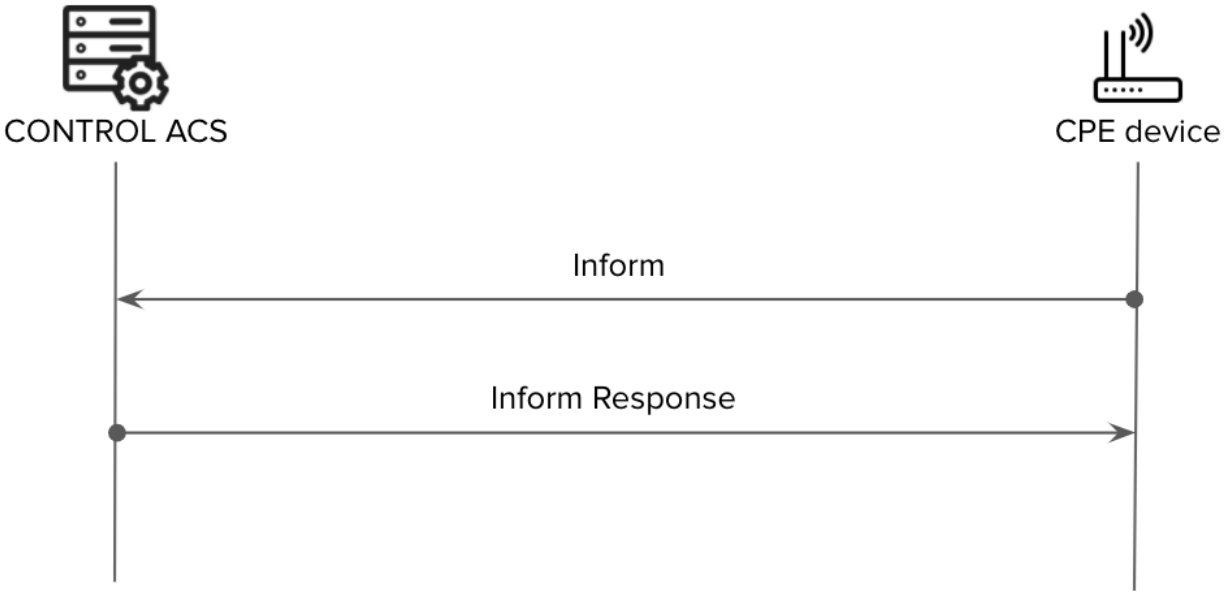
TR-069 Connection Request

Overview

TR-069 is a CPE-originated communication protocol, meaning that the CPE (Customer Premises Equipment) initiates connectivity toward the ACS (Auto Configuration Server) using a pre-agreed ACS URL, username, and password.



In a standard TR-069 communication flow, the CPE connects to the ACS at regular intervals defined by the **Periodic Inform Interval**. However, there are scenarios where the ACS needs to update or modify CPE parameters within a shorter timeframe than the configured interval. For example, a customer support agent may need to change a WiFi password immediately rather than waiting for the next periodic connection.

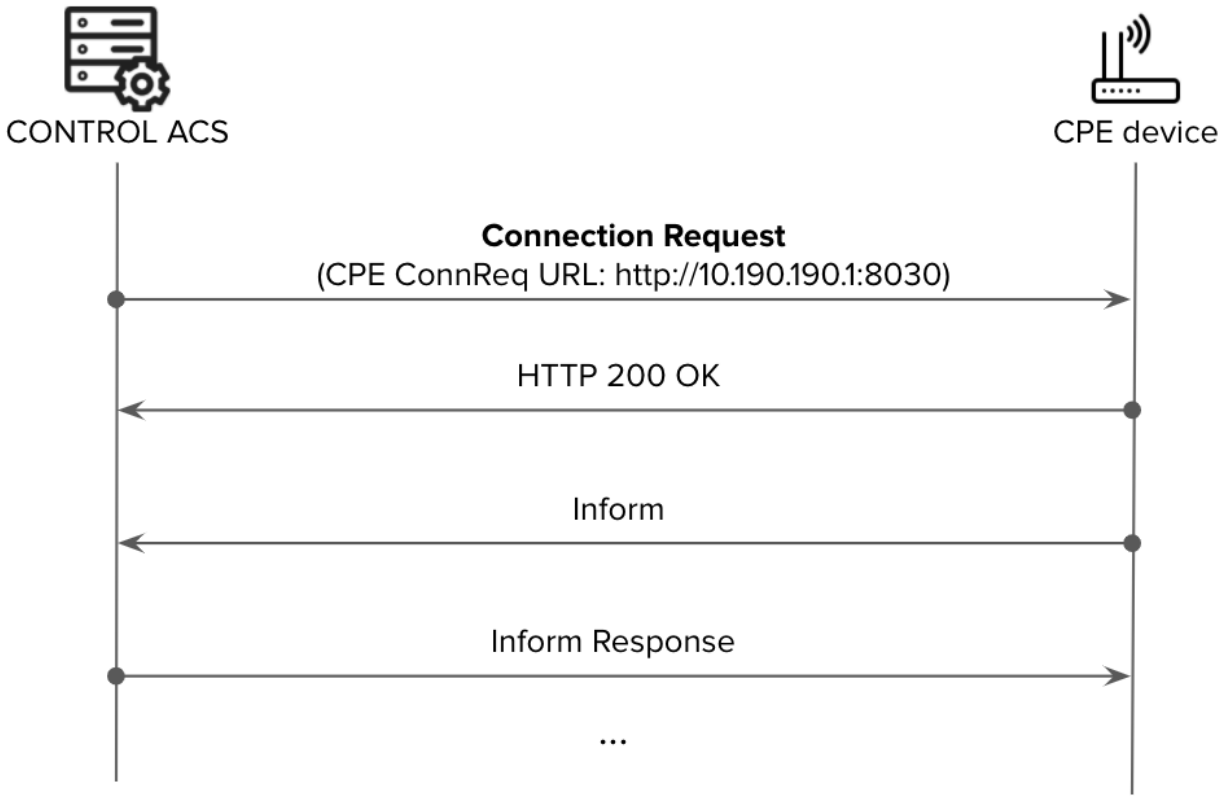
To address this requirement, the TR-069 standard defines a **Connection Request** functionality.

What is Connection Request?

Connection Request is a mechanism that allows the ACS to proactively request (or "poke") a CPE to initiate a TR-069 session at any time, independent of the Periodic Inform Interval.

How It Works

1. The ACS sends an HTTP request to the CPE using the **CPE Connection Request URL** with pre-agreed **Connection-Request Username** and **Connection-Request Password**
2. The CPE responds with either:
   - **Success**: `HTTP 200 OK` or `HTTP 204 No Content`
   - **Failure**: `HTTP 401 Unauthorized`
3. Upon successful acknowledgment, the CPE initiates a standard TR-069 session toward the ACS (beginning with the initial Inform message)



Benefits of Connection Request

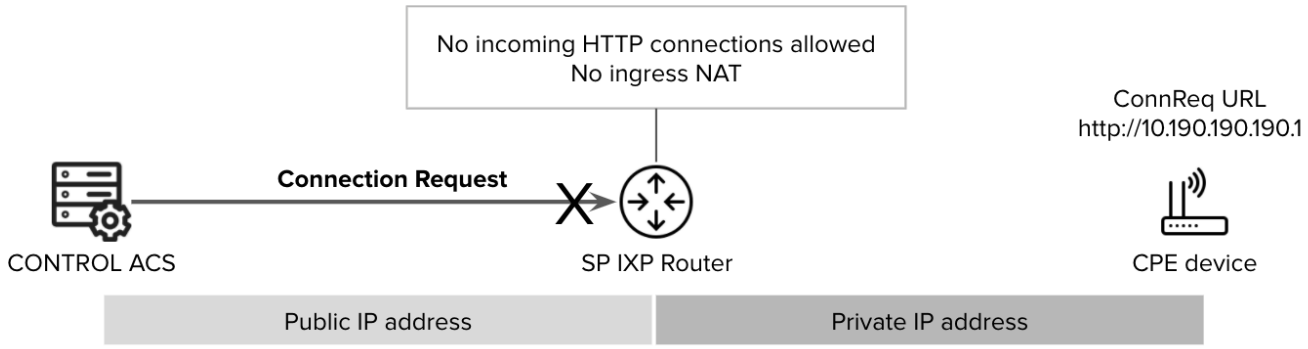
By enabling **Connection Request** between ACS and CPE, service providers can:

- **Reduce network overhead**: Use longer Periodic Inform Intervals to minimize network management traffic and CPE load
- **Maintain flexibility**: Retain the ability to make configuration changes or perform tests on-demand whenever required
- **Improve operational efficiency**: Enable immediate responses to customer support requests without waiting for the next periodic inform

Implementation Challenges

Implementing Connection Request presents challenges primarily related to enabling inbound HTTP connectivity from the ACS to the CPE. These challenges involve:

- **IP Reachability**: CPE devices are often behind NAT or use private IP addressing, making them unreachable from the ACS
- **Security Concerns**: Opening inbound connections to CPE devices requires careful security considerations

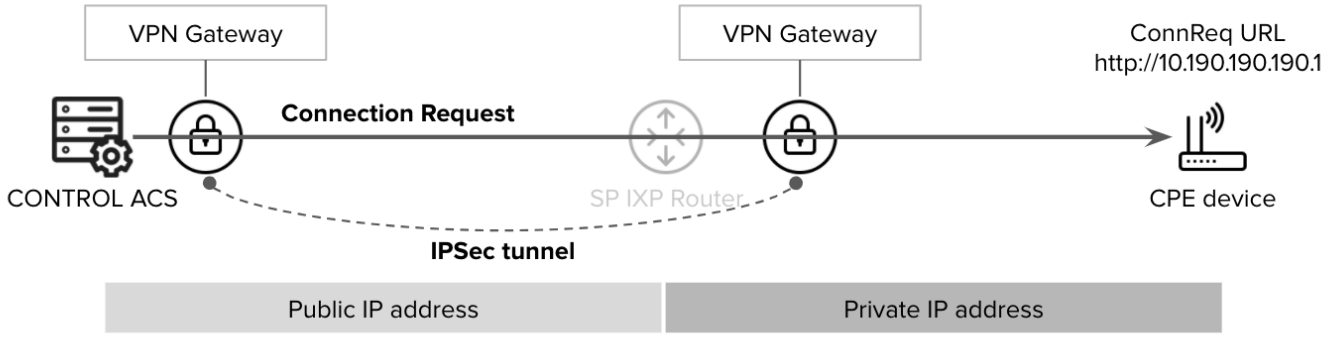


Connection Request Methods

Several approaches exist to overcome these implementation challenges. The following are the most widely deployed methods:

VPN-Based Connection Request

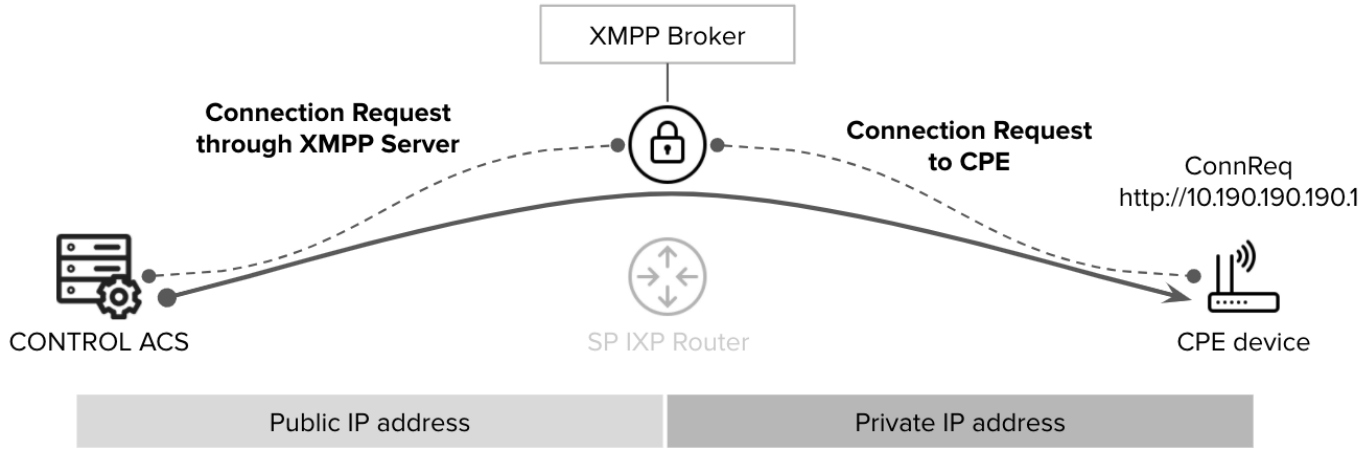
A VPN tunnel can be established to provide direct reachability from the ACS to CPE devices located within the service provider's private IP address space.



XMPP-Based Connection Request

This method uses an intermediate XMPP Broker that:

- Can reach CPE devices
- Is reachable by the ACS
- Can be located inside or outside the service provider's network (e.g., in a DMZ)

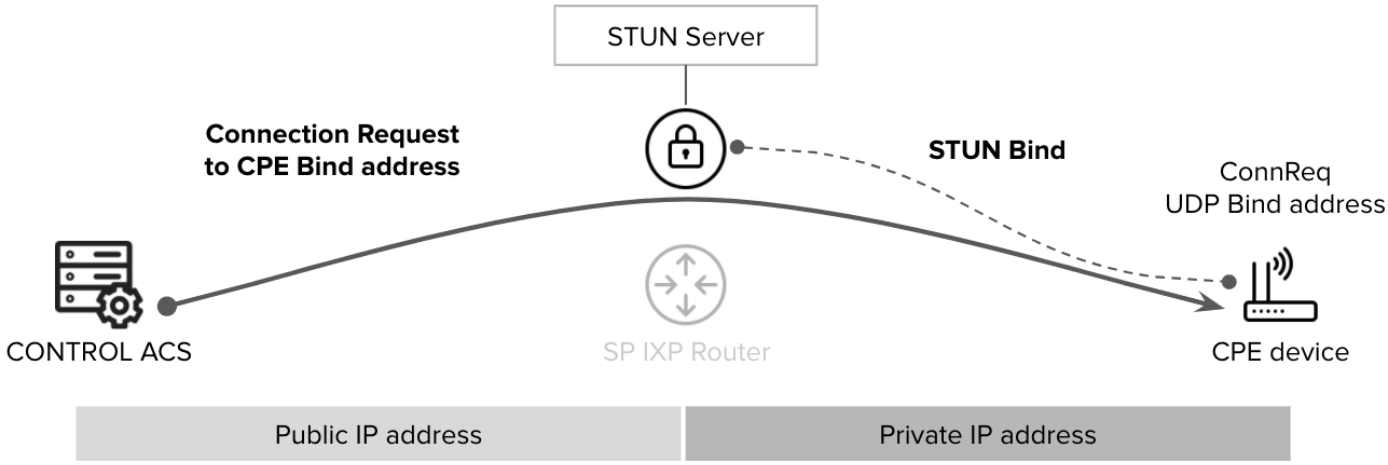


Reference: TR-069 Issue 1 Amendment 6 Annex K provides detailed specifications for this architecture.

STUN/UDP-Based Connection Request

This approach uses an intermediate STUN server to enable inbound UDP-based connection requests:

1. The CPE creates a UDP connection (bind) to the STUN server
2. The ACS can reach the CPE through the STUN server using the **UDP Bind address**
3. The STUN server can be located inside or outside the service provider's network (e.g., in a DMZ)



Reference: TR-069 Issue 1 Amendment 6 Annex G provides detailed specifications for this architecture.

Note: CONTROL ACS supports all of the connection request schemes described above.

Revision #2
Created 2026-02-13 22:32:24 UTC by ipena@zequenze.com
Updated 2026-02-14 01:08:16 UTC by ipena@zequenze.com