REVIEW ARTICLE

TRANSFER PROTOCOLS IN TR-069 CWMP

SAVYA K[1], YETHINDRA A1, RANJANI.G[2], B.ROJA REDDY[2], SATYANARAYANA C[3]

[1]2nd year, M tech, Digital communication, Telecom dept. RVCE Bangalore.
[2]Assistant Professor, Telecommunication dept. RVCE Bangalore.
[3]CEO, ATTO Communication Pvt. Ltd. Bangalore

ABSTRACT

TR-069 is a technical report numbered 69 which gives detail about a customer premises equipment (CPE) wireless area network (WAN) management protocol (CWMP). This paper is a review paper on transfer protocols which are used in TR-069 protocol stack, the transfer protocols which are used are Transfer Control Protocol or Internet Protocol (TCP/IP), Hypertext Transfer protocol (HTTP). The paper defines the main differences between other protocols and protocols used in TR-069. One of the best examples why these protocols are used can be given as use of HTTP makes TR-069 a NAT friendly where other fails in this.

Keywords— TR-069, CWMP, ACS, DSL FORUM, NAT, HTTP, TCP /IP, SOAP.

INTRODUCTION

TR-069 is a technical report which gives detail about network management protocol which is customer premises equipment wireless area network management protocol. TR-069 is a next generation protocol which is used for zero touch configurations between Auto-Configuration Server (ACS) and CPE, one of the main advantage of TR-069 s its functionality and its ability to go behind the Network Address Translation (NAT).

The functionality of TR-069 includes set parameter, get parameter values, get Remote Procedure Calls(RPC) methods, get parameter names, set parameter names, set and get parameter attributes, add and delete objects, upload and download and at last reboot and reset factory settings.

The parameters that are mentioned in the above Para describe the value given for the specific function, for example if there is an up-gradation of client device it as a parameter value to be changed over the old parameter value.

To transfer this parameters and the data we need transfer protocol which is fulfilled by the TCP/IP and HTTP, which are placed below the stack.

This protocol has six layers and they are

1. ACS management application.
2. RPC methods.
3. Simple object access protocol (SOAP).
4. HTTP.
5. SSL/TLS.
6. TCP/IP.

Transfer protocols HTTP and TCP/IP are used to transfer data between source and the destination in the TR-069 protocol; Hypertext protocol provides http encoding, Digest authentication, Transfer Data. TCP/IP which is a Transfer protocol which provides flow and error control option along with the checksum bit.

CPE/ACS APPLICATION

Application layer is for remote management between the device (CPE) and server (ACS). Application is installed towards CPE or ACS

with required properties. CWMP protocol sends an RPC methods in terms of SOAP over the HTTP and communicate as SSL/TLS through the TCP/IP protocol layer. CPE always initiates a connection which is called single TCP connection over which RCP is made back. Client begins with an inform message stating the reason of session initiated with provision functions.

RPC

Two RPC methods are defined they are ACS and CPE methods.

RPC Methods for CPE are

Get RPC methods, Set parameter values, Get parameter values, Get parameter names, Set parameter Attributes, Get parameter Attributes , Add object, Delete object, Reboot, Download.

RPC Methods for ACS methods

Inform, Get RPC methods, Transfer complete

Common RPC methods for both CPE and ACS are

Set parameter values, get parameter values, get parameter names, download.

RPC Methods required for CPE and optional for ACS are

Get RPC methods, Set parameter attributes, get parameter attributes, add object, Delete object, Reboot.

Optional methods for both CPE and ACS are

Schedule download, upload, factory reset, get queued transfers, get all queued transfers, cancel transfers, schedule inform, change DU state, Set vouchers, Get vouchers, Get options.

SOAP

SOAP is defined as simple object access protocol where message is sent over HTTP ,SOAP is used to format the messages transferred as calls and responses. SOAP messages are used to maintain the format of the messages transferred b/w the CPE and ACS. This protocol is used because it is simpler to design and readable to user . . SOAP contains envelope, header and body, where header is optional, where the envelope contains the destination address and the header is used when pointing to particular address, header is optional, it is used only when required, body contains the message to be conveyed ,when the message fails to reach particular destination results in fault code conveying message is not sent .

HTTP

Initially CPE sends an open connection to ACS. Two way oath will happen between CPE and ACS. After SSL initiation CPE will send an inform request to ACS, ACS will reply with the inform response message.

The service is served between the CPE and ACS within the limited session. After the session CPE will send an close connection to ACS to end the session.

CPE connection establishment

The process takes place with the following steps

- Initial installation
- Power reset
- Once every management server periodic
- Initiates an inform on change When a parameter is modified.
- ACE is notified when download or upload completes.

SSL

SSL is defined as Security socket layer and also called as TLS - transport layer security are the cryptographic protocols which provide security over a network. They encrypt the data flow between the client and server and vice versa.

TCP

TCP is defined as Transmission control protocol and also called as IP - Internet protocol, provides connectivity from end to end. Packetizing, addressing transmission control, routing to the specified destination are maintained by TCP/IP protocol.

TRANSFER PROTOCOLS

HTTP/1.1

The Hypertext Transfer Protocol (HTTP) an application layer which is used for hypermedia information systems , transfer distributed and collaborative. In World Wide Web data communication HTTP acts as foundation.

One of most advantage of the HTTP is it's a NAT friendly that is it can go behind all firewalls which are present in the client side for the authentication purposes.

Hypertext is structured and formatted text uses logical links that is hyper links between messages and nodes containing text . HTTP is the protocol used to exchange or transfer hypertext in formatted way.

HTTP works as a request and response protocol in the ACS and CPE in a computing model. A browser,

example, consider the CPE and the application running on a host computer site be ACS, The client sends an HTTP inform request messages to the server. The server which contains files, reply with a response message stating the request is accepted.

HTTP has been designed as intermediate network to provide communications between CPE and asynchronous servers. High-traffic servers benefit from cache servers that deliver content on behalf of upload or upstream servers to improve response time. server cache previously accessed server and reuse them when possible to reduce network traffic. HTTP proxy servers at private and public network boundaries can facilitate communication for CPE without a globally routed address, by replaying messages with Asynchronous servers.

HTTP an application protocol which is developed within the framework of INTERNET protocol (IP). It includes an underlying and reliable Transfer control protocol(TCP), However HTTP can also use unreliable protocols such as the user datagram protocol (UDP), Simple object access protocol(SOAP),secured socket layer (SSL) and File transfer Protocol(FTP).

TIM BERNERS-LEE and his team were the one who invented the original HTTP along with HTML and the associated technology for a text-based web browser and a web server .

HTTP has its own methods to fetch or attach the data and methods includes as given below.

1. GET: it is a Request that represents one of the specified resources. Requests using GET should only fetch the data and should have no other effect.

2. HEAD: This is used when there is no body of the message or doesn't have any message content, this is basically used to establish connection with single request and response messages or the inform messages.

POST: This is a request which is used Request the server to accept the entity enclosed in the request as a new subordinate of the client identified by the URI or the URL. The data which is used to be transfer; uploaded and downloaded it use POST data

PUT: This request is used to modify already present connection and also the repair the network connection between the client and the Server.

DELETE: Deletes the specified function or the method or the data or the resources.

TRACE: Gets a copy of request dent so that it can compare what are the changes made by the server or any other resources.

OPTIONS: This method returns the HTTP methods that are supported by the server by using URL. This can be used to check the functionality of the server and Client.

CONNECT: This request converts an HTTP connection request to a TCP/IP tunnel for the transfer of the data.

PATCH: This function provides partial modifications to a resource.

SECURITY: HTTP also provides a Digest authentication whenever the SSL/TLS fails in securing the connection.

Similar protocol which does the same work as the HTTP is GOPHER, SPDY and FTP. HTTP has overcome all the disadvantages of other protocols and has an advantage of going through the NAT.

2.1.1 Gopher VS HTTP

Gopher is also a browser similar to an HTTP browser; it has a Gopher server and client through which they transfer file. It is almost similar but gopher is text based browser and cannot handle the anything other than text, it has a interactive text display, Comparing with HTTP it has better interaction display with graphical display.

HTTP has universal resource location (URL) and universal resource identifier (URI) system which points the destination address which makes both client and server easy to transfer data, which makes the system fast in transferring the data.

Gopher is little bit complex when it comes to large users, while the HTTP simple and secure and used by whole world right now. Gopher doesn't have security to data sent.

Whole world is using HTTP that is web browsing but if anyone with gopher has his own advantage but problem is he cannot access the HTML data because Gopher cannot read HTML format.

For having a Gopher protocol or browser it should be licensed but for HTTP client and server you don't need licensing.

Gopher protocol doesn't support MIME and also uses domain name for addressing, which makes difficult for live connection or the continuity of the connection. For every new connection it requires a password entry and uses FTP for the file transfer, whereas in HTTP once connection is established it

does not requires further authentication and authorization.

2.1.2 FTP VS HTTP

HTTP and file transfer protocol (FTP) both are fast and can upload or download large data; both have their own advantages and disadvantages. FTP has both limits in transferring data while HTTP has limit of 4 GB data to transfer.

One of the main advantage of the http is it works for client and server file transfer but ftp is for batch transfer of file. Both actually have same speed and performance and send data over TCP/IP. But HTTP is preferred more due its friendly nature with fire walls.

HTTP allows interrupt downloads to restart, and can supply the media type along with the download (MIME), it is easier to encrypt. All the features were limits of FTP but HTTP successfully utilize features.

Ftp always fails to reuse the same socket for transferring multiple files whereas HTTP does it with ease.

2.1.3 SPDY VS HTTP

SPDY called as speedy is developed by GOOGLE which has most updates than the HTTP but has some limitation makes TR-069 use HTTP.

SPDY use content compression which makes transfer of more data than the HTTP has advantages of parallel request and response so it doesn't wait for one request to get a response it can send as many requests it wants.

In HTTP only client initiates the connection but in SPDY server can also initiates the connection hence its more bidirectional.

The problem with the SPDY is that it's a new technology and is not explained clearly, the binary framing which can be used easily in HTTP cannot be used in SPDY. To make this possible it uses transport layer security (TLS) or HTTPS hence which makes access to only browser with secured socket HTTP (HTTPS) not every server.

SPDY has limited host compared to the HTTP hence HTTP can have control more clients and server than the speedy. SPDY has one more disadvantage that is it should have different and separate connection to each host which makes some complex in networking whereas in HTTP it can have single connection to many clients and server.

SPDY is not yet standardized while HTTP/1.1 is standardized and is used by most of the browsers and hosts and in future it can be upgraded to HTTP/2.

When download and upload comes HTTP has the upper hand that is because it can download two files which are interdependent on each other but SPDY fails here to download or upload.

SPDY is more efficient in lower round trip delay whereas in large RIT it is less effective, but HTTP provide good performance in both RITs. SPDY also fails in download of large pages where in HTTP is easy task.

2.1.4 SMTP VS HTTP

SMTP is derived as Simple Mail Transfer Protocol which is an basically push based protocol. The main difference between HTTP and SMTP are described below.

HTTP mainly a protocol-- loading information on a server and client use HTTP to get the information from server. On other side, SMTP is a push protocol for sending mail server pushes the file to receiving mail server.

In SMTP ,each message to be in seven-bit ASCII, including the body of each message. Message to be encoded into seven-bit ASCII format if the message contains binary data. This restriction is not found in HTTP.

HTTP encapsulates response message each object of message in it while in SMTP one message contains all of the message's objects .

TCP/IP

Transfer Control Protocol (TCP) and Internet Protocol (IP) are the transfer protocol which transfer data in packets and does flow and error control while transferring the packets.

TCP and IP are two completely different protocols that are often go together. Several protocols linking is common since the different protocols functions can be complementary together they carry out task completely . Several protocols combined to carry out a particular task is also called as "stack".

The information broken up into "packets" or smaller pieces and sent over the Internet. The speedy transmission of packets since parts of a message sent as small packets in different routes and at the destination packets are reassembled. It overcomes information loss during the transmission process. TCP is meant for creating packets, reassembling them at the destination end, and to check for the correct ordered packets with no loss

during the transmission. If pocket is lost during transmission TCP requests for the resent of that pocket.

The method to route information (internet protocol) to the proper address. Every computer have its own unique address on Internet known as the IP address. Every packet sent will contain an IP address showing where it is supposed to go. A packet may go through a number of computer routers before arriving at its final destination and IP controls the process of getting everything to the designated computer. Note that IP does not make physical connections between computers but relies on TCP for this function. IP is also used in conjunction with other protocols that create connections.

UDP VS TCP

User Datagram Protocol (UDP) is older version of the TCP, UDP is simple and connectionless protocol whereas TCP is connection oriented protocol.

UDP after sending does not care about the data is reached to destined address or not while TCP has concern and work based on request and acknowledgement.

UDP can be used for small queries with very large clients attached to it but TCP can handle more no of clients and also large no of queries.

UDP does not fit for HTTP and its quit fast without error checking, TCP uses HTTP quit well and slow with flow and Error check before transferring the data.

UDP is lightweight. It has no ordering of messages, no tracking connections. It is a small transport layer designed on top of IP, while TCP is Heavy-weight where it reliable and congestion control over packet transfer.

TCP reads byte stream of data and message is transmitted to segment boundaries. UDP messages are packets which are sent individually and on arrival are checked for their integrity. Packets have defined boundaries while data stream has none.

CONCLUSION

In TR-069 it has HTTP and TCP/IP as a transfer protocol which has their own advantages which suits the need of protocol.

It need a wireless connection and a port utilizing protocol which controls the network and this feature is provided by the both TCP and HTTP that is HTTP works in PORT 80 and provides web browsing.

CWMP needs to go behind the firewalls of client and also have secured transmission, HTTP is only one protocol which goes behind the NAT that is Network Address Translation which is kind of protocol which provides authorization to client.

CWMP have large number of clients and has large queries and only TCP/IP can hold the control of that much of data with reliable and congestion.

Totally TR-069 CWMP Protocol has taken only that transfer protocol which suits its need; HTTP and TCP/IP are those protocol which are considered by the TR-069 protocol.

REFERENCES

[1] TR-069 Amendment 5, "CPE WAN Management Protocol", Broadband Forum Technical Report, November 2013

[2] Suzan D. McGinnis (2001). Electronic collection management. Routledge. pp. 69–72. ISBN 0-7890-1309-6.

[3] TR-069 Amendment 3, "CPE WAN Management Protocol", BroadbandForum Technical Report, November 2010.

[4] RFC 2616, "Hyper Text Transfer Protocol"IEFT,june 2014.

[5] "SPDY: An experimental protocol for a faster web". Chromium Developer Documentation. Retrieved 2009-11-13.

[6] Forouzan, B.A. (2000). TCP/IP: Protocol Suite (1st ed.). New Delhi, India: Tata McGraw-Hill Publishing Company Limited.

[7] RFC 959 (Standard) File Transfer Protocol (FTP). Postel, J. & Reynolds,J.(October1985).

[8] RFC 768, "User Data gram Protocol "IEFT, August 1980.

[9] Hunt ,C Send mail cookbook. O"Reilly Media, ISBN 0-201-43288-9, 2003.