1].

2. Terminology

Definitions of terms used throughout this document:

* "Telephony Service Provider" or "TSP"

The business entity from which a subscriber receives telephony service.

See RFC 2131 [6] for additional DHCP terminology.

3. Introduction

Cable Television Laboratories, Inc. (CableLabs) is a non-profit research and development consortium that serves the cable television industry via design and specification of new and emerging broadband service architectures. Several CableLabs initiatives define DHCP clients that have specific DHCP configuration requirements. One such initiative is the PacketCable project.

The PacketCable project is aimed at architecting, qualifying, and supporting Internet-based multimedia services over cable-based packet networks. These new multimedia services will include telephony and videoconferencing, delivered using the basic Internet Protocol (IP) technology that is used to send data via the Internet.

PacketCable 1.0 provides Voice over IP (VoIP) service delivery. The VoIP service is supported at the customer site by two key components: a Cable Modem (CM) and a Media Terminal Adapter (MTA). The CM converts the cable RF signals to/from various IP voice protocols, while the MTA converts the VoIP protocols into analog telephony compatible with a common telephone.

The CM and MTA may be packaged together or separately. If packaged together, the unit is referred to as an Embedded-MTA (EMTA - depicted in Figure 1). If packaged separately, the MTA is referred to as a Standalone MTA (SMTA).

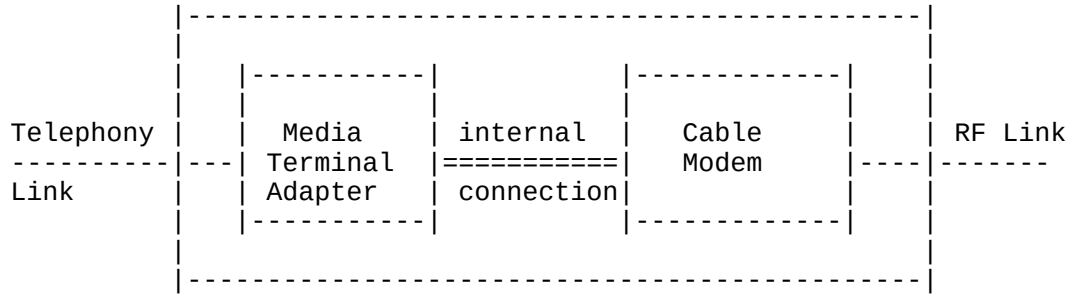


Figure 1. PacketCable 1.0 Embedded-MTA

The CM and MTA are distinct IP devices: each has its own MAC address and IP configuration. The CM and MTA utilize the DHCP protocol to obtain IP configuration. It is assumed that the CM and MTA may be administered by different business entities. The CM communicates with and is configured by the Data Access Provider's (DAP's) DHCP servers. Likewise, the MTA communicates with and is configured by the Telephony Service Provider's (TSP's) DHCP servers.

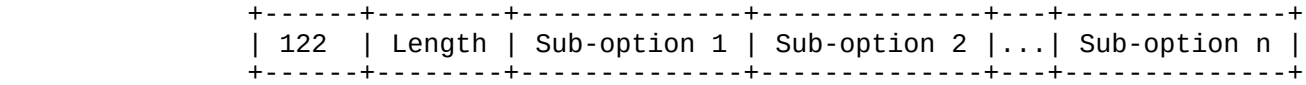
The PacketCable architecture requires that the business entity controlling the configuration of the CM also determines which business entities control the configuration of the MTA. This is similar to the example found in the PSTN system: individuals can pick their long distance carriers even though the ultimate control of their telephone remains with the local carrier.

Due to specific needs of the MTA configuration process (described in [7]), a new CableLabs Client Configuration (CCC) option is needed for the DHCP protocol. Both CM and MTA DHCP clients will request this option. When requested, both the DAP and TSP DHCP servers will populate this option into DHCP responses. See section 6 for further operational details.

It should be noted that, although the CCC option will be initially deployed to support PacketCable VOIP applications, the CCC option will also be used to support various non VOIP applications. Use of the CCC option does not necessarily mean that the service provider is a TSP.

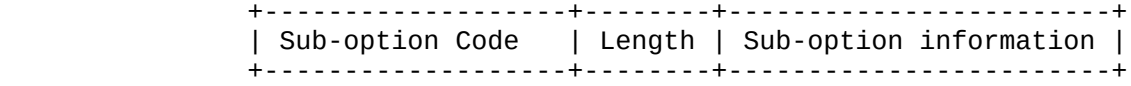
4. CableLabs Client Configuration Option Format

The option begins with a tag octet containing the option code (code 122). A length octet follows the tag octet. The value of the length octet does not include itself or the tag octet. The length octet is followed by "length" octets of sub-option content (total length, not sub-option count). The option layout is depicted below:



When the total length of a CCC option exceeds 255 octets, the procedure outlined in [4] MUST be employed to split the option into multiple, smaller options.

A sub-option begins with a tag octet containing the sub-option code. A length octet follows the tag octet. The value of the length octet does not include itself or the tag octet. The length octet is followed by "length" octets of sub-option information. The sub-option layout is depicted below:



The sub-option codes are summarized below.

Sub-option Code	Sent to	Description
1	CM	TSP's Primary DHCP Server Address
2	CM	TSP's Secondary DHCP Server Address
3	MTA	TSP's Provisioning Server Address
4	MTA	TSP's AS-REQ/AS-REP Backoff and Retry
5	MTA	TSP's AP-REQ/AP-REP Backoff and Retry
6	MTA	TSP's Kerberos Realm Name
7	MTA	TSP's Ticket Granting Server Utilization
8	MTA	TSP's Provisioning Timer Value
9 - 255		Reserved for future extensions

5. CableLabs Client Configuration Option: Sub-Option Definitions

The following sections provide detailed descriptions of each sub-option. There are a few general formatting rules:

- Fully Qualified Domain Names (FQDNs) MUST be encoded per RFC 1035 [3] section 3.1. Note that a terminating 0 is required. Also note that compression, as described in RFC 1035 [3] section 4.1.4, MUST NOT be applied.

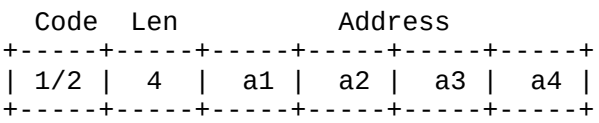
- IPv4 addresses MUST be encoded as 4 binary octets in network byte-order (high order byte first).

- All multi-octet quantities MUST be encoded per network byte-ordering.

5.1. TSP's DHCP Server Address Sub-Options

The TSP DHCP Server Address sub-options identify the DHCP servers from which an MTA is permitted to accept a DHCP OFFER. Sub-option 1 is the address of the TSP's primary DHCP server. Sub-option 2 is the address of the TSP's secondary DHCP server.

The sub-option length MUST be 4 and the sub-option MUST include the DHCP server's IPv4 address as follows:

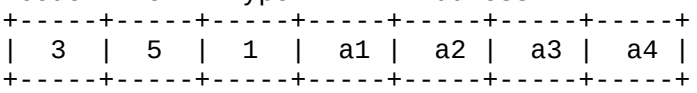


5.2. TSP's Provisioning Server Address Sub-Option

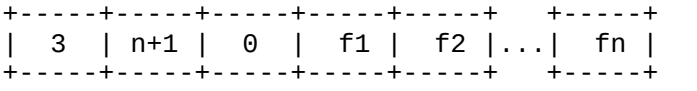
This option contains the address of the TSP's Provisioning server. MTAs communicate with the Provisioning server at various stages in their provisioning process.

The address can be configured as either an IPv4 address or as an FQDN. The encoding of sub-option 3 will adhere to one of 2 formats.

1. IPv4 address. The sub-option length MUST be 5. The length octet MUST be followed by a single octet that indicates the specific address type that follows. This type octet MUST be set to 1 to indicate an IPv4 address. The type octet MUST be followed by 4 octets of IPv4 address:



2. FQDN. The length octet MUST be followed by a single octet that indicates the specific address type that follows. This type octet MUST be set to 0 to indicate an FQDN. The type octet MUST be followed by the encoded FQDN:



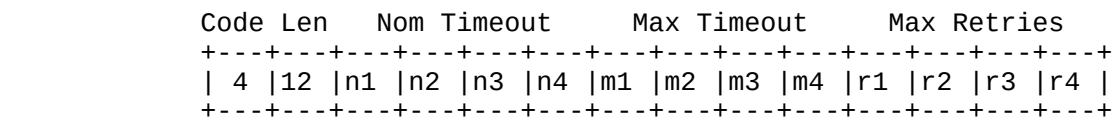
It is not anticipated that additional type codes, beyond IPv4 (1) and FQDN (0), will be required. Thus, IANA will not be required to maintain a registry of type codes.

5.3. TSP's AS-REQ/AS-REP Backoff and Retry

This sub-option configures an MTA's Kerberos AS-REQ/AS-REP timeout, backoff, and retry mechanism.

RFC 1510 [5] does not define a backoff/retry mechanism to be employed when an AS-REQ/AS-REP message exchange fails. This sub-option contains parameters required by the backoff/retry mechanism outlined in [8].

The encoding of this sub-option is depicted below:



The length octet of this sub-option MUST contain the value 12.

The length octet MUST be followed by 4 octets containing the AS-REQ/AS-REP nominal (initial) timeout value. This value is a 32 bit unsigned quantity in units of milliseconds.

The next 4 octets MUST contain the AS-REQ/AS-REP maximum timeout value. This value is a 32 bit unsigned quantity in units of seconds.

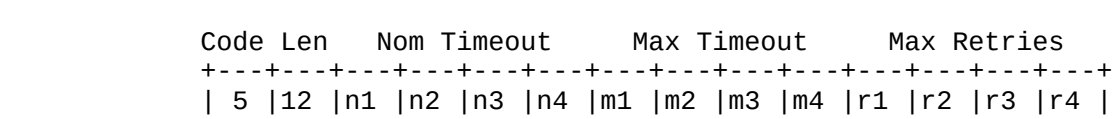
The final 4 octets MUST contain the AS-REQ/AS-REP maximum retry count. This value is a 32 bit unsigned quantity.

5.4. TSP's AP-REQ/AP-REP Backoff and Retry

This sub-option configures an MTA's Kerberos AP-REQ/AP-REP timeout, backoff, and retry mechanism.

RFC 1510 [5] does not define a backoff/retry mechanism to be employed when an AP-REQ/AP-REP message exchange fails. This sub-option contains parameters required by the backoff/retry mechanism outlined in [8].

The encoding of this sub-option is depicted below:



The length octet of this sub-option MUST contain the value 12.

The length octet MUST be followed by 4 octets containing the AP-REQ/AP-REP nominal (initial) timeout value. This value is a 32 bit unsigned quantity in units of seconds.

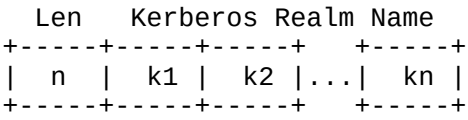
The next 4 octets MUST contain the AP-REQ/AP-REP maximum timeout value. This value is a 32 bit unsigned quantity in units of seconds.

The final 4 octets MUST contain the AP-REQ/AP-REP maximum retry count. This value is a 32 bit unsigned quantity.

5.5. TSP's Kerberos Realm Name Sub-Option

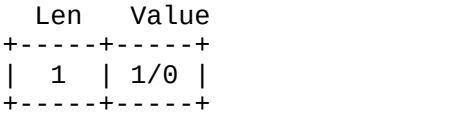
The PacketCable architecture requires an MTA to authenticate itself to the TSP's network via the Kerberos protocol. A Kerberos Realm name is required at the MTA to permit a DNS lookup for the address of the TSP's Kerberos Key Distribution Center (KDC) entity.

The Kerberos Realm name MUST be encoded per the domain style realm name described in RFC 1510 [5]. This realm name MUST be all capital letters and conform to the syntax described in RFC 1035 [3] section 3.1. The sub-option is encoded as follows:



5.6. TSP's Ticket Granting Server Utilization Sub-Option

This sub-option encodes a boolean value which indicates whether an MTA should or should not utilize a TGT (Ticket Granting Ticket) when obtaining a service ticket for one of the PacketCable application servers. The encoding is as follows:



The length MUST be 1. The last octet contains a Boolean value which MUST be either 0 or 1. A value of 1 MUST be interpreted as true. A value of 0 MUST be interpreted as false.

5.7. TSP's Provisioning Timer Sub-Option

The provisioning timer defines the maximum time allowed for the MTA provisioning process to complete. If this timer expires before the MTA has completed the provisioning process, the MTA should reset the timer and re-start its provisioning process from the beginning.

The sub-option length MUST be 1. The value octet specifies 0 to 255 minutes. A value of 0 means the timer MUST be disabled.

Code	Len	Value
8	1	(0..255)

6. Informational Description of CCC Option Usage.

Cablelabs client devices issue DHCP requests that include DHCP options 55 (Parameter Request List) and 60 (Vendor Class Identifier). Option 55 will request the CCC option from the DHCP server. Option 60 will indicate the specific Cablelabs client device type, thus directing the DHCP server to populate specific CCC sub-option content in its responses. The details of which CCC sub-options are populated for each specific client type are specified in various Cablelabs project specifications. For example, specific usage of the CCC option for the PacketCable project is described in [7].

Note that client devices never populate the CCC option in their DHCP requests.

7. IANA Considerations

IANA has assigned a value of 122 for the DHCP option code described in this document.

8. Legacy Use Information

The CableLabs Client Configuration option initially used the site-specific option value of 177 (0xB1). The use of the site-specific option is to be deprecated now that IANA has issued an official option number.

9. Procedure for Adding Additional Sub-options

IANA is requested to maintain a new number space of "CableLabs Client Configuration Sub-options", located in the BOOTP-DHCP Parameters Registry (http://www.iana.org/assignments/bootp-dhcp-parameters). The initial sub-option codes are described in section 4 of this document.

IANA is requested to register codes for future CableLabs Client Configuration Sub-options via an "IETF Consensus" approval policy as described in RFC 2434 [2].

10. Security Considerations

Potential exposures to attack in the DHCP protocol are discussed in section 7 of the DHCP protocol specification [6] and in Authentication for DHCP Messages [9].

The CCC option can be used to misdirect network traffic by providing incorrect DHCP server addresses, incorrect provisioning server addresses, and incorrect Kerberos realm names to a Cablelabs client device. This misdirection can lead to several threat scenarios. A Denial of Service (DoS) attack can result from address information being simply invalid. A man-in-the-middle attack can be mounted by providing addresses to a potential snooper. A malicious TSP can steal customers from the customer selected TSP, by altering the Kerberos realm designation.

These threats are mitigated by several factors.

Within the cable delivery architecture required by PacketCable, the DHCP client is connected to a network through a cable modem and the CMTS (head-end). The CMTS is explicitly configured with a set of DHCP servers to which DHCP requests are forwarded. Further, a correctly configured CMTS will only allow downstream traffic from specific IP addresses/ranges.

Assuming that server addresses and Kerberos realm name were successfully spoofed to the point that a malicious client device was able to contact a KDC, the client device must still present valid certificates to the KDC before being service enabled. Given the computational overhead of the certificate validation process, this situation could present a DoS opportunity.

Finally, it is possible for a malicious (although certified) TSP to redirect a customer from the customer’s selected TSP. It is assumed that all TSP’s permitted onto an access providers network are trusted entities that will cooperate to insure peaceful coexistence. If a TSP is found to be redirecting customers, this should be handled as an administrative matter between the access provider and the TSP.

11. References

11.1. Normative References

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

[2] Narten, N. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[3] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

[4] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002.

[5] Kohl, J. and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

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

11.2. Informative References

[7] "PacketCable MTA Device Provisioning Specification", PKT-SP-PROV-I05-021127. http://www.packetcable.com/specifications.html

[8] "PacketCable Security Specification", PKT-SP-SEC-I07-021127, http://www.packetcable.com/specifications.html

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

12. Acknowledgments

The authors would like to extend a heartfelt thanks to all those who contributed to the development of the PacketCable Provisioning specifications:

Sumanth Channabasappa (Alopa Networks); Angela Lyda, Rick Morris, Rodney Osborne (Arris Interactive); Steven Bellovin and Chris Melle (AT&T); Eugene Nechamkin (Broadcom); John Berg, Maria Stachelek, Matt Osman (CableLabs); Klaus Hermanns, Azita Kia, Michael Thomas, Paul Duffy (Cisco); Deepak Patil (Com21); Jeff Ollis, Rick Vetter (General Instrument/Motorola); Roger Loots, David Walters (Lucent); Peter Bates (Telcordia); Patrick Meehan (Tellabs); Satish Kumar, Itay Sherman, Roy Spitzer (Telogy/TI), Aviv Goren (Terayon); Prithivraj Narayanan (Wipro).

The authors would also like to extend a special "thank you" to Rich Woundy (Comcast) for his thoughtful inputs.

13. Authors' Addresses

Burcak Beser
Juniper Networks
1194 North Matilda Avenue
Sunnyvale, CA, 94089

EMail: burcak@juniper.net

Paul Duffy
Cisco Systems
300 Apollo Drive
Chelmsford, MA, 01824

EMail: paduffy@cisco.com

14. Full Copyright Statement

Acknowledgement

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