SCTE CABLE-TEC EXPO '13
OCTOBER 21-24 / ATLANTA, GA

SCTE Society of Cable Telecommunications Engineers

Customer Experience Management

Leveraging Device Management to Improve the Wi-Fi Experience

A Technical Paper prepared for the Society of Cable Telecommunications Engineers
By

Ellis Lindsay
GM, Customer Experience Solutions
Alcatel-Lucent
Ottawa, Canada
+1 (613) 784-1528
Ellis.lindsay@alcatel-lucent.com

Overview

Network operators around the world have begun to deploy public Wi-Fi networks for their subscribers, and others, to use. Designing, deploying, and operating a public Wi-Fi network encompasses only part of the overall service delivery requirements. From an end user perspective, having a Wi-Fi network available to connect to is only a small part of the expectation set.

Wi-Fi enables MSOs to extend their reach beyond their traditional networks. Subscribers demand a simple, seamless, and secure experience with Wi-Fi networks, and MSOs require that these deployments be both efficient and cost effective.

Device management protocols, such as TR-069 and Open Mobile Alliance's Device Management (OMA-DM), enable service management platforms to perform end to end analysis on a service then diagnose and resolve issues both reactively, and when coupled with real-time and analytical monitoring services, proactively as well.

This paper will introduce Wi-Fi deployment models, device management for both access and end user devices, and discuss the use of those key experience influencers and enablers to achieve customer experience management goals.

Contents

INTRODUCTION

Customer Experience Management is about ensuring a superior experience throughout the lifecycle of a product or service. In the context of online and data services, the critical touch points are between when a subscriber decides to get a service, through usage, to issue resolution. These touch points, also characterized as Get, Consume, and Support, are directly related to the devices and technologies encapsulated within the services being purchased.

For Wi-Fi services, both public and private, indoor or outdoor, there are many factors that can impact a customer's experience. It is this set of factors that are addressed by customer experience management techniques to deliver a high quality experience.

CONSUMER ADOPTION OF WI-FI

Wi-Fi has come of age, thanks to end-user device support as well as standardized improvements in the technology. As a result, carrier Wi-Fi is now an important strategic initiative that cable operators of all types want to, and are beginning to, leverage. For many operators, it's destined to become an important component within their overall mobile broadband strategy to keep their subscribers connected to the MSO network and services.

The flexibility of Carrier Wi-Fi means that it can be deployed in many different market applications, resulting in reduced churn, enhanced customer loyalty and brand value as well as opening up possibilities for new revenue streams. We see applications such as wireless network offload, home network and service extensions with community Wi-Fi, which has recently been termed 'Homespot' where home wireless router cable modems have a secondary SSID that is used to offer WiFi to the neighborhood with no impact on the subscriber's service within the home, and general urban hotspot deployments - as well as specific venue coverage.

MARKET DRIVERS

MOBILE BROADBAND AND NEW DEVICES

Wi-Fi is here now. It's used on many different devices every day - and its use is on the rise. According to the Wireless Broadband Alliance, the 1.3 million Wi-Fi hotspots seen worldwide in 2011, is forecast to grow 350% to 5.8 million by 2015. The fact that 70% of users are in Wi-Fi coverage more than 70% of the time during the day shows the great potential of Wi-Fi. Nearly all new devices coming to market today feature integrated Wi-Fi. Smartphones, tablets, net-books, laptops, game consoles, e-readers, even cameras all support Wi-Fi. Wi-Fi is effectively an expected feature in consumer electronics.

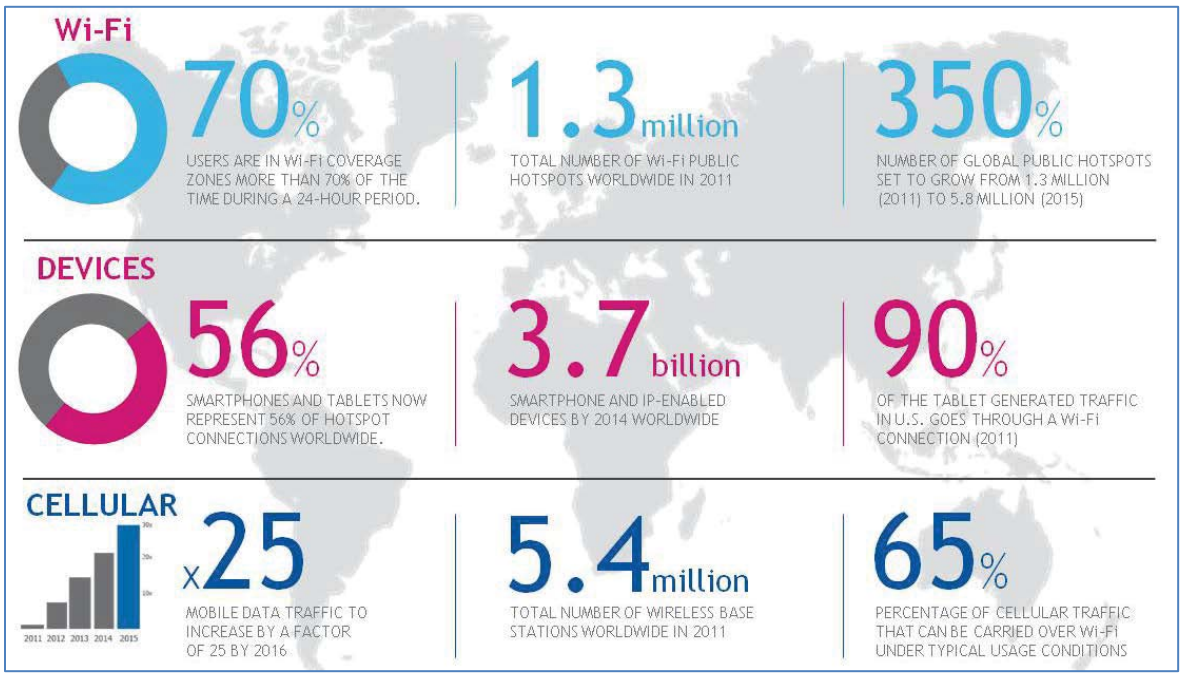

Figure 1 Wi-Fi Related Market Data, Alcatel-Lucent market analysis

TECHNOLOGY EVOLUTION

Furthermore, Wi-Fi has evolved significantly. Recent developments in the international standard bodies have stimulated further Wi-Fi adoption by addressing some of the previous key concerns such as;

- Performance: IEEE technology enhancements have been aimed at wider and different spectrum band (such as IEEE 802.11ac) usage. They also target the application of variants of the techniques which are common in the cellular world, e.g. multi-user, multiple input, multiple output (MU-MIMO) technology.
- Security and Authentication: driven by Wi-Fi Alliance (WFA), HotSpot 2.0 facilitates and automates secure and trusted Wi-Fi connections by enabling a variety of user or device-based credentials to be used in these connections. Hotspot 2.0 promises to help automate network discovery, connection and authentication – steps that today are often manual when a Wi-Fi user connects to a given hotspot.
- Policy: 3GPP defined the Access Network Discovery and Selection Function (ANDSF) to deliver policy driven network access enabling the use of the best available or preferred access, along with roaming between cellular and Carrier Wi-Fi access.

CONSUMER USE OF WI-FI

In 2012, 90% of tablet traffic in the United States used Wi-Fi, impacting fixed broadband, rather than cellular mobile networks. In addition, 78% of smartphone traffic is accessed through Wi-Fi today [1]. This demand appears to have been created by the common adoption of the latest 802.11-related specifications and industry initiatives.

WI-FI DEPLOYMENT MODELS

When consumers hear the term “Wi-Fi”, it is reasonable to expect that they think of connecting the electronic devices that they purchase to their home networks. It is also reasonable to expect that they equate Wi-Fi service with free. This home Wi-Fi is one of several deployment models that must be considered in assessing the end-to-end customer experience.

Home Wi-Fi, along with community, enterprise, and outdoor pole or building-mounted Wi-Fi make up the spectrum of Wi-Fi deployment models.

The existing North American multiple system operator (MSO) Wi-Fi deployments describe their access points as either “Indoor” or “Outdoor”. While this provides some indication to the user’s potential signal availability in an area, it relates more to the type of access point that has been deployed. The primary difference being that outdoor access points are designed to withstand the harsher environmental conditions prevalent outdoors.

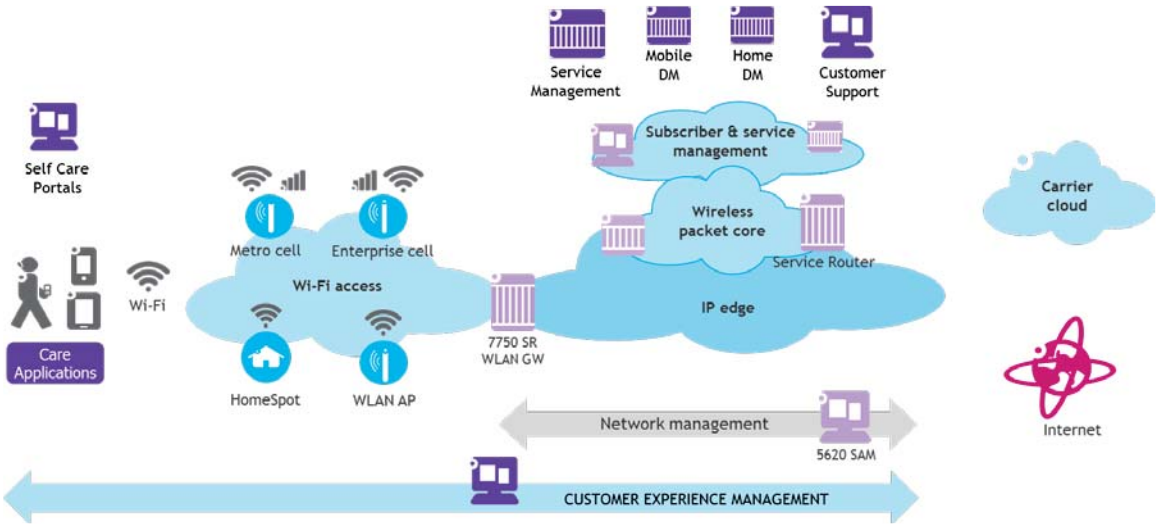

Figure 2 Wi-Fi Deployment Models

INDOOR WI-FI

Home Wi-Fi

Home Wi-Fi has become common, being generally provided with high speed internet access services as a feature of the integrated residential gateways. This type of CPE typically has an access network specific WAN connector, multiple LAN ports, Wi-Fi, and possibly additional ports such as USB.

The Home Wi-Fi CPE can also be used by small businesses to provide data services to the location. A coffee shop providing Wi-Fi services is a simple example of this usage.

Community Wi-Fi

Community Wi-Fi is the term used to describe a public or carrier Wi-Fi service that takes advantage of a residential home gateway. To do this, the CPE is configured with a public Wi-Fi service profile in addition to the home private Wi-Fi profile. All devices with this profile broadcast the same public SSID. Depending on the service architecture and design, customized CPE firmware may be required.

Configuration of the public profile on the device differs from the home Wi-Fi profile in that it cannot be set by the subscriber directly. It is pushed to the device in a configuration or boot file after service terms are accepted. When remote management systems are used, such as the Broadband Forum's TR-069, individual parameters can be set instead of a complete device configuration file.

OUTDOOR WI-FI

Outdoor Wi-Fi generally involves the use of weather proof access points that are pole or building-mounted. Outdoor Wi-Fi networks are managed differently than community Wi-Fi networks. Whereas community Wi-Fi uses home device management systems, outdoor AP's are managed using the vendor supplied control system. These may or may not be standards-based, and are designed for operational purposes.

From a profile perspective, the parameters required are generally the same for all deployment models. The exceptions being either for proprietary features or technology limitations of the access point.

ENTERPRISE

Enterprise Wi-Fi is similar in nature to outdoor Wi-Fi, but may use a mixture of indoor and outdoor access points. It is a managed private network, but with restricted access based on enterprise credentials. When deployed as part of a carrier Wi-Fi network, the subscriber credentials are used in place of the enterprise's directory services for authentication.

Enterprise Wi-Fi is a separate, although related, segment that will not be discussed in this paper.

PRACTICAL DEPLOYMENT MODELS

As part of the service provider's solution definition, the community Wi-Fi network can be either open or secure. Open networks only require users to select the SSID from the list of available networks seen by their device. There is no passphrase or other credential required to set up the network connection. However, the user may be required to pass through a captive portal by signing in or signing up to the service.
Secure networks require that the access point be configured to require credentials. These credentials may be a passphrase or a more secure method such as EAP-TTLS. The user and end device must be preauthorized and the end device be provisioned with the access credentials.

While each of these models has their own benefits and considerations, a combination of models appears to be the most effective at delivering Wi-Fi services. Current market activity indicates a combination of outdoor and community Wi-Fi models are being used to provide public Wi-Fi service to subscribers.

North American MSOs that have deployed Wi-Fi services have used a combination of community, or indoor, and outdoor Wi-Fi for their service offers. The Cable WiFi group (http://www.cablewifi.com/) partners show where their various indoor and outdoor hotspots are to help their customers find service.

Each of these deployment models has its own set of customer experience requirements. Addressing the resultant needs requires a broad approach. Device management is a fundamental enabler of customer experience management for Wi-Fi.

MANAGING THE CUSTOMER EXPERIENCE

COMMON CUSTOMER EXPERIENCE ISSUES

In order to understand the customer experience issues in managing Wi-Fi as a carrier service, we can look at how operators are currently managing 3G/4G broadband services and triple-play services in the home.

In the customer experience lifecycle, there are three key touch points that have direct relationships to communications services and their technologies. These three are Get, Consume, and Support.

Get: This touch point involves provisioning and activating the service and associated equipment and devices so that it can be consumed; for example, the remote configuration of a cable gateway.

Consume: End users actively using services on their associated device(s), e.g. browsing the Internet on their PC

Support: When service expectations are not met, end users call customer support or use self-service tools to diagnose, troubleshoot, and resolve their issues.

Customer Experience Management addresses these three touch points from a technology perspective. Using readily available technologies and standards enables MSOs to deliver high quality services with a positive customer experience at the lowest possible cost.

THE *GET* TOUCH POINT

Activation is the portion of the get touch point which goes beyond BSS and OSS interactions to involve the CPE and end point devices. It involves setting up the services and the devices for the consumer. In the case of Wi-Fi services, this includes the customer accepting service terms and conditions as well as the expected device configurations.

Captive portal-based applications are typically used for driving the operational support systems (OSS) and business support systems (BSS) interactions as well as the service term acceptance. These portal applications are generally bespoke development by either internal IT teams or are performed through professional services engagements.

Beyond the required end-user interactions in the service activation processes, the device activation processes pose a greater customer experience management challenge.

Setting up home Wi-Fi involves the consumer logging in to the device and enabling the Wi-Fi features. This process includes selecting the version(s) of 802.11 to use, i.e. 802.11 a, b, g, n, ac, in addition to selecting the 2.4 GHz band or 5 GHz band as applicable. In addition, the consumer must name the Wi-Fi network, set security methods if desired, enter a passphrase, and print out the settings so that they may be remembered and entered into a client device.

This end-user involvement creates a high risk for error and misconfiguration of devices. This leads to connectivity and service performance issues that may not be detectable without device management capabilities.

THE *CONSUME* TOUCH POINT

Once activated, with devices properly configured, end-users can consume the Wi-Fi services. On an ongoing basis, end-users are likely to change their environment. New mobile phone models are released, new tablet devices come to market, and technology and social changes tend to result in devices being added and removed from networks.

Adding devices to a network is not complex, although end-users must know the network name and their login credentials in order to connect. For secure networks, the device must be known and trusted in order for connectivity to be established. Open Mobile Alliance's OMA-DM specification can be used to provision Wi-Fi profiles on devices so that connectivity can be established without additional end-user intervention.

Similar-behaving mobile devices may not necessarily be configured using the same methodologies. For example, both Google Android and Apple iOS-based devices automatically join Wi-Fi networks when possible. However, the methods used to configure their Wi-Fi profiles are different. Android can leverage OMA-DM to configure a profile, while iOS uses Apple notification services. As a result, implementing applications to enable a simple customer experience requires additional effort for additional supported device types.

Operationally, metrics can be gathered from end point devices and access points in order to monitor performance and issues so that proactive care can be performed.

THE *SUPPORT* TOUCH POINT

End-users will have issues that will result in them contacting customer care through either the telephone or an alternative channel. The benefits of using device management for activation and changes is that it enables the ability to identify, diagnose, and resolve customer issues. These issues may include an inability to connect, slow connectivity, device misconfiguration, or changes in service profile.

Customer support has evolved from being telephone support only, to interactive voice response (IVR), web, and more recently to web and on-device application based self-care using for example TR-069. These different support channels are changing the way that support can be delivered.

While many service providers still deliver FAQ-based linear or trial and error based care, the ability now exists for end-users to benefit from real time visibility of device and system settings and metrics.

A user can now use their mobile data connection to diagnose the connectivity of a different device on a Wi-Fi connection.

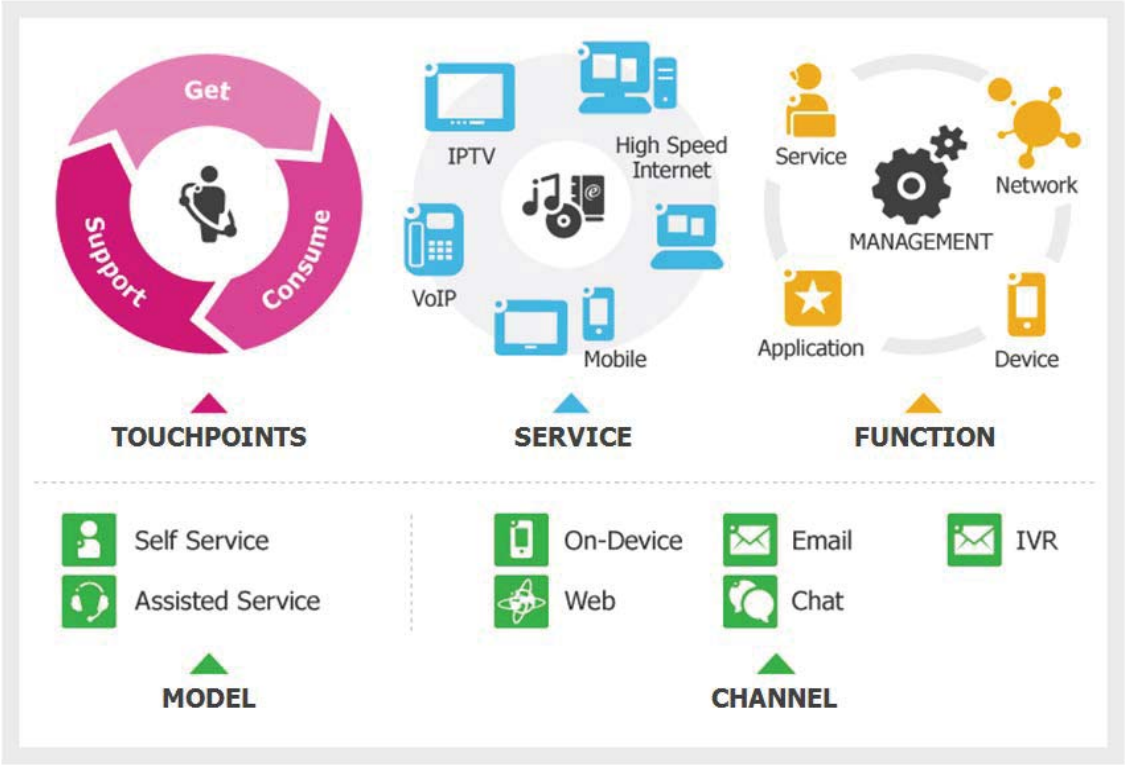

Figure 3 Customer Experience Management Elements

THE ROLE OF DEVICE MANAGEMENT

Device management is an important aspect of enabling the customer's Wi-Fi experience. It provides several benefits to both operators and end-users.

Device management protocols allow the service provider to remotely:

- Configure and manage Wi-Fi networks within the customer premises without interaction by the customer
- Monitor and troubleshoot Wi-Fi networks by collecting performance statistics and other operational data for access point and end point devices
- Configure and install Wi-Fi connection profiles on end point devices
- Verify end point device settings to troubleshoot connectivity and service issues

The enablement that is provided by device management to Customer Experience Management is quite significant. When considered in the context of the Customer Experience touch points of Get, Consume, and Support, device management plays an integral role is delivering the desired experiences. It allows the customer to reduce their involvement in many processes.

For example, in the Activation processes which are required when the consumer wishes to Get a service and Consume it on a device. Without device management, a low-touch process would not be possible when the consumer upgrades from a basic cable modem to a Wi-Fi gateway for their DOCSIS® service. Consumers would be required to manually configure devices instead of using streamlined processes to push or pull configuration parameters to their devices.

Common standardized protocols are Broadband Forum's TR-069 Family of Specifications and Open Mobile Alliance's Device Management protocols. When used together, a Wi-Fi service provider has detailed visibility into the devices sending and receiving Wi-Fi signals, including mobile devices. This enables the service provider to support customers and gain insights into their service.

TR-069 FAMILY OF SPECIFICATIONS

DESCRIPTION

The Broadband Forum has developed a series of specifications that have been termed the TR-069 [2] Family of Specifications. These specifications provide the capability to manage CPEs within the connected home. MR-239 Broadband Forum Value Proposition for Connected Home [3] provides an overview of the value proposition for utilizing the TR-069 family of specifications for the connected home.

This family of specifications and functionality enables service management platforms to orchestrate the use of device data and parameters in workflow processes. It is in this manner that issues can be diagnosed and resolved with minimal, if any, end-user interaction.

FUNCTIONS

The TR-069 family of specifications is intended to support a variety of functionalities to manage a collection of devices, and includes the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Firmware image management
- Software module management
- Status and performance monitoring
- Bulk data collection
- Diagnostics
- Proxy Management

ARCHITECTURE

The TR-069 family of specifications is anchored by the TR-069 specification for the base CPE WAN Management Protocol (CWMP) protocol that includes the capability for the Auto-Configuration Server (ACS) to manage devices that are CWMP capable as well as devices that are proxied behind a CWMP capable device.

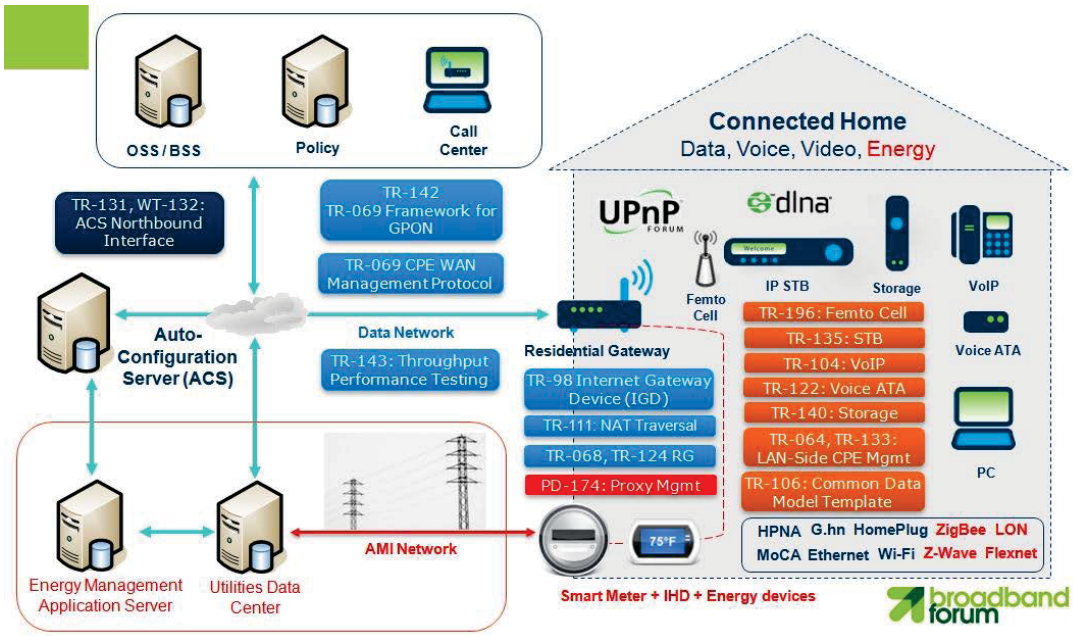

Figure 4 TR-069 Family of Specifications

In addition, Service Providers are increasingly interested in retrieving large quantities of data from their installed CPE base at regular intervals. The amount of data being requested represents a significant portion of the CPE's data model and is thus a large

amount of data. In response to this, the Broadband Forum has documented a data collection solution in TR-232 Bulk Data Collection [3]. This specification is based on the Internet Protocol Detail Record (IPDR) protocol from the TMForum [4].

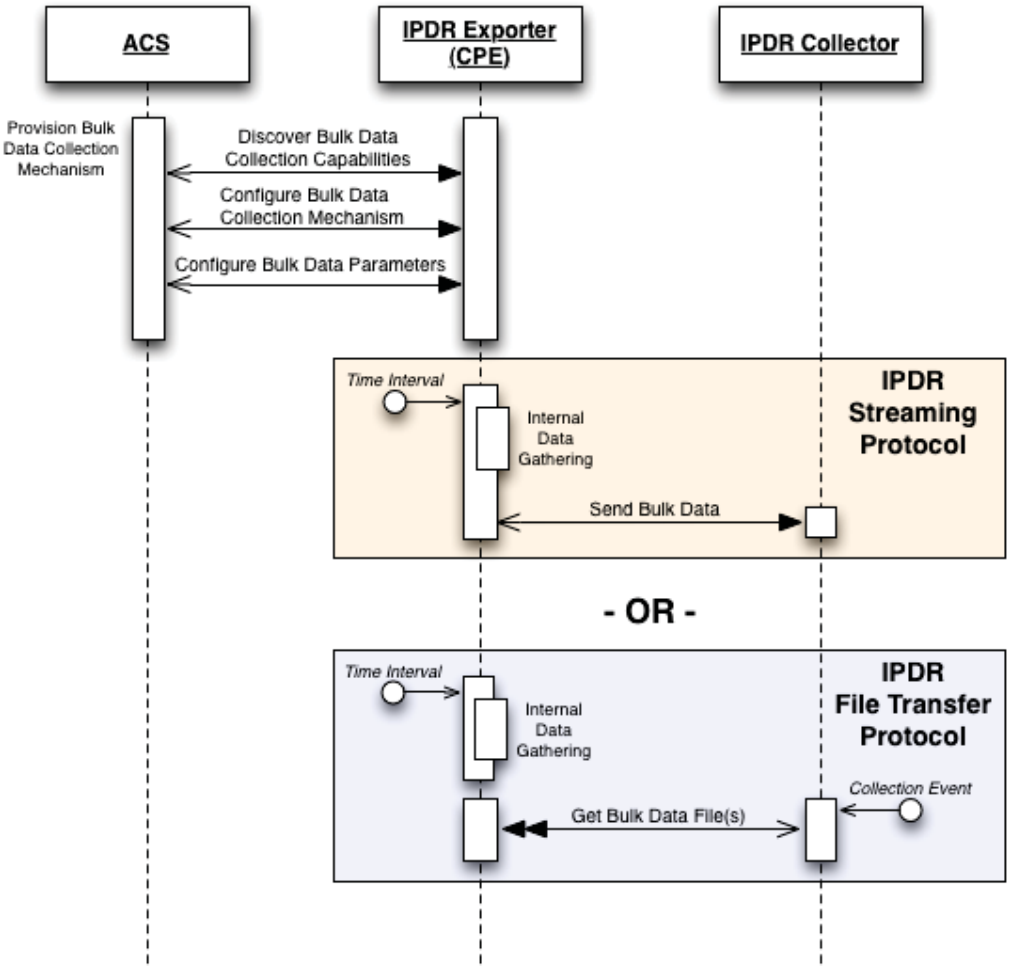

Figure 5 TR-232 Bulk Data Collection

TR-069 PROXY MANAGEMENT

CWMP can be extended to devices that do not have a native CWMP Endpoint of their own, but instead support another management protocol or "Proxy Protocol". A CPE Proxier is a CPE that supports a CWMP Endpoint(s) and also supports one or more Proxy Protocols (e.g., UPnP DM, Z-Wave, ZigBee). A CPE Proxier uses these Proxy Protocols to manage the devices connected to it, i.e. the Proxied Devices. This approach is designed to support Proxy Protocols of all types that can exist in the CPE network now or in the future. Annex J of the BBF TR-069 CPE WAN Management Protocol provides an overview of CWMP Proxy Management.

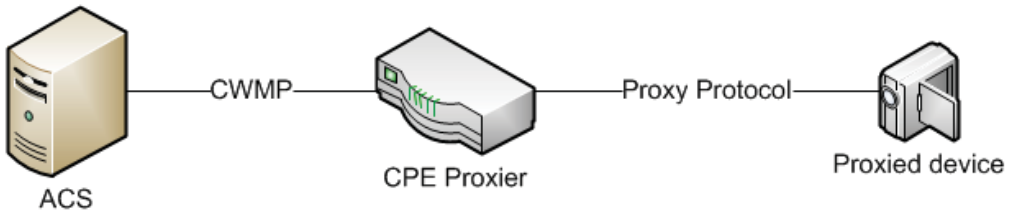

Figure 6 Proxy Management Terminology

WI-FI DEVICE MANAGEMENT USING TR-069

The Broadband Forum manages Wi-Fi networks using the device data model defined in TR-181 [4]. The TR-181 data model contains objects and attributes that permit the auto-configuration and troubleshooting of Wi-Fi networks in the customer premises. The TR-181 data model's objects and attributes are accessed using CWMP or are collected in bulk by the IPDR protocol documented in TR-232 [5]. The TR-181 data model allows for multiple Wi-Fi networks and Radios within a device enabling the use of both customer and service provider defined networks within the customer premises.

Configuration of Wi-Fi Networks

The TR-181 data model has the objects and attributes that permit configuration of Wi-Fi networks for Customer (guest, home, office) and Service Provider (Hotspot) use. These objects include:

- Wi-Fi profiles to setup a Wi-Fi network (e.g., Security mode, SSID)
- Control of the attributes associated with the Radio (e.g., Channel selection, Transmit Power, Operating Frequency Band and Supported Standard) and SSID layers
- Configuration of the Access Point (e.g., Security, Radius Authentication and Accounting, SSID Advertisement, WMM and U-APSD Capabilities, AP Isolation)

Troubleshooting of Wi-Fi Networks

The TR-181 data model has defined the objects and attributes that permit viewing of the topology of devices attached to Wi-Fi networks within the customer premises as well as statistics associated with the devices (i.e., AP, End Point) as well as the Wi-Fi network. These objects include:

- Radio statistics (Bytes and Packets transmitted, received, discarded, errors) and operational (e.g., Status, Maximum Bit Rate, Supported Frequency Bands, Supported Standards, Possible Channels) parameters
- Wi-Fi network statistics (Bytes and Unicast, Multicast, Broadcast Packets transmitted, received, discarded, errors) and operational (e.g., Status, SSID, BSSID, MACAddress) parameters
- Access Point operational parameters for the AP (e.g., Status, Retry Limits) and each associated device (e.g., Presence, MACAddress, Authentication State, Data rate, Signal Strength, Retransmissions)

THE OMA-DM STANDARD

DESCRIPTION

OMA DM [6] is a device management protocol defined by Open Mobile Alliance (OMA). It is typically used to configure and monitor mobile devices. OMA DM has achieved commercial deployment of 1.4 Billion devices. One major feature used by many of these devices is the Firmware Update Management Object (February 2012).

In a wireless environment, the crucial element for device management protocol is the need to efficiently and effectively address the characteristics of devices including low bandwidth and high latency and to provide for support of these management operations remotely and over-the-air. With this in mind OMA-DM has been designed to support mobile specific features such as out of band device triggering, an optional binary XML format, and a device initiated alert mechanism and mobile specific bootstrap using smartcard.

The protocol has been designed as an extensible framework with information and operations exposed by the DM client in the Device via a logical interface, the Management Object (MO). Management Objects are XML based structures defined in the standard.

ARCHITECTURE AND PROTOCOL

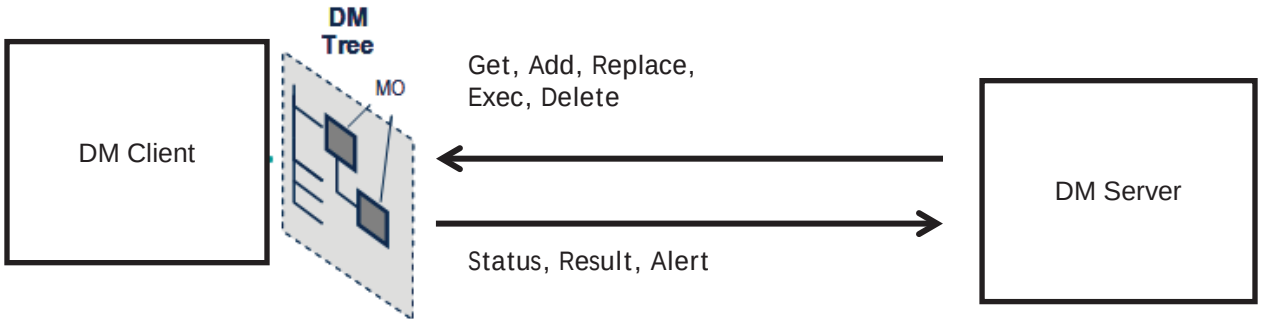

Figure 7 Device management protocol

OMA DM is a protocol that enables a DM Server to send commands to a DM Client residing on a Device and to receive command status reports and unsolicited messages (alerts) from the Device.

The resources of the device that are exposed by the DM Client are represented as a tree structure of Management Object instances with nodes holding the values. The protocol defines the following commands : Get to read values, Replace to set the value, Add to create a new node or subtree, Delete to remove of a subtree or a node, Exec to execute a predefined function defined by a node.

OMA DM Protocol Flow

A typical OMA DM message exchange is shown in Figure x.2. The protocol is based on XML formatted messages that are exchanged during an OMA DM Session. Five message types, called packages, are defined each playing specific roles during the protocol exchange.

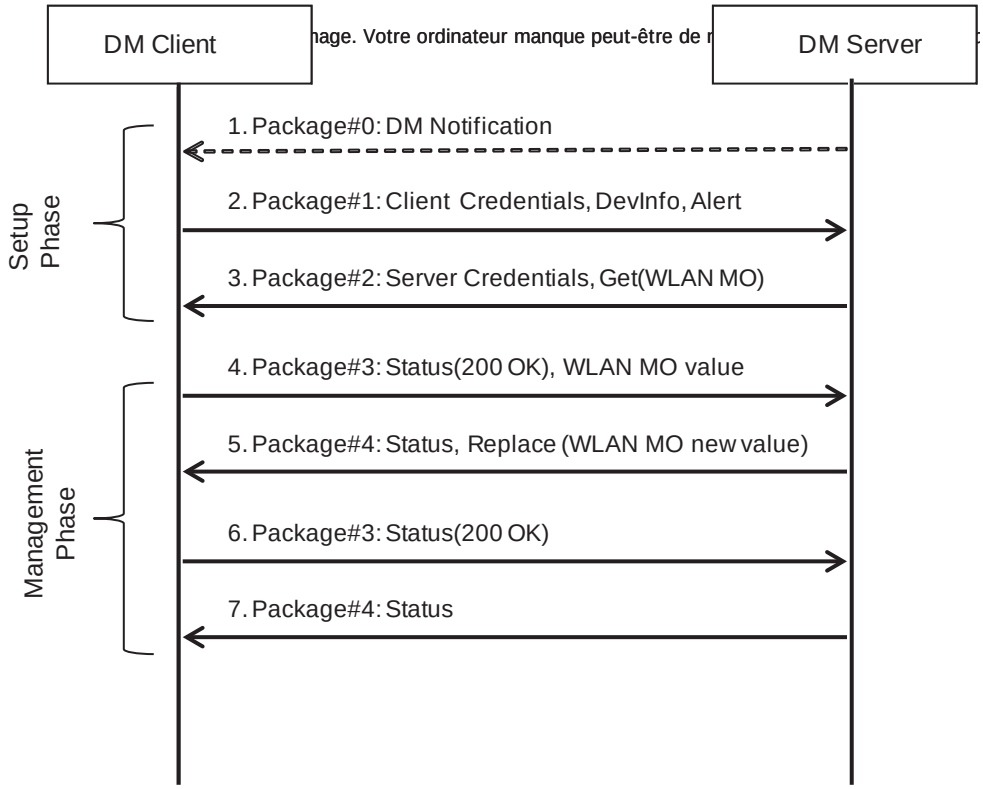

Figure 8 OMA-DM typical flow

A first phase takes place to setup the DM Session. Sessions are always established by the DM client sending package#1 with Client credentials and device information including device identification, make and model (step 2). The DM Server then sends package#2 with Server Credential and first management commands (step 3). The DM Server can request the DM Client to open a DM session by sending an out of band notification as a first step (step 1). This is not required for Device Initiated sessions.

The exchange continues in the Management Phase for as long as the DM Server sends commands to the Device. DM Client and DM Server exchange package #3 and package #4 for as long as needed. Step 5 and 6 can be repeated. The DM Server indicates the end of the DM session by sending a package#4 without commands.

Several other scenarios are supported in the protocol and are not shown here. For example, the Device may send alerts to the DM Server, packages may include

sequence of commands, deferred command results may be send in alerts in further DM Sessions, user interaction commands may be sent by the DM Server.

OMA DM supports several transport bindings for DM messages exchange over a DM session. Typically HTTP over TCP/IP is used. However mobile Devices are not always reachable by a public IP address from the DM Server. Therefore DM defines an out of band trigger mechanism (Server notification on package#0) which requests the Device to establish the DM session with the server. Typical service provider deployments use OMA Push over SMS as a transport binding for package#0, but a number of other bindings have been defined including SIP transport. In addition vendor specific notification transport mechanisms may be used - for example, Google Cloud Messaging on Android devices for Wi-Fi only devices.

FUNCTIONS AND MANAGEMENT OBJECTS

The device management functionalities are achieved by the Management Objects (MO) defined by OMA and other organizations. Examples of supported features include:

- Schedule and automate device management tasks
- Configure connectivity
- Update firmware
- Diagnose problems
- Monitor performance
- Install and update software
- Lock and wipe personal data
- Manage device capabilities

DM tree and Device Description Framework

OMA DM uses Management Objects to describe the syntax and the semantics associated with a specific resource within a Device. Figure 9 shows the standard definition of an MO that is used to represent WLAN bearer specific parameters in a device. Each node of the MO is specified with its format, access types and supported values.

Such a MO is a template for a subtree that may be instantiated at runtime by the device when they correspond to static resources (e.g. battery…) or may be created by the DM Server when such dynamic creation is possible (e.g. connectivity parameters). All MOs are instantiated and named using a path to the DM root thus forming the DM tree.

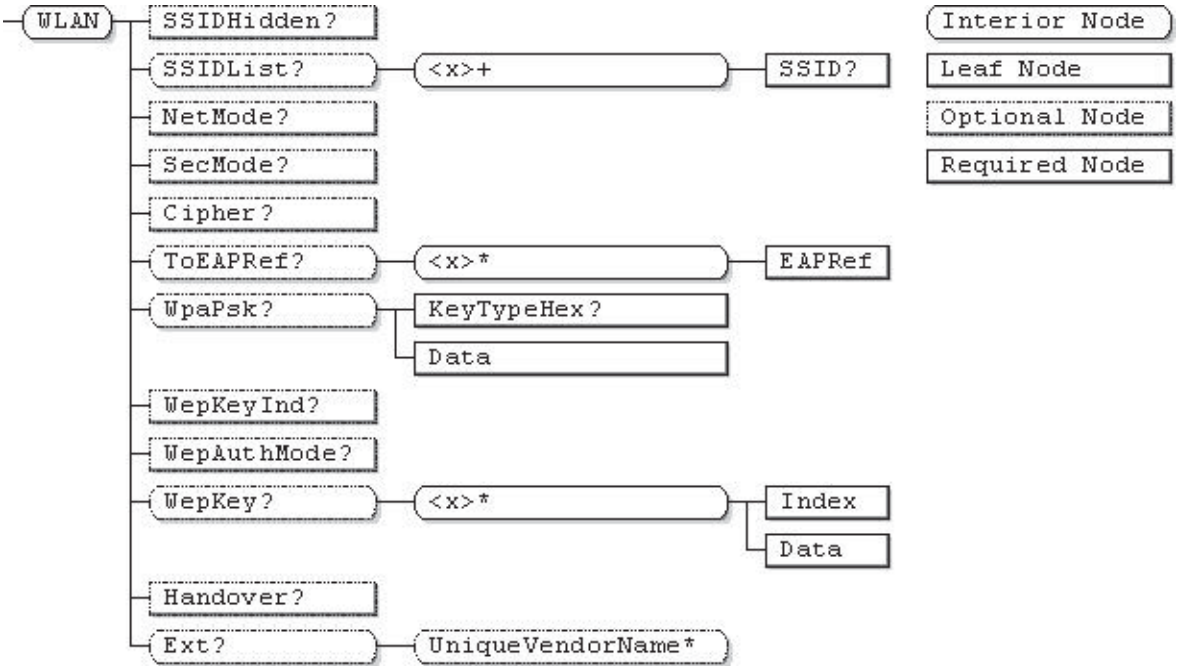

Figure 9 WLAN Management Object

OMA DM Management Objects may be standardized by OMA and external standard bodies.
In addition vendors may also develop Management Objects in a vendor specific fashion. As different management systems still need to understand the management objects for each individual device that may come from these varying sources, OMA developed device description framework (DDF). In short, this framework prescribes a way for device vendors to describe their devices so that a management system can understand how to manage the device.

Using the Device Description Framework, a device vendor will eventually merge standard defined MOs with its vendor extensions and provides its Device Description (DDF) to the DM Server in an XML machine readable format.

WI-FI DEVICE MANAGEMENT USING OMA-DM

OMA-DM protocol stack and architecture is applicable to the management not only of Cellular devices but also mixed Cellular/Wi-Fi devices or Wi-Fi only devices. OMA and other standard bodies have developed Management Object specifications that are geared to the configuration and monitoring of Wi-Fi network settings in mobile devices.

OMA Wi-Fi related Management Objects

OMA DM protocol standard objects (e.g. DevDetail MO) support features to report the current bearer in use (WLAN or other), and the preferred bearer to be used for the OMA DM session.

OMA DM ConnMO [7] is a series of MO specifications which defines common bearer configurations and Wireless LAN (e.g. WLAN MO) bearer specific parameters in order to have a complete standardized Network Access Point definition for WLAN connectivity settings in the OMA DM management tree.

OMA DM DiagMon [8] defines a Diagnostics and Monitoring framework and specific functions applicable to Wireless bearers.

OMA DM DCMO [9] OMA Device Capability Management Object allows to remotely enable and disable device features and in particular the WLAN connectivity.

Network selection policies and Wi-Fi related Management Objects

Two standardization efforts are underway to answer to the need for setting Network Selection Policies in multi-operator, multi technology radio access networks: 3GPP Access Network Discovery and Selection Function (ANDSF) function and the Hotspot2.0 (HS2.0) Wi-Fi Alliance (WFA) initiative.

ANDSF is a cellular technology standard which allows an operator to provide a list of preferred access networks with policies for their use up to the granularity of a single IP flow or all traffic for a given PDN network (APN).

WFA Hotspot2.0 is a Wi-Fi technology standard that allows devices to more easily discover Wi-Fi roaming relationships, determine access point capabilities and loading conditions, and more easily connect to Wi-Fi networks securely. Release 2, currently under development, will allow a service provider to download network selection policies to the device. These policies will be used by the connection manager to select roaming partners depending on the device context and location. Service providers will be able to configure rules based on network load or roaming partner selection.

Both organizations, WFA and 3GPP, have selected OMA DM protocol and have defined their own Management Objects to represent the standard data model and behavior.

USING DEVICE MANAGEMENT

Customer service tools that leverage TR-069 device management solutions can help cable MSOs improve customer satisfaction, differentiate themselves from the competition, and enhance the bottom line. Studies have shown that 70% of customers who switch to a competitor do so because of poor customer service. So delivering good customer support is a critical business imperative, and it can be a key differentiator for cable providers in the connected home.

The "connected home" has become a complex array of devices, applications, and services, all knitted together with user-challenging home networking technology. When something doesn't work as it should, the customer support center is likely to get a call. The customer experience that plays out during this interaction could have a significant impact on the consumer's perception of the service being provided.

A high-quality customer experience is a powerful asset that inspires loyalty, generates up sell opportunities and attracts new customers. But in today's connected home, advanced broadband services combine with a multitude of Internet-ready devices to create a challenging environment for both cable operators and consumers to manage. MSOs may have little or no visibility into what devices are connected in the home network, what services consumers are using, and how these services and the home network are performing. This can result in increased support costs for operators and quality of experience issues for consumers.

DOCSIS® protocols support basic management of the primary cable device in the home, be it a set-top box or a gateway. One key element of TR-069 is providing operators with far more control and visibility over PCs, mobile devices, connected TVs and other CPE. TR-069 provides the management layer that will be needed as MSOs move into the home automation sector; it can simplify and extend customer self-fulfillment; and it can help enable MSO Wi-Fi initiatives by providing management capabilities both within the home and beyond.

The TR-135 specification for IP video STBs is a logical path to take to manage next generation video devices. As part of the specification family, additional management platforms should not be required. Recognizing that home and public Wi-Fi are effectively the same is essential to success, with primary differences being in activation and diagnostic processes.

Customer experience solutions focus on managing, optimizing, and supporting the multi-user, multi-device, multi-service home environment - starting with service activation all the way through troubleshooting and problem resolution, and on-going maintenance. The main elements include:

- Service activation
- Home and mobile device management and support

- Home network management and support, including Wi-Fi
- High speed data services support

Customer experience solutions enable MSOs to pro-actively monitor consumers' devices, services and home networks, and address any problems before they impact the end-user's service experience. They also make it easier for MSOs to manage the rapidly-growing number of smartphones, tablets, home gateways, set-top boxes and other devices connecting to subscribers' home networks, and to the MSO network. Good customer experience solutions integrate next generation device management and customer care systems into a single managed experience that allows MSOs to manage the connected home:

- Providing MSOs with the ability to activate, manage and support new devices in the home.
- Offering greater visibility and control of the home network, connected devices and home services by enabling consumers and help desk agents to quickly, easily and accurately diagnose and troubleshoot home network issues and enhance home network performance.
- Enhancing customer satisfaction, reduces call center expenses, and helping MSOs deliver a differentiated, high-quality service and support experience to subscribers.

MANAGING THE CUSTOMER EXPERIENCE FOR WI-FI

Specific Customer Experience Issues for Carrier Wi-Fi

For new Wi-Fi services, subscribers demand a simple seamless and secure experience. Cable operators, meanwhile, will require that these deployments be both efficient and cost effective. To achieve these goals, there are two primary areas that require addressing once a Wi-Fi network is available for subscribers to use: activation and customer care.

Activation

Wi-Fi activation involves both the Wi-Fi service and the devices, along with several backend processes, but must still be a simple experience for the subscriber. Activation, as the first step in gaining access to Wi-Fi services, has three facets for Carrier Wi-Fi. These are subscriber sign up and registration to activate the service for the user, device activation and configuration so a device can use the Wi-Fi service, and from the network equipment viewpoint, the access point or CPE activation and configuration to provide the Wi-Fi service for subscribers to access.

Self-Activation

Subscribers should have the ability to enable and activate carrier Wi-Fi services without having to contact their service provider. They should be able to do this from the device

they want to use it with, and from an application or portal on a home device, such as their home PC. This device independent interaction is known as multi-channel activation.

The online sign-up service, through a portal or client application, provides end users with a simple mechanism to start using Wi-Fi. Application and portal flows can be slightly different due to the pre-existence of customer data. The client application can be knowledgeable of the subscribers' service profiles, home network, devices, and home Wi-Fi parameters. From this starting point, users can quickly and easily add a mobile device and provide a mechanism to have the carrier Wi-Fi profile delivered to the mobile device. The portal based service requires that the subscriber have mobile or another Wi-Fi connection active.

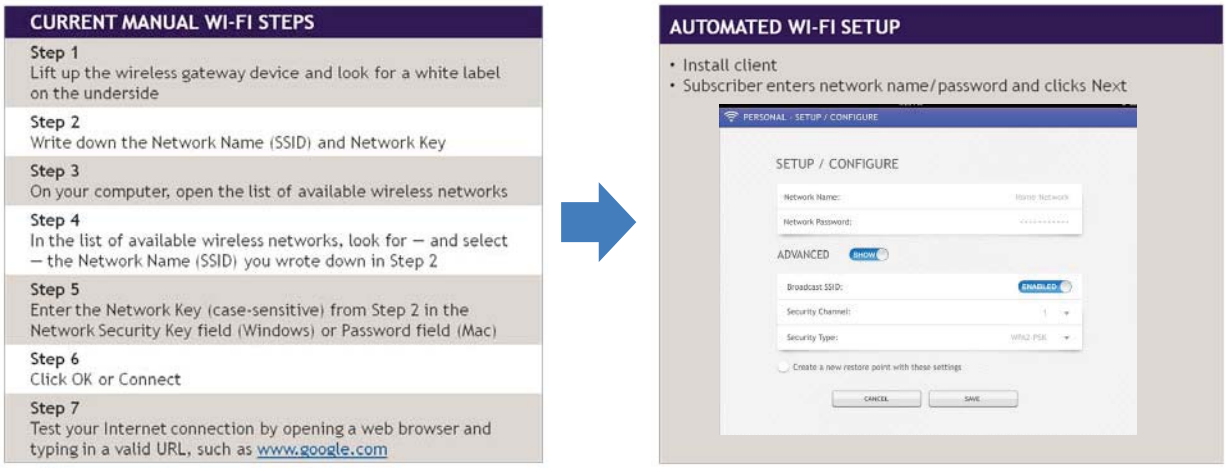

Figure 10 Simplified, Automated Wi-Fi Setup

Subscriber and Service Activation

Portal based activation is likely to be the most commonly used method. It is the initial focus of the solution and includes:

- Existing customer login using existing account credentials and service activation
- Set opt in / out status on subscriber profile
- Initiate device activation and configuration for UE
- Initiate device activation and configuration for CPE, if needed
- New customer sign up and account creation
- AAA verification of the subscriber
- Identification of the device type and o/s
- Creation of new subscriber profile in BSS/OSS for new customer sign up
- Subscriber service registration and profile updating to BSS/OSS systems

- HotSpot 2.0 enrollment service
- Time or usage based conditions accepted during the signup process are passed to the policy server and AAA as required

The portal should be independent of existing self-service portals, but the functionality must also be accessible from other existing portals, such as a self-service account management portal.

User Device Activation and Configuration

The second stage of the activation process is to create a Wi-Fi profile for the target device and deliver it to the device. This profile must contain any required security methods and parameters for secure Wi-Fi connectivity. These include EAP methods and the appropriate parameters.

This stage of the activation includes

- Registering the device with the customer profile in B/OSS systems
- Ensuring AAA sources have the device MAC address and other required identifying parameters
- Generating a carrier Wi-Fi access profile for the device o/s, in compliance with security requirements
- Delivering the profile to the device and confirming the delivery
- Delivering ANDSF policy to the ANDSF client, if required
- Turning on the Wi-Fi radio, if required by policy or the user

Activation Scenarios

1. A customer should be able to, from their mobile device using a mobile or Wi-Fi connection, whether or not they are in a carrier Wi-Fi zone, go to a sign up portal to register for the service. The service should activate and the device should be configured for use on that carrier Wi-Fi network. [Service activation, Device activation]
2. If the customer gets connected to an open carrier Wi-Fi zone for the first time, either manually or automatically by the device, they should be redirected to a captive portal to sign up or register for the service and be activated. [Service activation, Device activation]]
3. A customer should be able to activate a Wi-Fi only device while in their home for use on their home network and the carrier Wi-Fi network with a minimum of effort
4. A customer should be able to activate for carrier Wi-Fi a separate device from the one being used to perform the activation. E.g. use a lap top to activate a mobile device.

CPE AND ACCESS POINT CONFIGURATION

Activation and configuration of access points can be performed for both CPE (residential gateways) and outdoor APs. CPE and outdoor APs with TR-069 management stacks can be managed with a TR-069 Auto Configuration Server (ACS). TR-069 management enables the AP to be diagnosed and to provide information in end-to-end troubleshooting for customer care and network operations.

Existing zero touch activation workflows can be adapted to incorporate the carrier Wi-Fi needs of:

- Activate CPE/AP in device management system
- Register the CPE with the customer profile in B/OSS systems
- Configure carrier Wi-Fi settings, including EAP parameters
- Configure AP connection policies on device

CUSTOMER CARE

Customer care for carrier Wi-Fi is targeted to addressing and resolving issues relating to management and services. Activation issues are characterized as administration and management relating to the customer account and device and service configuration. Some of these issues may be considered a sub category of connectivity issues from an end-user perspective. Service issues can generally be divided into two main categories of Cannot Connect, and Slow Connectivity.

Management related functions:

- Reset the CPE/AP
- Update CPE/AP firmware
- Validate CPE/AP configuration
- Ensure opt in/out policy setting is applied to device configurations
- Verify policy from PCRF and history
- Verify device MAC address with AAA
- Get data usage and limit per period

Cannot Connect functions:

- Verify Wi-Fi profile on UE
- Verify Wi-Fi radio setting on UE
- Verify UE connection status on WLAN GW
- Verify subscriber service profile for access to Wi-Fi services
- Verify AP backhaul/WAN status
- Verify current data network for UE

- Verify PCRF subscriber policy and transaction history
- Verify AP connection to WLAN GW
- Get IP Network diagnostic/status from NMS
- Verify AP is part of carrier Wi-Fi network
- Verify EAP method parameters on device

Slow Connection functions:

- Diagnose AAA transaction history
- Check number of concurrent connections on AP
- Check radio parameters on AP for UE
- Check UE Wi-Fi signal strength
- Check UE resource usage
- Check available APs in UE location via PCRF
- Change AP Wi-Fi channel
- Get AP Wi-Fi radio connection parameters for connection
- Change policy for UE

CONCLUSIONS

Customer Experience Management is about improving the end user experience with the products and services they purchase. For services such as Internet access or public Wi-Fi, the rapid change of consumer technologies creates complications, but also provides opportunities for improvement, and for cable operators to differentiate themselves from the competition. Device management is a critical enabler to delivering a high-quality, ongoing experience. The capabilities detailed here have shown how standardized protocols can be used for this purpose.

Service management and orchestration platforms are used to transform device management capabilities into effective processes to solve customer issues. These are exposed in end-user applications and customer care solutions. Addressing the key Wi-Fi issues of connectivity and performance requires a combination of CPE and end point device management with workflow processes, which cross technical and business boundaries, to identify diagnose and resolve customer issues.

Bibliography

[1] Chetan Sharma Consulting – US Wireless Market Update, 2012
[2] BBF TR-069 CPE WAN Management Protocol Issue: 1 Amendment 4, July 2011
[3] BBF MR-239 Broadband Forum Value Proposition for Connected Home Issue: 1, April 2011
[4] BBF TR-181 Device Data Model for TR-069: Issue 2 Amendment 6, November 2012
[5] BBF TR-232 Bulk Data Collection Issue: 1, May 2012
[6] OMA Device Management, Version 1.x, Open Mobile Alliance™, URL:http://www.openmobilealliance.org
[7] Standardized Connectivity Management Objects, Version 1.0, Open Mobile Alliance™, URL:http://www.openmobilealliance.org
[8] OMA Diagnostics and Monitoring, Version 1.2, Open Mobile Alliance™, URL:http://www.openmobilealliance.org
[9] OMA Device Capability Management Object, Version 1.0, Open Mobile Alliance™, URL:http://www.openmobilealliance.org

Abbreviations and Acronyms

ACS	Auto-Configuration Server
ANSDF	Access Network Discovery and Selection Function
AP	Access Point
BBF	Broadband Forum
BSS	Business Support System
CPE	Customer Premises Equipment
CWMP	CPE WAN Management Protocol
DDF	Device Description Framework
DM	Device Management
DOCSIS®	A CableLabs interface specification that enables high-speed Internet services over HFC. The DOCSIS® brand for these specifications and devices built to them developed from the specifications' original name, "Data Over Cable Service Interface Specifications."
EAP	Extensible Authentication Protocol
EAP-TTLS	Extensible Authentication Protocol – Tunneled Transport Layer Security
GW	Gateway
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPDR	Internet Protocol Detail Record
IrDA	Infrared Data Association
IVR	Interactive Voice Response
MO	Management Object
OMA	Open Mobile Alliance
OSS	Operation Support System
OTA	Over The Air
PAN	Personal Area Network
SIP	Session Initiation Protocol
SMS	Short Message Service
SSID	Service Set Identifier
UDP	User Datagram Protocol
UE	User Equipment
UI	User Interaction or User Interface
WAP	Wireless Application Protocol
WAN	Wide Area Network
WFA	Wi-Fi Alliance
WSP	Wireless Session Protocol

Contributors

Tim Carey
Industry Standards Manager
Alcatel-Lucent
Plano, TX, USA
timothy.carey@alcatel-lucent.com

Jay Fausch
Marketing Manager
Alcatel-Lucent
Raleigh, NC, USA
jay.fausch@alcatel-lucent.com

Pierre-Henri Gross
Industry Standards Manager
Villarceaux, France
pierre.gross@alcatel-lucent.com

Ellis Lindsay
GM, Customer Experience Solutions
Alcatel-Lucent
Ottawa, Canada
ellis.lindsay@alcatel-lucent.com

Alan Marks
Sr. Marketing Manager
Alcatel-Lucent
Raleigh, NC, USA
alan.marks@alcatel-lucent.com