BROADBAND FORUM'S USER SERVICES PLATFORM (USP)

UTILIZING NEW TECHNOLOGIES TO CONTROL AND MANAGE DEVICES IN THE HOME

JOHN BLACKFORD - PRODUCT MANAGEMENT DIRECTOR, ARRIS

ARRIS®

TABLE OF CONTENTS

INTRODUCTION

The home network is growing more and more complex every year with the addition of multiple connected devices such as smart TVs, set-top boxes, thermostats, temperature sensors, cameras, lights, door locks, smoke detectors and others.

There are also more and more services using these connected devices, including pay TV, home automation, home security, telehealth, delivery services and others. Services often overlap, and use the same connected devices, increasing the complexity of permission and privacy; which Service Providers have access to the various connected devices, and at what level of access. At the same time, the home network is becoming more complex, and the homeowner just wants it to work as easy as the electricity, or any other utility.

A new management and control framework, called User Services Platform (USP), has been created by the Broadband Forum. The goal of USP is to fix this problem by providing always-on communications, streamlining control and management messaging and enabling multi-tenant management.

This white paper is targeted at the Operators that provide pay TV, Internet, and Wi-Fi services in the home network. This includes the telecommunications, cable and satellite Operators that nearly every homeowner calls when something goes wrong with the home network or connected devices, whether part of the service purchased through that Operator or not. In this white paper, we explore the difficulties in managing and controlling a home network, how those difficulties lead to problems for the Operators and their customers, and how those problems can be solved through device management and control concepts handled by the Broadband Forum's USP framework.

PROBLEM STATEMENT

The complexity of the home network leads to problems for Operators as they try to provide a high quality of experience for their customers. To address these home networking problems, Operators started by sending technicians to the house, but that was both costly and inconvenient for their customers. The Operators then turned to customer call centers that used remote management solutions to resolve home networking problems.

Operators are now starting to place mobile applications in the hands of their customers, allowing them to resolve their own home network problems and reduce customer support calls. They are also enabling devices in the home network to communicate with each other to resolve issues *before* they impact customers.

There are currently three key device management flavors:

- Remote management
- In-home management
- Machine-to-machine management

The current standards-based management and control solutions only really address the remote management flavor, while others are handled by proprietary solutions. This approach causes long-term problems for Operators, as they become locked into a solution, or worse, dependent on a specific vendor relationship.

To address this problem, we need a standards-based solution that blends both management and control concepts into a single protocol that allows for:

- Always-on communications for fast interactions
- A small code footprint for smaller devices
- A small network footprint for Internet of Things scenarios
- Multiple management entities for multi-tenant management solutions

This solution also needs a sophisticated, yet easy to understand access control mechanism that functions both inside the home network for in-home management, and outside of the home network for remote management. This solution must be able to gather data consistently over time for back-end analysis and detection of intermittent issues, and most of all — *it needs to be secure*.

HISTORICAL APPROACH

In the early days of delivering Internet services into the home, the modem was the only device, and it was directly connected to the computer by a physical wire, if not embedded directly in the computer itself. With only one modem and one computer, there was little need to remotely diagnose problems. Any remote management needs were easily handled by Simple Network Management Protocol (SNMP), which was commonly used to manage parts of the core network.

Then came the age of the residential gateway offering the ability to connect more than one computer to the Internet service by providing a combination of a modem and an Ethernet switch in a single device. It was during this time period that Internet service providers split into two different types of providers.

The telecom/cable split

Telecommunications Operators embraced the residential gateway and offered it as a service, including the first Wi-Fi home network capabilities. However, Cable Operators primarily kept offering modems, and relying upon their customer base to install their own stand-alone gateways behind Operator-provided modems. In addition, remote management split between the two types of Operators.

Cable Operators could stick with SNMP as they were only managing a simple modem, while Telecommunications Operators required a more sophisticated remote management protocol for the more complex residential gateway product. The Telecommunications Operators started with proprietary remote management solutions offered by individual device vendors, but quickly concluded that they needed a standard remote management solution. This is where CWMP came into play. CWMP represents CPE WAN Management Protocol, as defined in Broadband Forum's TR-069 specification. Eventually Cable Operators started offering services that included residential gateways with Wi-Fi capabilities, and also adopted CWMP as well.

New horizons

Emerging from the split, new technologies and new service offerings became available to consumers, causing additional disruption for Operators.

Pay TV services

Pay TV services further expanded the simple analog cable and satellite solutions to include more digital and interactive solutions. The paid TV service offering started to include video on demand, and the ability to order movies at the click of a button. Telecommunications Operators began offering a pay TV service, Cable Operators started combining their Internet and pay TV services, and Satellite Operators started connecting their boxes to the Internet for ordering content, as well as more advanced functionality.

Many Operators started looking at ways they could remotely manage their set-top devices, with several going down the CWMP path. They later abandoned it in favor of proprietary home-grown solutions that met their specific pay TV needs, or for bundled TV platforms that included some rudimentary remote management concepts.

For those Operators, CWMP wasn't the right solution for managing a set-top device — *the focal point of a home entertainment system where interactions are expected to be immediate*.

CWMP was designed to remotely manage residential gateways that are behind the scenes and don’t interact much with other devices, because the residential gateway is fairly self-sufficient once it has been configured.

Wi-Fi

The next major change in the home network environment was the proliferation of Wi-Fi, and the desire of the homeowner to put any device, in any room, without being tethered by a wire — *expecting the device to perform as if it had an endless supply of Internet bandwidth*. Homeowners started turning to start-up companies for home network solutions that would allow them to put Wi-Fi access points anywhere in the house, with the promise of the home network becoming a smart network.

Once again, proprietary solutions were created for managing the devices and these solutions spanned several different flavors of management:

- Communications between Wi-Fi access points in the house
- Delivery of data collected about the home network performance to back-end servers for analysis
- Remote configuration of Wi-Fi access points in the house to create a better user experience

Internet of Things

At roughly the same time as the Wi-Fi explosion in the home network, the Internet of Things (IoT) industry also exploded in the form of home automation and home security solutions, where cameras, lights, door locks, thermostats, temperature sensors, etc. started connecting to the home network —*many of them via Wi-Fi.* In essence, the Wi-Fi and IoT explosions fueled each other*.*

Instead of proprietary solutions for managing and controlling the IoT devices in the home, big consumer electronics companies (e.g. Amazon, Apple, Google), created a small set of closed ecosystem solutions associated with individual IoT vendors. Those closed ecosystems only communicated with other devices in the same closed ecosystem. This forced consumers to either commit to a single ecosystem, or resort to using multiple solutions to manage their entire home.

Some IoT vendors helped address this new challenge by integrating their solution into multiple ecosystems to simplify the management for consumers, but at a larger price tag.

So, where does that leave us?

Residential gateways are managed by CWMP, set-top devices are managed by proprietary solutions controlled by pay TV Operators, Wi-Fi devices are managed by proprietary solutions that are controlled mostly by start-up companies, and IoT devices are managed and controlled by closed ecosystems, preventing communications across ecosystems. Basically, the home network is a complex tangle of devices, and only the most tech-savvy home network engineers can make it work seamlessly.

SOLUTION

The Broadband Forum has created a new solution, User Services Platform (USP), with the goal of controlling and managing devices in the home network. USP is an open standard that was published in beta form for many months and has just recently been formally published (http://usp.technology).

USP blends both management and control concepts into a single protocol, enabling:

- Always-on communications
- Streamlined messaging
- Multiple management entities

USP uses Message Transfer Protocols (MTPs), as referred to in USP terminology, for several different scenarios:

- CoAP for fast in-home communications
- WebSockets for point-to-point communications either in-home or outside of the home network
- STOMP for a message bus driven communications mechanism that can function across almost any home network configuration

USP also has an HTTP bulk data collection mechanism to off-load the periodic, yet regular, collection of home networking data for offline analysis.

And we can't forget about *security*. USP has two different layers of security defined.

- First at the MTP layer, via Transfer Layer Security (TLS) or Datagram Transport Layer Security (DTLS), depending on the MTP in play
- Second at the application layer, with an end-to-end TLS-based USP encryption solution

Always-on communications

When a USP Agent comes online, it automatically establishes a communications channel with the management entities (USP Controllers) that it knows about, and then maintains that communications channel as an always-on means of communicating. This means that when a USP Controller wants to interact with a USP Agent to retrieve some data, configure the device, or invoke a command, it simply sends the request over the open communications channel. This increases the efficiency of USP and reduces the overall latency of communications.

The following figure shows a comparison between CWMP (TR-069) and USP for something as simple as asking the device what its current local time is. With TR-069, the management entity (ACS) and CPE establish a communications channel each time an interaction is required. Whereas with USP, the Controller and Agent simply re-use the always-on communications channel to perform the request.

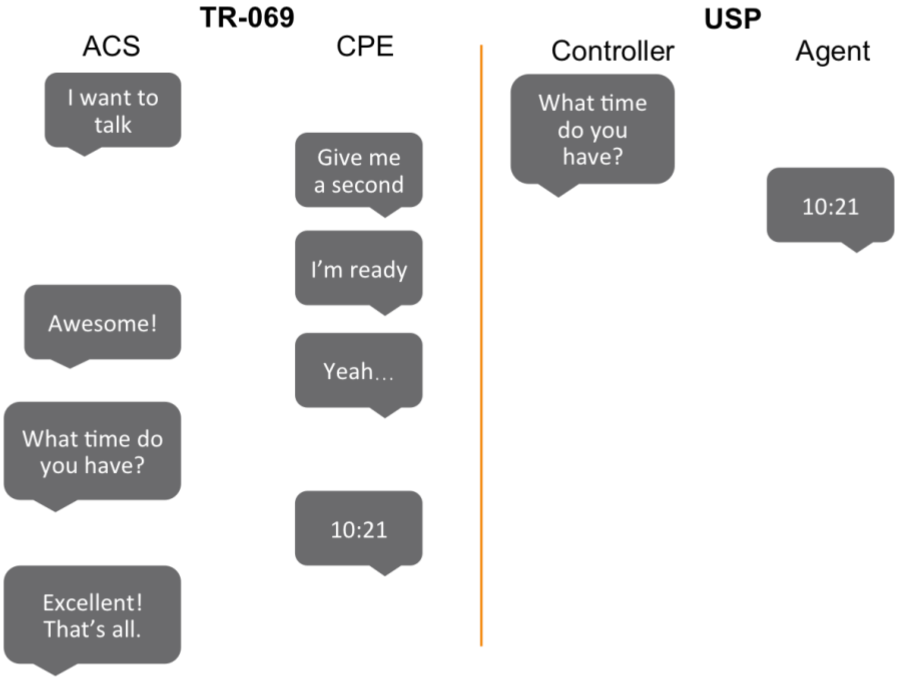

Figure 1 - Comparison of basic communications between TR-069 and USP

Streamlined messaging

The streamlined messaging aspects of the USP protocol messages have been designed to be forgiving, because if we've learned nothing else from our 14 years of CWMP experience, we've learned that different devices implement different data models, even when they have the same basic functionality. The USP protocol messages isolate different parts of the requests and responses so they can fail in isolation instead of failing the entire request.

For example, in CWMP, a request to retrieve four parameters would fail if a single parameter wasn’t implemented by the device. Whereas in USP, that same request would return the three parameters that were implemented and provide an error message for the one parameter that wasn’t implemented. This increases the efficiency of USP by reducing the discovery process, which in turn reduces the number of communications transactions required.

Furthermore, USP tackles the long-standing concern about the CWMP hierarchical data model structure that causes responses to be overly verbose. USP uses *relative paths* in responses instead of constantly repeating the portion of the parameter path that was in the request. Reducing message sizes further increases the efficiency of USP.

Multiple management entities

The USP protocol allows for more than one management entity (USP Controller) to interact with a USP Agent at any given time. This means that multi-tenant management, where multiple Operators can manage the same devices at the same time, is now a real possibility. And, Operators’ customers are empowered to manage and control their own devices at the same time as the Operators. All of this is made possible by USP's role-based access control mechanism that allows different USP Controllers to be assigned different sets of permissions based on the device capabilities with which they interact.

For example, an Internet Service Provider (ISP) could be given permission to interact with the home networking aspects of all devices in the house, while not given permission to access the camera's recording or playback abilities. And, at the same time, a Home Security Service Provider could be given permission to access the camera's recording and playback abilities, while not having any permission to access the home networking aspects of the cameras. This accelerates the time to market for new home networking services for USP-based devices, as there is no longer a single management entity acting as the gatekeeper of the entire home network.

So, which home networking devices will benefit the most from a USP adoption perspective? *All of them!* USP can be utilized on residential gateways, either as a replacement to CWMP, or in conjunction with CWMP.

Since USP re-uses the Broadband Forum’s Device:2 root data model (TR-181 Issue 2), it simplifies the migration from CWMP to USP. The adoption of USP benefits both operators and consumers due to the following capabilities.

- More efficient and faster than CWMP, so it can also be utilized on IoT and set-top devices
- Serve as a secure machine-to-machine protocol inside of the home for handling frequent messages that require low latency to automatically optimize the Wi-Fi home network

- Support back-end analysis with a remote management optimization path because of its bulk data collection mechanism
- Unify the management of the home network

Conclusion

The Broadband Forum's User Services Platform solution provides the control and management infrastructure needed for the homeowner, the Operator and the various Service Providers to each take control of the home network as it continues to grow in complexity. USP addresses all the pain points we have today with remote management by delivering:

- Faster interactions
- Support for smaller devices
- A smaller management traffic footprint on the network
- Multi-tenant management
- The ability to work both inside and outside the home
- An efficient data collection mechanism
- Security

USP also provides a smooth migration path from existing CWMP solutions as it can co-exist with CWMP on the CPE, allowing the existing access control system to continue performing its daily duties, while new USP Controllers can be introduced for more agile solutions.