Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

TR-069 and DHCP based automated ACS configuration to Residential Gateways

Amey Deshpande

Sr. Cloud Delivery Manager
Calix Inc.
McKinney, TX, USA
amey2612@gmail.com

Abstract:
Broadband Service Providers (BSP) are often tasked with provisioning initial configuration on Residential Gateway (RG) devices before deploying them out in subscriber premises. This becomes a strong use case for an automated approach for provisioning Auto Configuration Server (ACS) information to Customer Premises Equipment (CPE) devices using the TR-069 protocol and Dynamic Host Control Protocol (DHCP) options. Manual configuration of ACS credentials on each device is inefficient and error-prone in large networks. The emphasis in on how the DHCP Vendor Class Identifier (Option 60) and Vendor Specific Information (Option 43) can be leveraged to automatically deliver the ACS URL and related parameters to CPEs during DHCP address assignment. This method enables zero-touch provisioning of devices, ensuring they are configured with the correct ACS settings upon connection to the network. The TR-069 framework, the role of the ACS, the mechanism of DHCP Options 43/60 for ACS URL discovery, and the automation as part of the process of a BSP addresses scalability and deployment efficiency.

Keywords: TR-069, DHCP, ACS, Router.

I. INTRODUCTION

The proliferation of Internet access devices (e.g., routers, modems, IoT gateways) has made remote management essential for Internet Service Providers (ISPs) and network operators. Technical Report 069 (TR-069) [1] defines the CPE WAN Management Protocol (CWMP), a standardized mechanism for communication between a CPE and an Auto-Configuration Server (ACS). Using TR-069, an ACS can remotely configure devices, push firmware updates, monitor performance, and perform diagnostics on a large scale. However, before a CPE can be managed via TR-069, it must know how to contact its ACS—specifically, it needs the ACS URL (and any required credentials) configured [1]. Traditionally, installing this information involved manually logging into each device's local interface and entering the ACS URL, username, and password, as provided by the service provider. This manual provisioning is time-consuming, error-prone, and impractical for large deployments. To address this problem, the TR-069 specification itself allows for automatic ACS discovery using the Dynamic Host Configuration Protocol (DHCP) [1]. In particular, DHCP Option 43 (Vendor-Specific Information) and Option 60 (Vendor Class Identifier) work in tandem to convey ACS server details to CPEs during the IP address assignment process [2]. By leveraging these DHCP options, service providers can achieve zero-touch or plug-and-play provisioning, whereby devices automatically receive the correct ACS address when they connect to the network. This paper focuses on how DHCP Options 43 and 60 enable automated distribution of ACS configuration to CPEs. We outline the TR-069 protocol fundamentals, describe the ACS server's role, explain the DHCP options mechanism for ACS URL delivery, and present a summary of the key parameters involved. The solution's benefits and considerations, such as security in DHCP-based provisioning, are discussed in the conclusions.

II. TR-069 PROTOCOL OVERVIEW

TR-069 CWMP provides a framework for remote management of CPE devices by a centralized ACS [1]. Under this protocol, the CPE initiates a connection to the ACS, typically over HTTP/S, and exchanges SOAP/XML messages containing remote procedure calls. This allows the ACS to instruct the device to perform actions such as configuration updates or to query its status. A fundamental requirement for this communication is that the CPE is pre-configured with several parameters, most importantly the URL of the ACS (e.g., "http://acs.example.com:7547"). Additionally, security credentials like an ACS authentication username/password may be needed if the ACS requires device authentication.

In practice, there are three primary ways a CPE can obtain its ACS URL [1]:
1. It may be factory-preprogrammed with the correct ACS address.
2. It can be configured locally via a technician or a user interface.
3. It can discover the ACS address through network protocols.

The third method is often the most scalable. TR-069 explicitly recommends using DHCP for this discovery process when manual or factory configuration is not feasible [1]. On first boot or after a factory reset which would trigger a TR-069 “bootstrap” event, a CPE that knows its ACS URL will immediately attempt to contact the ACS and register itself, sending an Inform message with a 'BOOTSTRAP' event code. If the ACS URL is not yet set, the device must find this information automatically to avoid manual intervention. This is where DHCP-based provisioning becomes crucial.

III. ACS SERVER ROLE

The ACS server is the control center in the TR-069 architecture. It is a server-side software system that manages the configuration and monitoring of a fleet of CPEs [1]. The ACS maintains a database of device settings and firmware versions and can apply configuration profiles or perform mass upgrades across devices. Through TR-069 sessions, the ACS can retrieve device parameters, push new settings or firmware, and run diagnostics remotely. This centralized management dramatically reduces the need for on-site support or manual configuration of individual units. However, to establish a TR-069 session, each CPE must first know how to reach the ACS.

In a default scenario without automation, a technician would have to manually input the ACS URL and possibly the credentials into the CPE via a local management interface. Such a process does not scale well when deploying hundreds or thousands of devices. Furthermore, any mistake in typing the URL or credentials into a CPE can prevent that device from ever connecting to the ACS. Therefore, automating the ACS discovery process is highly desirable. The goal is for new or reset devices to automatically learn the ACS address as soon as they come online. DHCP-based ACS provisioning resolves this challenge by utilizing the established mechanism that configures IP addresses and other network parameters for devices.

IV. DHCP OPTION 43 AND SUB OPTION 60

DHCP provides an ideal opportunity to deliver configuration data to CPEs the moment they join the network. The TR-069 standard takes advantage of this by defining a convention for using DHCP Option 43 (Vendor Specific Information) to convey the ACS URL and related settings to the CPE [1]. The process relies on coordination between two DHCP options: Option 60 and Option 43. Option 60 is the Vendor Class Identifier sent by the DHCP client (the CPE) to inform the DHCP server about the type of device or the services it supports. The Figure 1 shows the steps for a CPE to obtain ACS URL from a DHCP server.

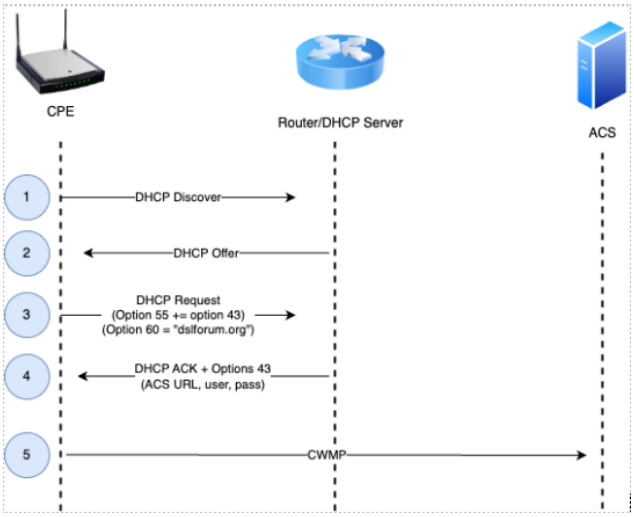

Figure 1. DHCP server and CPE steps for handing out ACS URL [6].

For any TR-069 capable devices, the Broadband Forum specifies that the CPE should include the text "dslforum.org" in the Option 60 string. This acts as a flag indicating - This device supports TR-069 and is requesting ACS configuration. Configuring DHCP option 60 helps in identifying the incoming DHCP client. If the vendor class identifier (VCI) advertised by the DHCP client matches with the DHCP server, the server makes a decision to exchange the vendor-specific information (VSI) configured as part of DHCP option 43 [5]. Option 60 defines the vendor type and configuration, while option 43 defines the vendor-specific information (VSI). If option 60 is configured, the VSI (defined in option 43) is returned to clients that provide the appropriate vendor type and configuration value. If option 60 is not configured, the VSI is sent to all clients [5].

Additionally, the CPE may use the Parameter Request List (Option 55) to explicitly ask for Option 43 (or the newer Option 125) in the DHCP offer. When a DHCP server recognized a CPE's Option 60 containing "dslforum.org", it will respond with the appropriate vendor-specific data in Option 43 of the DHCP Offer/Ack message. Option 43 in DHCPv4 is essentially a container for vendor-specific sub-options [2]. In the context of TR-069, these sub-options are encoded to provide the necessary ACS connection parameters to the CPE. Table I below summarizes the key sub-options defined for TR-069 ACS provisioning via DHCP [1].

DHCP Option / Sub-Option	Description (TR-069 Parameter)
Option 60 (Vendor Class Identifier)	String used by the CPE to identify itself as a TR-069 capable device. Must include "dslforum.org" to trigger ACS provisioning.
Option 43 (Vendor Specific Info)	DHCP server response option that carries vendor-specific TR-069 configuration information (encapsulated sub-options).
Sub-option 1: ACS URL	URL of the ACS server to contact. <ManagementServer.URL>.
Sub-option 2: Provisioning Code	Provisioning code identifying the service provider or configuration profile. <DeviceInfo.ProvisioningCode>.
Sub-option 3: Retry Wait Interval	Initial wait time for TR-069 retry attempts. <ManagementServer.CWMPRetryMinimumWaitInterval>.
Sub-option 4: Retry Interval Multiplier	Multiplier for the TR-069 session retry interval for exponential backoff. <ManagementServer.CWMPRetryIntervalMultiplier>.

Table 1. DHCP Options and functions.

All these Option 43 sub-options are encapsulated within the single Option 43 field in the DHCP response. The CPE, upon receiving its DHCP ACK, will parse Option 43, extract the sub-option values, and apply them to its local TR-069 client configuration [1]. At a minimum, sub-option 1 which defines the ACS URL is critical. Once that is configured, the CPE now knows the address of its ACS and can immediately initiate a TR-069 session to complete the bootstrap process.

Sub-options 3 and 4 provide default timing parameters for how often the CPE should retry contacting the ACS if the first attempt fails. They set the initial values for the CPE's retry logic. These optional parameters help avoid overloading the ACS with too many simultaneous connection attempts in large deployments. The Provisioning Code, which is defined with sub-option 2 is an optional string that the ACS can use to identify the subscriber's service or configuration context. For example, a service provider could use different provisioning codes to distinguish between residential and business customers, and the ACS could apply multiple unique configuration profiles accordingly.

V. MULTI-VENDOR AND DHCP OPTION 125

In multi-vendor networks, different device vendors might use their own proprietary encoding for Option 43. To mitigate potential conflicts, DHCP Option 125 (Vendor-Identifying Vendor Options) was introduced as a more structured alternative [3]. Option 125 allows multiple sets of vendor-specific data, each tagged with an IANA Enterprise Number, enabling the DHCP server to provide ACS information for devices from different vendors simultaneously [3]. TR-069 specifies that a CPE may request either Option 43 or Option 125; if both are provided, the CPE will use the one it requested. In a scenario where non was requested, the CPE will use Option 43 by default. In practice, many deployments continue to use Option 43 since it is widely supported, but Option 125 is useful for distinguishing vendors in the same network environment [3]. Similarly, for IPv6 networks, the equivalent mechanism uses DHCPv6 Option 16 (Vendor Class) and Option 17 (Vendor Specific Info) to carry the ACS URL and related options [1].

VI. CONCLUSION

Automating the distribution of ACS server information to CPE devices greatly streamlines the deployment and management of broadband networks. By utilizing DHCP Option 60 and Option 43 as defined in the TR-069 standard, service providers can ensure that newly installed or factory-reset devices automatically discover the correct ACS URL during the DHCP lease process. This eliminates the labor-intensive and error-prone task of manually configuring each device with ACS credentials, enabling true zero-touch provisioning. Field experience shows that this approach significantly reduces provisioning time and configuration errors, especially in large-scale rollouts. The DHCP-based ACS provisioning mechanism described is grounded in open standards [1][2] and has been adopted across various vendor implementations. It provides a low-overhead solution since it piggybacks on the existing DHCP exchange that every RG device performs when joining the network.

The CPE, upon obtaining its ACS URL from DHCP, can immediately initiate a TR-069 session signaled by a BOOTSTRAP inform to register with the ACS and download any initial configuration or firmware updates. This end-to-end automation—from IP address assignment to full device configuration—considerably accelerates service activation for customers. However, there are important considerations: since DHCP does not natively authenticate the source of options, operators must secure the DHCP infrastructure (e.g., using trusted networks or DHCP snooping) to prevent malicious actors from spoofing ACS URLs [1]. In practice, the ACS URL is typically an internal address or one reachable only via the provider's network, which mitigates the risk of redirection to unauthorized servers.

Overall, the use of DHCP Options 43 and 60 for ACS URL provisioning is a proven technique to enhance the scalability and reliability of TR-069-based management systems. It embodies the principle of

configuration automation, allowing ISPs and enterprises to deploy large numbers of CPEs with minimal manual intervention while ensuring that each device seamlessly comes under centralized management as soon as it comes online.

REFERENCES:

[1] Broadband Forum, "TR-069 CPE WAN Management Protocol," Technical Report 069, Amendment 6, Jun. 2020.
[2] S. Alexander and R. Droms, "DHCP Options and BOOTP Vendor Extensions," IETF RFC 2132, Mar. 1997.
[3] J. Littlefield, "Vendor-Identifying Vendor Options for DHCPv4," IETF RFC 3925, Oct. 2004.
[4] P. Chiodi, "ACS URL Configuration via DHCP Vendor Specific Information," Pierky's Blog, May 20, 2009.
[5] RUCKUS FastIron DHCP Configuration Guide, 09.0.10 - https://support.alcadis.nl/Support_files/Ruckus/ICX//Software%20Manuals/Ruckus%20ICX%20FastIron%20v09.0.10d/fastiron-09010-dhcpguide.pdf
[6] https://made4it.com.br/en/dhcp-option-43-for-auto-configuration-of-acs/