Journal of Theoretical and Applied Information Technology
30th June 2012. Vol. 40 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCEMENT OF CUSTOMER PREMISES EQUIPMENT WAN MANAGEMENT PROTOCOL USING TR-069

[1]J. ALEX MICHAEL RAJ, [2]K. JOHN SINGH
[1]Final Year M.Tech (IT), School of Information Technology and Engineering
VIT University, Vellore, Tamil Nadu, India
[2]Assistant Professor (Senior), School of Information Technology and Engineering
VIT University, Vellore, Tamil Nadu, India
E-mail: jalexmichaelraj@gmail.com, johnsinghaj@yahoo.com

ABSTRACT

Wireless technology makes today's work more flexible and easier. The customer premises wan management protocol is used to communicate between customer premises equipment and an auto-configuration server. The CPE wan management protocol uses the TR-069 framework architecture for self-configuration of devices. In this paper, using the broadband forum CWMP (TR-69) support the applicability of our implementation by adding the wireless devices without rebooting our system.

Keywords: *Home Area Networks (HAN), Customer Premises Equipment (CPE), Customer Premises Equipment Wireless Area Network Management Protocol (CWMP), Internet Service Provider (ISP)*

1. INTRODUCTION

In last few years, the wireless networking is growing widely and manufacturers are trying to implement them in almost all electronic gadgets or devices even in home appliances. By this, for home users it will become easy to manage it using a broadband interface. All these devices can be managed using the Home Area Network (HAN). The HAN is a network formed in local residential area. In this small number of wireless devices like Internet Protocol Television, laptops, Voice over IP etc can be maintained.

The Internet Service Providers has come up with their management scope to end the borderline equipment for domestic customers who use their own gateways. But the situation is gradually changing, since the need for ISPs to be able to manage equipments inside the customer LAN is increasing.

Some of the key services now provided by operators (VoIP, IPTV, VoD, etc.) heavily depend on devices placed on the customer LAN but intended to be managed by the ISP (e.g. set-top boxes).Customers expect these new IPbased services to match or exceed the performance and reliability of their conventional counterparts. Since most customers lack the willingness or technical skills to properly manage associated devices, this implies that operators must be able to remotely manage those devices and the path between them and the access network (i.e. at least a segment of the customer LAN), in order to maintain adequate service levels.

In this paper, using the self-configuring devices without rebooting we will be able to add devices. Because for adding a new device we need to reboot the whole system which will take a lot of time and till that time we need to stop the services, which will be difficult. In Section II we will describe the concept of self configuring.

2. RELATED WORKS

CWMP in particular has been a good part the research area. Based upon the IBM MAPE-K framework the architecture is done. Many have come up with their own protocol concepts and architecture. The self configuring of ACS and managing them is based on IBM MAPE-K [4]. In this, whenever we connect or add new devices we need to reboot the whole system, which becomes a big disadvantage and problem when working and managing the devices.

IBM has introduced its own ACS architecture. The IBM MAPE- K [4] is based upon the TR-69. In this also it doesn't have to option to add devices without rebooting the system. The protocols are done using the SOAP –RPC mechanism. Mi-Lung Choi and their team have given the concept of managing the IP network devices using XML. This concept will help in

Journal of Theoretical and Applied Information Technology
30th June 2012. Vol. 40 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

implementing the SOAP-RPC for the ACS. Klie.T and Straub.F use the agents in the XML for the configuring the devices. They have integrated the SNMP agents and XML for managing their devices.

Apostolos et al. proposed a solution for remotely managing the home environment by UPnP. This will make the consumers to manage the home devices by UPnP. This will improvise the overall performance. The E2R (end-to-end re-configurability) architecture was proposed [8]. Though this is used for managing mobile devices it's based on E2R which has an Advanced Device self Managing framework for mobiles.

A suite tool and methodologies was proposed [3] for CWMP. The advantage of these is to manage and create many device objects like Management Information Base (MIB). In this it provides good standard UPnP and CWMP protocols for home devices.

3. FUNCTIONAL COMPONENTES

The CPEWMP supports for many functionality. This will make our work easy in managing the CPE devices with the following provisions: Self configuring of device, Software Management, Monitoring the CPE devices and Diagnostics.

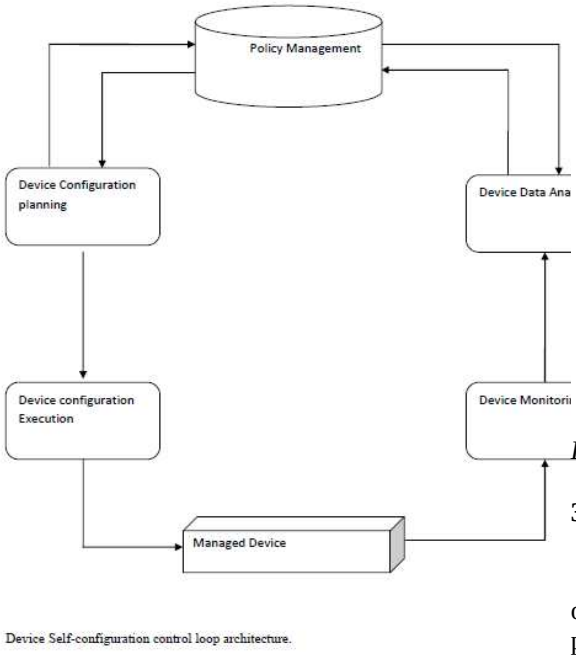

Fig. 1: Device Self-configuration Control Loop

3.1 Auto-Configuration and Dynamic Service Provisioning

As in Fig.2 the ACS configures with the CPE devices and service configuration Manager. When the ACS communicates with the devices is called the South Bound interface and when the ACS communicates with the ISP is called the North Bound. Whenever new devices are added, initially the ACS does the self configuration part The ACS only acts as an intermediate between the CPE devices and the ISP. The ACS is also acts as a server and it records the operations or processes done. These records are stored as history to know the operations taken place in case of any security issues.

When creating a network we also need to take care of security which plays a main role in the safe guarding the privacy. Here, the security will be taken by third parties. And there are many internet securities available in online. Like Kaspersky Internet Security, Bit Defender and many other internet securities to safe guard or monitor the intruders. The security software's will be installed in the ACS server. Above all of these a separate broadband connection with good internet speed should be provided for managing all of these devices.

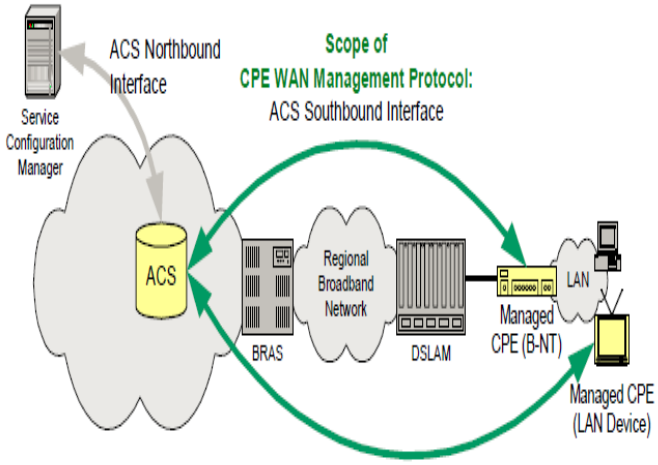

Fig. 2: ACS Architecture

3.2 Software Management

All devices cannot be auto-configured with one software version. According to the device platform software gets differed. The versions of the software's differs according to the notifications received while auto configuring. When the configuration is not successful an error message or a notification is sent about the particular device.

Journal of Theoretical and Applied Information Technology
30th June 2012. Vol. 40 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

And according to it a new version of it is released or updated. A new version will be updated in this field where the users will be able to download and install it. The versions will be digitally signed, so that it can be known that it was developed from the same organisation and is safe to install.

3.3 Monitoring

In this the overall CPE devices are monitored and statistics of its performance are taken. Buy this we will know the status of the device and whether any security alert is alarmed. If there is any intrusion or threat regarding security, using the third party internet security system we will be intimated. There are some predefined procedures or conditions; when it is out of it then we get a notification regarding the behavior.

3.4 Diagnostics

When while connecting or adding any devices if any problem occurs, then this steps diagnosis the error. When the issue is not rectified then we go for manual configuration. The connectivity issue arises even based upon the version installation, so it's not concerned with configuration alone.

4. CUSTOMER PREMISES EQUIPMENT WIRELESS AREA NETWORK MANAGEMENT PROTOCOL ARCHITECTURE

The CWMP consists of a five basic protocols: TCP/IP, SSL/TLS, HTTP, SOAP and RPC Methods and one ACS management protocol as in Fig.3.These six protocols form a CWMP stack which we are using in this system network.

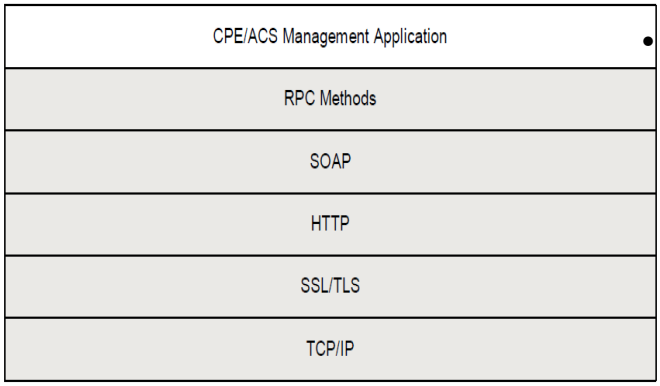

Fig.3: CWM Protocol Stack

The Transmission Control Protocol (TCP) and Internet Protocol (IP) were the first networking protocol designed. The TCP/IP is used to communicate between the ACS and the CPE device. The TCP/IP provides an end-to-end connectivity, where their will not be any data loss. The Secured Socket Layer (SSL) and Transport Layer Security (TLS) provide a secured gateway for communication between the server and devices. The SSL/TLS are also known as cryptographic protocols, because they encrypt the segments with the help of asymmetric encryption for key, MAC for messages and symmetric for private data. Based upon the sharing of data the HTTP protocol provides authentication.

It's recommended to use SSL/TLS for the CWMP, even though we can directly establish connection using TCP. SSL/TLS has a good security feature when compared with the TCP. There are some restrictions while using the SSL/TLS protocol:

- When SSL/TLS supports then 128bit encryption algorithm with keys should be used.
- CPE initiated connections should be accepted by ACS.
- CPE should authenticate using ACS certificate.
- CPE should initiate outgoing connections.

Here we also use SOAP for doing remote procedure call SOAP messages are one-way transmissions and they are combined with request/response. There are few procedures to be followed while using SOAP:

- Request and response messages must be encoded as structures.
- For each parameter input, there must be an element with the same name as the parameter.
- For every parameter output, there should be an element with a matching name.

Journal of Theoretical and Applied Information Technology
30th June 2012. Vol. 40 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

```
Request
<SOAP-ENV:Body>
    <m:GetLastTradePrice xmlns:m="some-URI">
        <symbol>DEF</Symbol>
    </m:GetLastTradePrice>
</SOAP-ENV:Body>

Response
<SOAP-ENV:Body>
    <m:GetLastTradePriceResponse xmlns:m="some-URI">
        <price>22.50</price>
    </m: GetLastTradePriceResponse>
</SOAP-ENV:Body>
```

Fig. 4: SOAP Parser

Simple Object Access Protocol (SOAP) is a platform independent communication protocol, which is used to communicate between the applications. SOAP uses XML message format. SOAP also uses other protocols such as Simple Mail Transfer Protocol, HTTP and even TCP for communicating with the other applications. As in Fig.4 SOAP message is divided with different parts Namespace, Header and Body.

Namespace: In fig.4 the elements and the attributes of the message is defined in the first namespace. The SOAP also uses the RPC protocol to communicate. For encoding the message the SOAP uses predefined elements.

Header: The header element is the first child element. The SOAP Header is written using XML. This holds the authentication codes and other secured transactions. By using XML web services, client can send and receive headers. Here in Fig.4 mstUdst attribute is used in the header. The value the attribute is set to 1. When the value is set to 1 the server accepts the message and performs the transactions. If the server is not able to understand the transactions then it will be marked as error or send as fault. And the message will be sent to client by the server. If the mstUdst value is as 0 then it is left as optional and no special processing will done. Only using SOAP Envelope and add Header method the SOAP header is created.

Body: The body element is the mandatory part in the SOAP. As in Fig.4 the body uses the RPC and the XML. The XML is used to encode the request and response. The encodings in the body element can also be disabled. It's not compulsory thar we enable the encoding style in the SOAP body. The text in the body should be nested inside the child element. The request and response are the two patterns by default. The message exchange in SOAP is same as the web browser communicates with the server. The initial request will be sent by the client and not by the server.

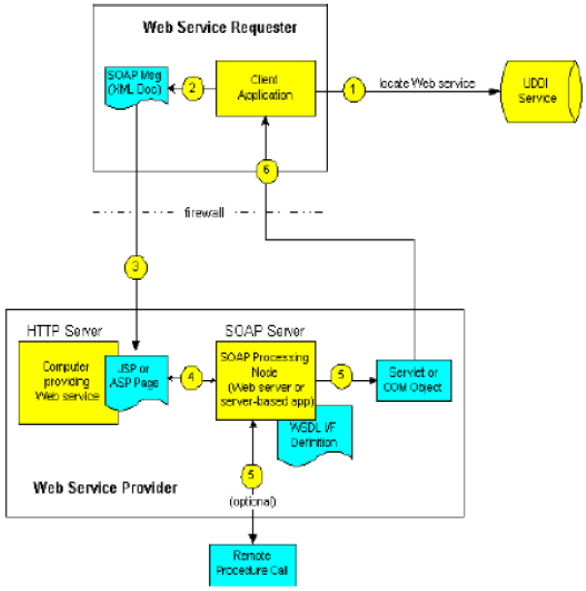

Fig. 5: SOAP processing Steps in Use-case

A SOAP client uses the UDDI registry to locate a Web service as in Fig.5. Rather than manipulate WSDL directly, in most cases a SOAP application will be hardwired to use a particular type of port and style of binding, and it will dynamically configure the address of the service to be invoked to match the ones discovered through UDDI. After locating the UDDI service the XML document is done by the client application.

The document is send to the listening HTTP server. The XML document should pass through the firewall in order to send to the listening server. Next it sends to the SOAP server where the processing is done. Here it extracts the packages and the parameters. If the RPC is used then it sends or uses the RPC. It's not compulsory that it should pass through the remote procedure call. Otherwise it will pass through the servlet. The server related process is done in the Web Service provider.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. CONCLUSION

In this paper, using the self-configuration framework we can add devices without rebooting the system. We have used the IBM MAPE-K control loop for the self-configuration of devices. By this we no need to stop our services for adding any new device. This makes the operation easier and faster.

In future research, there are several concepts which can be taken into work. Though people have proposed using agents, but they have discussed the scenarios using broadband forum.

REFERENCES:

[1] Houda Rachidi and Ahmed Karmouch, "A framework for self-configuring devices using TR-069", Proceedings of IEEE International Conference on Multimedia Computing and Systems, pp 1-6, July 2011.

[2] Alonso. V, Fernandez, M.A, Davila, P, Gallegos, D, Castillo, A and Paniego. E, "New Self- Paradigms for Managing Customer Networks", IEEE *GLOBECOM Workshops*, pp. 1-5, January 2009.

[3] Nikolaidis, A.E, Papastefanos, S, Doumenis, G.A, Stassinopoulos, G.I and Drakos, M.P.K, "Local and remote management integration for flexible service provisioning to the home", IEEE *Communications Magazine* , vol. 45, no.10, pp.130-138, October 2007.

[4] K. IBM, Autonomic computing initiative, 2001. Available: http://www.research.ibm.com/manifesto/autonomic_computing.pdf.

[5] E²R2 "End –to-End Reconfigurability II", http://www.e2r2.motlabs.com

[6] DTMF,"Web Services for Management," http://www.dmtf.org/

[7] Steinke, B and Strohmenger, K, "Advanced Device self Management through Autonomics and Reconfigurability", Mobile and Wireless Communications Summit, 2007, pp.1-4, July 2007.

[8] Home Gateway Initiative (HGI), "Home Gateway Technical Requirements Residential Profile Version 1.0", April 2008.

[9] Broadband Forum, "TR-143: Enabling Network Throughput Performance Tests and Statistical Monitoring Issue 1", May2008.

[10] Broadband Forum, "TR-157: Component Objects foe CWMP Issue 1, Amendment 1", September 2009.

[11] W3C Consortium, "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)", www.w3.org, April 2007.