Implementation of TR-069 connection request mechanism

Ivana Savić, Milan S. Savić, Gordana Velikić
RT-RK Computer Based Systems,
Novi Sad, Serbia
ivana.ostojic@rt-rk.com,
msavic@rt-rk.com
gordana.velikic@rt-rk.com

Abstract—**This paper proposes and evaluates an approach for monitoring and controlling devices over a network based on TR-069 protocol. Protocol itself relies on communication between server and clients (devices). Main characteristic of this protocol is that all the communication is initiated from the device side. In order to allow server to initiate interaction, a connection request mechanism is defined. It serves as a notification system that informs the device to start interaction with the server. Depending on the network state, available resources at hand and security considerations, there are four types of connection request to choose from: connection request over TCP, connection request over TCP with port forwarding, Session Traversal Utilities for NAT (STUN) based connection request and Extensible Messaging and Presence Protocol (XMPP) based connection request.**

Keywords-TR069, connection request, STUN, XMPP

I. INTRODUCTION

The purpose of this paper is to propose a solution for device monitoring over a network with the emphasis on connection requests from server side. As shown in [1], TR-069 CPE WAN Management Protocol (CWMP) is protocol dedicated to monitoring and management of end-user devices. It enables communication between customer-premises equipment (CPE) and auto configuration server (ACS), as shown in Fig. 1.

Communication between ACS and CPE is initiated exclusively by CPE. Only way for ACS to initiate a connection with CPE is to notify CPE that it should engage in a session. This is achieved with connection request. It represents ping mechanism that allows the ACS to initiate connection. Connection requests are divided primarily into two groups depending on TR-069 protocol version used.

When TR-069 amendment 1 – 4 is used [1] – [4], then connection request that is going to be used is determined by network state. If CPE has a routable IP address TCP based connection request is used. Main characteristic of this kind of connection request is that it is used when ACS and CPE are inside the same address space. When CPE is behind Network Address Translation (NAT) gateway, STUN based connection request is used. Key note for this connection request is that it relies on tunneling mechanism which is created between each CPE and ACS.

Latest version of TR-069 protocol [5] proposes two new types of connection requests, TCP based connection request that relies on port forwarding and it is used in highly controllable network and it is not suited for requests over open internet. Alternative to previous request is XMPP based connection request which is usable in all network architectures with highest security of all proposed solutions.

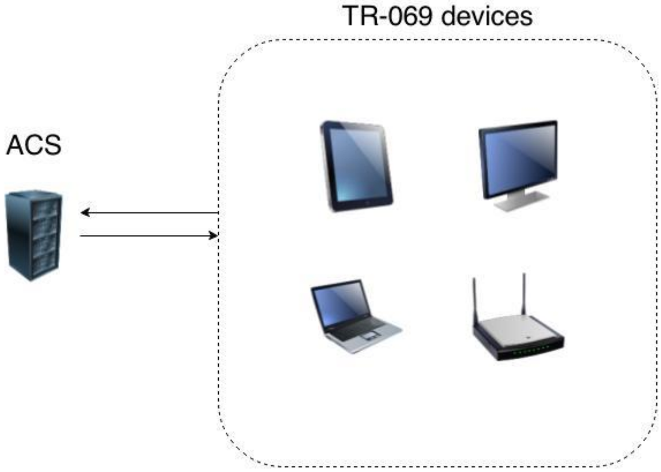

Figure 1. TR-069 Environment

Existing solutions that are based on CWMP protocol [6] don't follow the protocol by the letter, that way making devices that use it not compatible with other TR-069 solutions. A method for establishing connection through NAT is presented in [7], but instead of STUN based approach, TCP connection is used. Both solutions are not standardized and hard to implement in practice.

II. SOLUTION CONCEPT

When ACS has the need to inform CPE that it should engage in a session connection request process is started. Essentially it is an authentication process which depends on type of connection request implemented. In case of TCP connection request, HTTP Digest authentication is used. When STUN based approach is used, custom authentication defined in TR-069 protocol is used. If XMPP Connection request is used, Transport Layer Security (TLS) authentication is in place.

A. TCP Connection Request

This mechanism is used when CPE is not behind NAT gateway as shown in Fig. 2. Authentication method used is HTTP digest [8]. CPE acts like HTTP server and ACS has the client role. Authentication challenge contains data which combined with data from TR-106 datamodel [9] represent all the information necessary for successful authentication. TCP protocol is used for communication between ACS and CPE and for that reason it is important that ACS and CPE are in the same address space, in order to be visible to each other. More important it is essential that CPE is visible from the ACS because server sends connection requests and thus it has to be able to reach client.

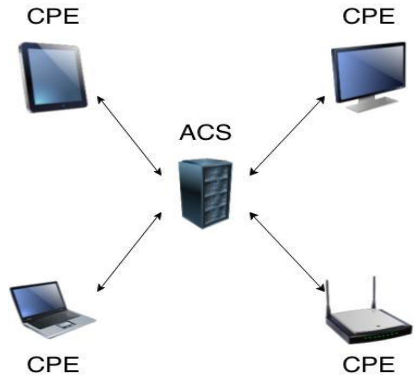

Figure 2. TR-069 environment with ACS and CPE in the same address space

As shown on Fig. 3, successful authentication serves as a signal for the CPE to start a session with CPE. Authentication is based on two steps. First empty GET request is send on which server responds with unauthorized response in which challenge for successful authentication is present. Client resends GET request, but this time with all the necessary data for successful authentication.

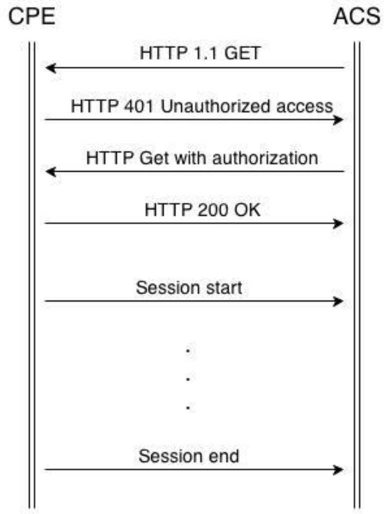

Figure 3. TR-069 connection request mechanism

B. STUN based connection request

When end-device is behind a gateway and if resources at hand do not allow use of latest TR-069 protocol version, STUN based connection request is used. It allows ACS to send requests to CPE even if end-device is in private address space. As shown on Fig. 4, STUN based connection request comprises out of:

- STUN server
- STUN client
- UDP server
- UDP client

STUN server is located on ACS side and STUN client on CPE side. Their role in connection request is to make a tunnel between ACS and CPE and that way make direct communication possible.

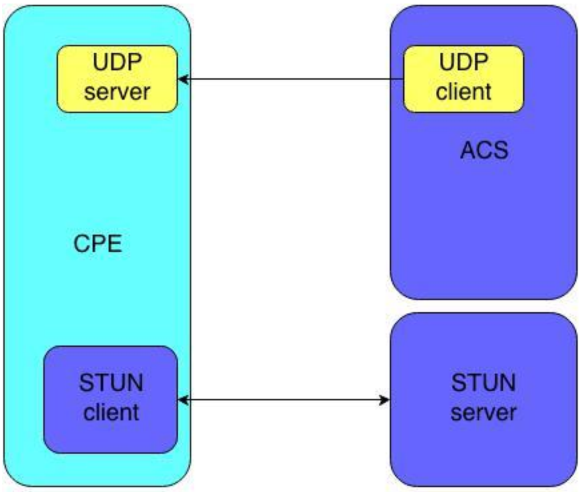

Figure 4. STUN based connection request

The purpose of STUN mechanism is to discover network and port translation and maintain that binding over time [10]. Mechanism is fairly simple, client sends a request to server and in response address and port on which response is send is conveyed. That way client is aware if port and address translation is in progress. If client determines that it is behind a NAT gateway, keep alive mechanism is activated. In this mode client sends messages periodically in order to keep the binding. For that purpose secondary port in STUN mechanism is defined and all the messages in keep alive process are sent from it. In keep alive message address and port on which response should be sent is present and in case that response arrives on that specific port, binding is in place.

Second part of STUN based TR-069 connection request is UDP server and client. It is similar to implementation of TR-069 connection request over TCP with couple of exceptions:

- Instead of TCP, UDP connection is used
- Authentication mechanism isn’t HTTP digest, instead custom authentication mechanism is used
- Client doesn’t get a response from server, only requests are sent and no response is generated.

C. TCP connection request with port forwarding

Connection request with port forwarding is used when gateway, behind which CPE devices reside, and ACS are in the same address space. That allows ACS to reach end devices through designated port on gateway which is mapped to a port on CPE as shown on Fig. 5.

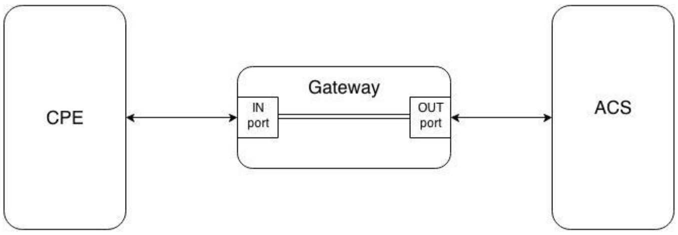

Figure 5. TR-069 connection request with port forwarding

Except this modification concerning network architecture everything is the same as in case of regular TR-069 connection request over TCP without port forwarding.

D. Connection request over XMPP

Connection request over XMPP protocol [11] enables the ACS to reach end device no matter the network architecture as shown on Fig. 6. All the data necessary for successful communication is conveyed through TR-157 datamodel [12]. Connection request architecture can be divided into three parts:

- XMPP client on CPE
- XMPP client on ACS
- XMPP server

Architecture defers from previous connection requests where CPE had the role of server and ACS the role of client. Now both ACS and CPE are clients and their messages are conveyed through XMPP server which is responsible for enabling communication between clients.

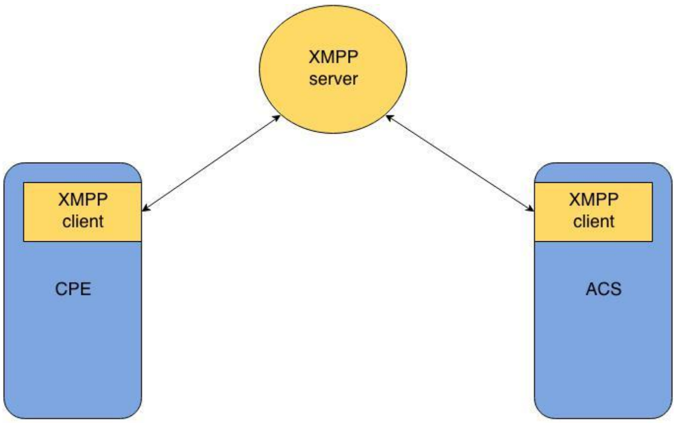

Figure 6. TR-069 XMPP connection request

Connection between XMPP clients and server is based on TCP. Once client is connected on server, connection is kept alive by periodic ping messages from server to clients. That way clients are always reachable and client state (offline or online) can easily be determined. Knowing the client state at any time makes this connection request robust which is not the case for some previous implementations. This kind of connection has it downside in higher data consumption.

III. Experimental Results

The proposed concept was validated on Linux based set-top-box (STB) on client side and for the ACS side Intel based server was used. With connection request ACS gets almost instance response from the CPE, that way making TR-069 system more responsive and agile.

TR-069 connection request over TCP and connection request with port forwarding have the same authentication process and thus have same experimental results, as shown in Table I. Although the network architecture is different, the complexity itself remains almost the same. Only difference is that port forwarding is used when gateway is between CPE and ACS. That doesn't add up much to network complexity and for that reason it doesn't add any delay to the system response.

TABLE I. TR-069 Connection Request

Test	Value
Channel change	~2.8 s
Authentication time	~50 ms

TR-069 request over STUN is used when gateway or numerous gateways are between CPE and ACS. This kind of connection request is best suited when connection between ACS and CPE is conveyed through open internet. Due to custom authentication process which is simpler than HTTP digest mechanism used in connection request over TCP, system response time is faster, as shown in Table II.

TABLE II. TR-069 STUN Connection Request

Test	Value
Channel change	~2.1 s
Authentication time	~18 ms

Connection request over XMPP can be used on any network configuration. Because of the architecture of the XMPP server/client communication, authentication between client and server is done only once upon authentication with XMPP server, that way every time the connection request is sent over XMPP there is no authentication process. There is only the time it takes a message to be sent from one XMPP client to another. As shown in Table III, system with XMPP connection request is highly responsive and gives the best results out of all proposed connection request mechanisms.

TABLE III. TR-069 XMPP CONNECTION REQUEST

Test	***Value***
Channel change	~2 s
Authentication time	0 s
Message transfer time	2-7 ms

IV. CONCLUSION

Connection request enables instantaneous system response from end-device. No matter what network architecture is, end-device is always reachable from the ACS. Connection request mechanism is highly usable when TR-069 protocol is used in home automation. In smart house solutions user has the need to interact with his household over the Internet. In order to achieve comfortable usage system has to be responsive and enable the user to experience almost real time monitoring with data available right. Only concern regarding TR-069 protocol is privacy. User data resides on server which is outside of users reach and therefore making private data vulnerable. The solution might be in small household systems where the ACS would reside inside a house and would be used to monitor and control household appliances. Without a third person having access to your personal data, privacy issue is basically non-existing.

ACKNOWLEDGMENT

This work was partially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia, under grant number TR 32034.

REFERENCES

[1] DSL Forum, "TR-069 CPE WAN Management Protocol v1.1", November 2006.

[2] DSL Forum, "TR-069 CPE WAN Management Protocol v1.2", December 2007.

[3] DSL Forum, "TR-069 CPE WAN Management Protocol v1.3", November 2010.

[4] DSL Forum, "TR-069 CPE WAN Management Protocol v1.3", July 2011.

[5] DSL Forum, "TR-069 CPE WAN Management Protocol v1.4", November 2013.

[6] Tiago Cruz, Paulo Simőes, Patrício Batista, João Almeida, Edmundo Monteiro, "CWMP Extensions for Enhanced Management of Domestic Network Services", LCN 2010, Denver, Colorado.

[7] Jeffrey L. Eppinger," TCP Connections for P2P Apps: A Software Approach to Solving the NAT Problem", Institute for Software Research International, School of Computer Science, Carnegie Mellon University, 2005.

[8] "HTTP Authentication: Basic and Digest Access Authentication", IETF RFC 2617, 1999.

[9] DSL Forum, "TR-106 Amendment 1 Data Model Template for TR-069 –Enabled Devices", November 2006.

[10] "STUN – Simple Traversal of User Datagram Protocol through Network Address Translators", IETF RFC 3489, March 2003.

[11] "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence", IETF RFC 6121, March 2011.

[12] DSL Forum, "TR-157 Amendment 5 Component Objects for CWMP", November 2011.