CableLabs® Custom Connectivity

An Architecture To Bridge The Digital Divide

A Technical Paper prepared for SCTE by

Darshak Thakore
Principal Architect
CableLabs
858 Coal Creek Circle, Louisville, CO 80023
+1-303-661-3456
d.thakore@cablelabs.com

Craig Pratt
Lead Software Architect, Security & Privacy Technologies
CableLabs
858 Coal Creek Circle, Louisville, CO 80027
+1 303.661.3408
c.pratt@cablelabs.com

Mohan Gundu
SVP, Engineering
Veea Inc.
164 E 83rd Street
New York, NY 10028
+1 212 535 6050
mohan.gundu@veea.com

Roger Lucas
SVP, Systems Engineering
Veea Inc.
Veea Systems Ltd., Cambridge House, Henry Street, Bath, BA1 1JS, England
+44 7776 234297
roger.lucas@veeasystems.com

Jose Quintero
Senior Director, Innovation Labs
Liberty Latin America
Boulevard Costa del Este, Panama City, Panama
+507 208-5197
jose.quintero@lla.com

Table of Contents

Title **Page Number**

1 Introduction 3
2 Background 3
3 The Digital Divide 4
4 CableLabs® Custom Connectivity Architecture 4
4.1 Architectural overview 4
4.2 The Custom Connectivity Controller 6
4.3 The Custom Connectivity Portal 6
4.4 The Custom Connectivity Gateway Agent 6
4.5 The Custom Connectivity Administrative Interface 7
4.6 The Custom Connectivity APIs 9
5 Panama Trial 10
5.1 Service Requirements 10
5.2 User Experience Considerations 11
6 Implementation Details 12
6.1 Network segmentation on shared Access Points 12
6.2 Per-device credential management 13
6.3 Roaming within the Multi-AP mesh 14
6.4 Enforcement of Service policies 14
7 Conclusion 15
8 Abbreviations 15
9 Bibliography & References 16

List of Figures

Title **Page Number**

Figure 1: Custom Connectivity high-level architecture 5
Figure 2: Custom Connectivity AP Components 7
Figure 3: Custom Connectivity Reference UI - Overview Page 8
Figure 4: Custom Connectivity Reference UI - Service Detail Page 9
Figure 5: Custom Connectivity Component Interoperation 9
Figure 6: Custom Connectivity User Experience 12
Figure 7: Adding a device using a Custom Connectivity-enabled mobile app 13
Figure 8: Inter-AP VXLAN, Extender and Access Network Interconnects 14

1 Introduction

In today's world, reliable internet connectivity is a necessity. The COVID-19 pandemic has accentuated the need to stay connected while also highlighting the digital divide that exists across the globe. When we talk about the "digital divide", we typically think about serving remote and rural areas. But a lesser-recognized digital divide exists in dense urban areas. Socio-economic factors in developing countries have provided broadband internet access to upper income, educated communities while economically disadvantaged neighborhoods are left unserved or, at best, underserved.

These unserved and underserved areas pose multiple challenges for providing affordable service using traditional deployment models where end-user service is provided as a post-paid recurring subscription via a Consumer Premise Equipment (CPE) installed to a household with a billable home address. These models focus on postpaid subscription for the address where, over time, the ROI model recoups the cost of installation, the CPE, and recurring costs to bring connectivity to the household.
Overcoming the challenges of installation cost, installation logistics, device / CPE security while unleashing the purchasing power of the unbanked in these economically disadvantaged neighborhoods is key to bridging the digital divide and allows for deployment models across high-density, shared residential and MDU communities.
In this paper we present a novel approach based on the CableLabs® Custom Connectivity (CC) architecture to delivering internet service, directly to a device and/or to a group of devices without the need for an in-home deployed CPE or requiring a fixed household address for broadband service delivery. This Custom Connectivity architecture, implemented in collaboration with Liberty Latin America and Veea Inc, enables alternate deployment models utilizing edge compute based shared Wi-Fi access points that provide on-demand virtualized home gateways to subscribers. The rest of the paper is organized as follows
Section 2 (Background) talks about traditional CPE based deployment architecture and some of the shortcomings of that model.
Section 3 (The Digital Divide) dives into the unique constraints in some of the unserved and underserved communities that hinders broadband services delivery using the traditional CPE based model.
Section 4 (Custom Connectivity Architecture) provides an overview of the Custom Connectivity architecture and some of the unique capabilities provided by that architecture.
Section 5 (Panama Trial) describes the technical and business requirements that shaped the trial implementation of the Custom Connectivity architecture to provide broadband services to the underserved and unserved communities.
Section 6 (Implementation) explains the functional components that collectively allows delivery of broadband services directly to subscriber's devices through an on-demand subscriber specific virtual home gateway service that is hosted using the shared-CPE design.

2 Background

Traditionally broadband services are delivered to a physical home address with a consumer premise equipment (CPE) like a cable modem or an ONU terminating the access network. The subscriber's billing relationship is also tied to the address where the CPE is installed. This model has served well over the past few decades where the focus was on delivering cable video as well as broadband services to a household with a limited number of consumer devices connecting to the network. Over time the number of consumer devices connecting to the network have been increasing and continues to increase exponentially. Consumers are also connecting an increasingly wider variety of devices to the network and these devices may have specific connectivity requirements. For example, security cameras require increased upstream bandwidth compared to a Smart TV and/or a work computer. These trends have highlighted several constraints with the existing deployment model:

- The need for a CPE to be installed and activated for each subscription adds to the cost of servicing a subscriber. This cost goes beyond just the cost of the CPE and includes the costs associated with inventory management, installation logistics, CPE security and maintenance etc.
- Operators typically do not have visibility into the devices behind the CPE that are connecting to the network. This makes it difficult to troubleshoot problems caused by individual devices and makes it harder to deliver custom service(s) to a device or group of devices.
- The billing for the subscription is typically tied to the home address where the CPE is installed instead of the devices to which the services are being delivered to. This prevents the operators from offering device-centric value-added services that can optionally be tied to different payers.
- It prevents sharing of CPE across subscribers which, as described below is one of the factors that contributes towards the difficulty in offering broadband services in certain unserved and underserved communities.

3 The Digital Divide

The global COVID-19 pandemic brought into focus the importance of reliable internet connectivity in our lives and the devastating consequences to people and communities that did not have access to reliable internet connectivity. While a majority of the population in developed countries were able to sustain themselves and their families by depending on reliable broadband services, there was a significant population in low-income communities in Latin America and other developing countries across the globe that were either unserved or underserved in terms of broadband connectivity. The impact to these communities was substantial. Children were unable to access educational content and adults were largely unable to participate in today's digital economy. A lot of these communities were composed of daily wage earners and the gig-economy participants that primarily lived in high-density neighborhoods. These neighborhoods had remained largely unserved or underserved because the traditional CPE based service delivery model did not scale economically in these neighborhoods. A number of factors contributed to it being non-viable for the operators. First and foremost, the costs associated with the CPE (see Section 2) resulted in a negative ROI in most cases due to the low-ARPU in these communities. A significant population in these communities were unbanked which made it difficult to establish a BSS relationship with the subscribers. In certain instances, there wasn't a fixed home address to deliver the service to. The subscribers preferred a subscription model that was more on-demand, where they could stop/disable their service on certain days and not have to pay for it. Such on-the-fly service activation/deactivation is hard if not impossible to support with the existing home-address based billing model. These factors contributed to creating a digital divide for these communities and put them at a significant disadvantage during the pandemic.

4 CableLabs® Custom Connectivity Architecture

4.1 Architectural overview

The Custom Connectivity architecture encompasses a set of technologies that collectively enable the delivery of broadband services using an alternate device-centric service delivery model. In particular, Custom Connectivity provides per-device credentials and per-device policy for consumer-grade wireless devices – essentially providing enterprise-grade device access and management capabilities to non-enterprise devices.

The core of the Custom Connectivity system is the Custom Connectivity Controller (CC Controller) – which coordinates wireless access points to provide access for the provisioned network services and associated devices. The Controller interfaces with the operator OSS/BSS systems and customers via the Custom Connectivity Portal (CC Portal) – which is adapted to the operator's infrastructure. Service and device configuration and monitoring, as well as AP provisioning and deployment, can be performed using the Custom Connectivity Controller API – either via a stand-alone operations interface or integrated with existing network operations interfaces and tools. Similarly, the Custom Connectivity telemetry interface can be used to monitor the health of the network(s) and, along with the network operations interface, provide customer support.

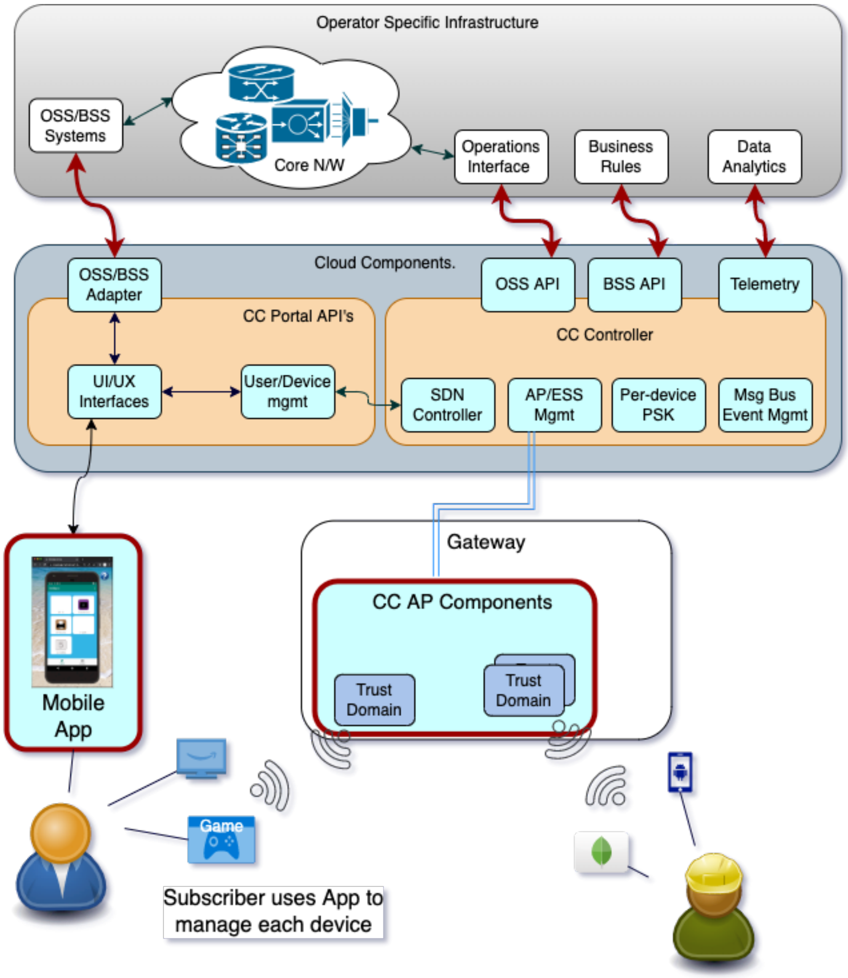


Figure 1: Custom Connectivity high-level architecture

4.2 The Custom Connectivity Controller

The Custom Connectivity Controller contains the information regarding … and operational state information for the Custom Connectivity network and has the responsibility of keeping all parties in a Custom Connectivity network synchronized so that all elements are operating with a common network/device model. In particular, the Controller provides:

- REST API's to manipulate the Custom Connectivity Service model
- The Custom Connectivity PSK Engine – for identifying valid PSKs and determining device associations
- A reference operator interface for provisioning Custom Connectivity-enabled Wi-Fi access points
- An MQTT Broker to communicate model changes to provisioned access points
- REST API's to for access points to communicate Wi-Fi telemetry and device connectivity status

4.3 The Custom Connectivity Portal

The Custom Connectivity Portal is the communication bridge between the Controller, operator OSS/BSS infrastructure, and mobile application communication. The Portal is intended to be highly adaptable to the operator network and infrastructure. The Portal is responsible for:

- Interfacing with the provider's customer-facing systems/applications – which can be used by the customer to setup their Custom Connectivity Service, determine funding, establish per-device access rules, onboard Wi-Fi devices, confirm device additions, and manage their services/devices.
- Communicating with the Custom Connectivity Controller to manipulate the service/device objects on behalf of the customer.
- Communicating customer-initiated service/device changes with OSS/BSS infrastructure.
- Associating Custom Connectivity Services with customer subscription plans and maintaining service according to the subscribed plan and payment status – including handling expiration times/dates.
- Process notifications from the Controller regarding service/device object status changes (e.g. when a device connects/disconnects) and communicating the changes to the customer and OSS/BSS infrastructure.

4.4 The Custom Connectivity Gateway Agent

Every wireless access point that supports Custom Connectivity must include a Gateway Agent provisioned with credentials to connect and communicate with the Custom Connectivity Controller. The Gateway Agent is responsible for:

- Establishing and maintaining a connection with the Controller using credentials provisioned by the vendor and/or operator
- Performing initial setup of the AP by interrogating the Controller and setting up Wi-Fi credentials, VLANs, bridges, and inter-AP VXLAN connections to support the Custom Connectivity services and devices provisioned for the AP the agent is running on
- Handling DHCP requests for Custom Connectivity devices and providing IP addresses according to the Custom Connectivity service model provided by the Controller
- Delegating Wi-Fi 4-way handshake authentication requests for devices which are being onboarded to the Custom Connectivity Controller – which in-turn performs the necessary decryption steps to determine if/which device is associated with the presented password

- Handling MQTT messages from the Controller to update the access point to reflect changes to Custom Connectivity services/devices associated with the access point
- Setting up and maintaining inter-AP VXLAN tunnels – to support the CC inter-AP mesh
- Providing per-device telemetry to the Controller
- Routing Internet inbound/outbound traffic to the access network
- Routing intra-Service device-to-device traffic across inter-AP tunnels when devices within the same Service are connected to different APs (mesh routing)

The Custom Connectivity Reference Implementation includes a reference gateway implementation with the components outlined in Figure 2: Custom Connectivity AP Component

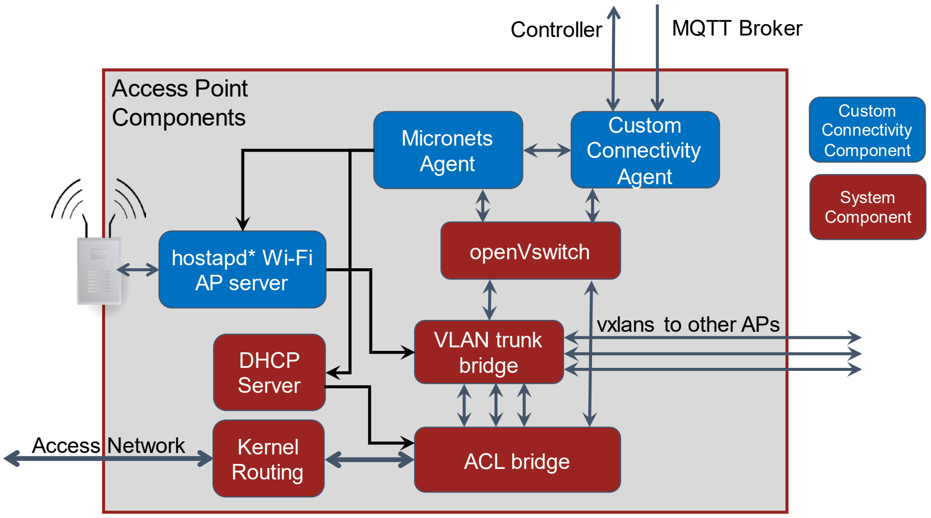


Figure 2: Custom Connectivity AP Components

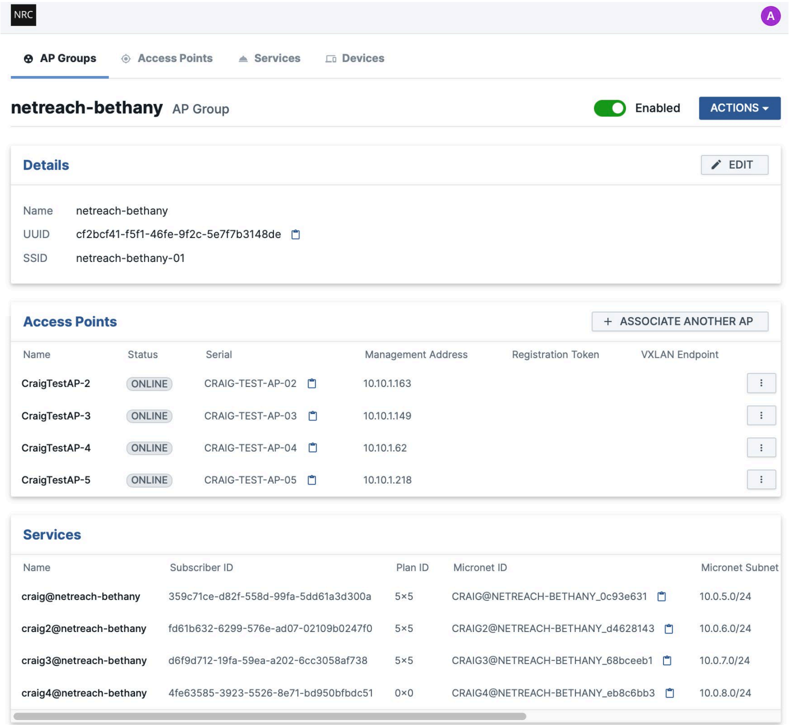
4.5 The Custom Connectivity Administrative Interface

For monitoring and managing a Custom Connectivity system by network operators and customer support the Custom Connectivity Controller provides a REST Operations API and notification support for enabling web- and/or smart device-based management interfaces. This Operations API can enable existing operation center user interfaces to incorporate Custom Connectivity administrative/support functions and/or enable the implementation of stand-alone management interfaces.

The Custom Connectivity Reference Implementation includes a reference web interface which allows for:

- The enumeration of Custom Connectivity services, devices, AP groups, and APs and their various association
- The provisioning of APs using public keys and registration tokens
- The monitoring of devices with live updates on connected devices and associated APs
- The creation of APs and AP groups, as well as associating/disassociation of APs with AP groups

Some illustrations of the Custom Connectivity management reference web interface can be found in Figure 3 and Figure 4.



netreach-bethany AP Group

Details

Name	netreach-bethany
UUID	cf2bcf41-f5f1-46fe-9f2c-5e7f7b3148de
SSID	netreach-bethany-01

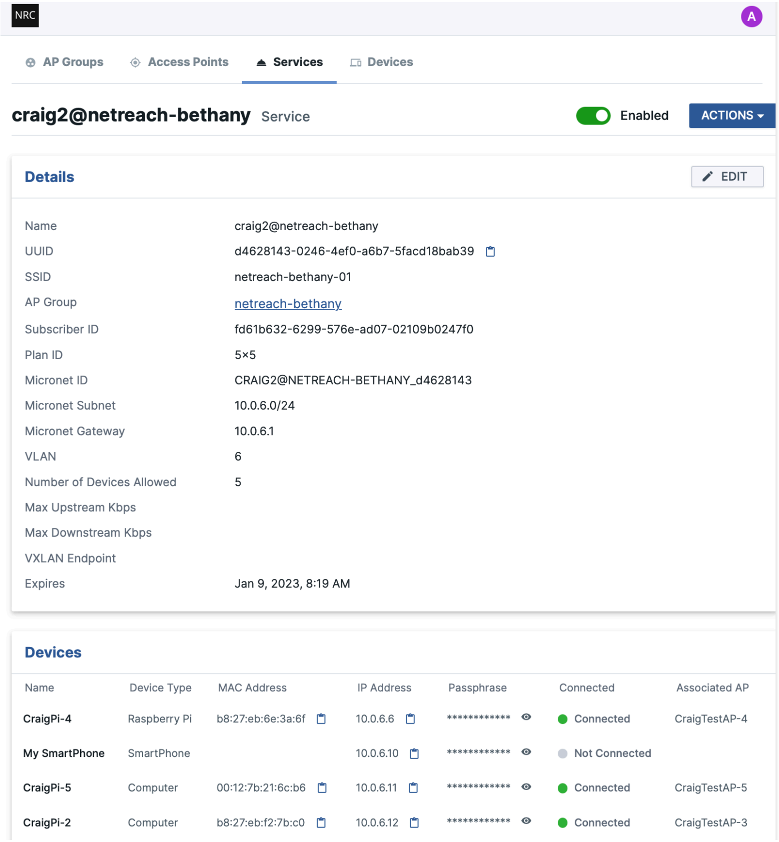
Access Points

Name	Status	Serial	Management Address	Registration Token	VXLAN Endpoint
CraigTestAP-2	ONLINE	CRAIG-TEST-AP-02	10.10.1.163		
CraigTestAP-3	ONLINE	CRAIG-TEST-AP-03	10.10.1.149		
CraigTestAP-4	ONLINE	CRAIG-TEST-AP-04	10.10.1.62		
CraigTestAP-5	ONLINE	CRAIG-TEST-AP-05	10.10.1.218		

Services

Name	Subscriber ID	Plan ID	Micronet ID	Micronet Subnet
craig@netreach-bethany	359c71ce-d82f-558d-99fa-5dd61a3d300a	5×5	CRAIG@NETREACH-BETHANY_0c93e631	10.0.5.0/24
craig2@netreach-bethany	fd61b632-6299-576e-ad07-02109b0247f0	5×5	CRAIG2@NETREACH-BETHANY_d4628143	10.0.6.0/24
craig3@netreach-bethany	d6f9d712-19fa-59ea-a202-6cc3058af738	5×5	CRAIG3@NETREACH-BETHANY_68bceeb1	10.0.7.0/24
craig4@netreach-bethany	4fe63585-3923-5526-8e71-bd950bfbdc51	0×0	CRAIG4@NETREACH-BETHANY_eb8c6bb3	10.0.8.0/24

Figure 3: Custom Connectivity Reference UI - Overview Page



craig2@netreach-bethany Service

Details

Name	craig2@netreach-bethany
UUID	d4628143-0246-4ef0-a6b7-5facd18bab39
SSID	netreach-bethany-01
AP Group	netreach-bethany
Subscriber ID	fd61b632-6299-576e-ad07-02109b0247f0
Plan ID	5×5
Micronet ID	CRAIG2@NETREACH-BETHANY_d4628143
Micronet Subnet	10.0.6.0/24
Micronet Gateway	10.0.6.1
VLAN	6
Number of Devices Allowed	5
Max Upstream Kbps	
Max Downstream Kbps	
VXLAN Endpoint	
Expires	Jan 9, 2023, 8:19 AM

Devices

Name	Device Type	MAC Address	IP Address	Passphrase	Connected	Associated AP
CraigPi-4	Raspberry Pi	b8:27:eb:6e:3a:6f	10.0.6.6	************	● Connected	CraigTestAP-4
My SmartPhone	SmartPhone		10.0.6.10	************	○ Not Connected	
CraigPi-5	Computer	00:12:7b:21:6c:b6	10.0.6.11	************	● Connected	CraigTestAP-5
CraigPi-2	Computer	b8:27:eb:f2:7b:c0	10.0.6.12	************	● Connected	CraigTestAP-3

Figure 4: Custom Connectivity Reference UI - Service Detail Page

4.6 The Custom Connectivity APIs

The Custom Connectivity APIs are used to manage a common Custom Connectivity entity model. The ability to modify different elements of the model is grouped into four functional areas that have group-level access controls.

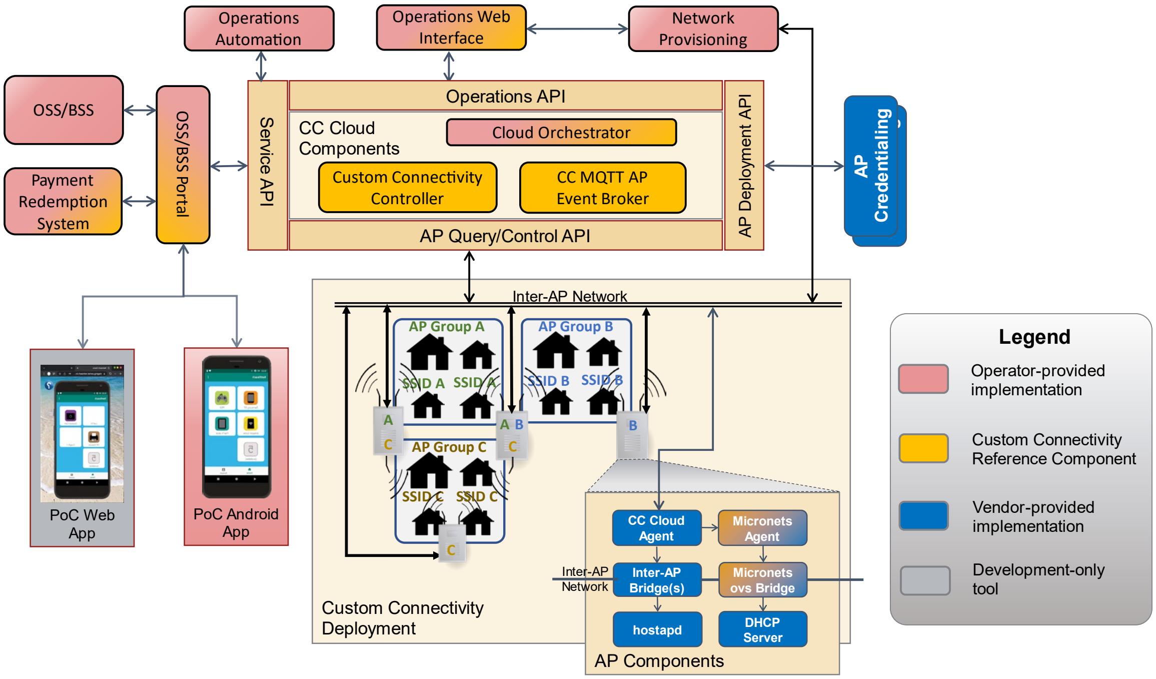


Figure 5: Custom Connectivity Component Interoperation

The Custom Connectivity Controller APIs help ensure interoperability between vendors components, operator components, and the Controller. The intent of the Custom Connectivity architecture – and having well-defined APIs - is to enable either the operator or a service provider to host and manage the Controller on behalf of the operator. This can enable different degrees of regional colocation based on desired cost, reliability, and scaling factors.

The Custom Connectivity APIs are divided into the following functional groups:

- Service API: While the Custom Connectivity Portal primarily communicates via interfaces which are OSS/BSS-specific, Portal implementations expose a single REST endpoint that the Custom Connectivity Controller uses to notify the Portal of changes to Custom Connectivity Services and associated Devices. The Portal in-turn uses the Controller APIs to enact changes and enable/disable services and associated devices based on customer subscription/payment changes, service expirations, and/or customer preference.
- AP Deployment API: Supports the creation of authentication credentials for APs and putting APs into/out of service. This interface enables credential provisioning in a variety of ways – either at time of AP manufacture/configuration or at initial power-on the AP using provisioning tokens.

APs can also be put into/out of service in a controlled fashion to facilitate replacement, relocation, debugging, and/or network upgrades.

- AP Query/Control API: Custom Connectivity-enabled APs are informed of changes in the Custom Connectivity data model via MQTT and update their internal state by performing queries to the Controller regarding affected model elements. APs also use these APIs to update the state of Device elements based on physical device state (e.g. “authenticated” or “connected”) and connection quality (e.g. the station’s RSSI and error rate).
- Operations API: These APIs enable operators to administrate and automate the Custom Connectivity system. Network operators and automated tools can monitor the state of the APs, Services, and Devices to help identify potential issues in concert with network backhaul monitoring. APs can be organized/reorganized into different AP groups to optimize the access and backhaul network and ensure sufficient wireless coverage. This API also enables customer service to diagnose device and network connectivity issues and take corrective actions.

5 Panama Trial

5.1 Service Requirements

The Custom Connectivity Architecture described in Section 4 provides an alternate service delivery model that is based on a shared-CPE paradigm and rather than linking a subscribers’ broadband services to the CPE, it focuses on providing those services directly to the devices. This paradigm made the architecture suitable for bridging the digital divide and providing broadband services to the unserved and underserved communities (see Section 3). Our goal was to validate the architecture by running a limited trial in a representative unserved community. Consequently, a small neighborhood in Panama was selected for the trial where the houses were grouped along a street with utility poles along the street. The service would be delivered through external AP’s mounted to the utility poles and the subscriber’s devices would connect directly to these AP’s. The following technical and operational requirements were addressed for the trial.

- Service to each subscriber was to be provided directly over Wi-Fi without the need to run any wiring to the subscriber’s home
- The subscriber should be able to connect their devices anywhere within the service area and not have to select any specific AP to connect to (seamless to them)
- The subscriber’s connectivity experience should resemble a traditional home Wi-Fi experience where they can connect any device including Smart TV’s, printers, casting devices, tablets, Chromebooks etc. and be able to discover and communicate amongst them.
- The subscriber should be able to connect any standard Wi-Fi enabled device without having to perform any special procedure on those devices (i.e no captive portal interactions, no mac address registration, no custom software). The only interaction required on the device to be connected is to select the service set identifier (SSID) and enter the Wi-Fi passphrase.
- The service provider has the capability to apply rate limits (packet data rates) by subscriber independently, with option to provide different service tiers per subscriber.
- Capability to add extenders (future capability) for improved indoor coverage (with Wi-Fi as a backhaul from the extender)
- Be able to use any backhaul technology including standard FTTH/xPON from the AP’s/shared-CPE’s.

5.2 User Experience Considerations

In addition to the technical and operational requirements described above, another goal for the trial was to ensure that the entire service experience, from service activation to service and device management to billing and payment – was to be kept simple and familiar to the subscriber. In this neighborhood, most subscribers were accustomed to activating and managing their pre-paid cellular plans using pre-paid vouchers that they purchased from the local stores. The following requirements were taken into account while developing the overall user experience

- Since the subscribers were accustomed to using pre-paid vouchers, we leveraged the existing voucher-based BSS system and integrated it with the BSS interfaces on the Custom Connectivity Portal. This allowed the users to use the same pre-paid vouchers to either renew their cellular plans or activate their Wi-Fi based home broadband service plan.
- The only requirement imposed on the user was for them to install and/or use a mobile app that allowed them to self-manage their services - creation of a new account, redeeming vouchers, service activation, adding/managing devices and their credentials etc.
- The subscriber should be able to self-manage their subscription, i.e be able to choose how long they would like their service enabled and be able to suspend their service if they did not need it on a given day.
- The subscriber should be able to renew their subscription as and when needed.

The sequence diagram in Figure 6 shows the overall user experience that was developed and provided in the trial.

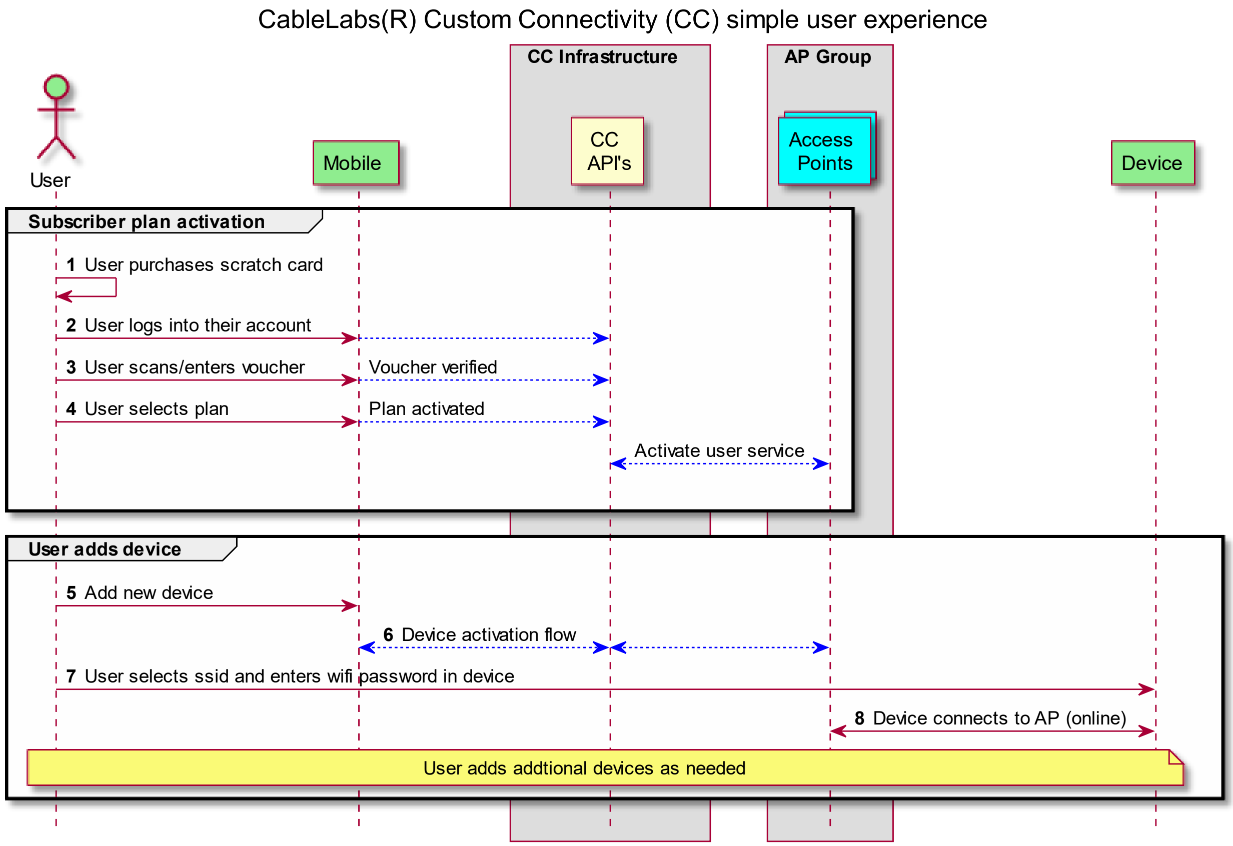

CableLabs(R) Custom Connectivity (CC) simple user experience
CC Infrastructure
AP Group
User
Mobile
CC API's
Access Points
Device
Subscriber plan activation
1 User purchases scratch card
2 User logs into their account
3 User scans/enters voucher
Voucher verified
4 User selects plan
Plan activated
Activate user service
User adds device
5 Add new device
6 Device activation flow
7 User selects ssid and enters wifi password in device
8 Device connects to AP (online)
User adds addtional devices as needed

Figure 6: Custom Connectivity User Experience

6 Implementation Details

CableLabs® Custom Connectivity offers to deploy Internet access without a drop, a CPE, or an in-home wireless access point. And unlike hotspot or captive portal solutions, Custom Connectivity offers to also provide a complete home network that works with all Wi-Fi devices - including smart TVs, IoT, and home assistant devices. In short Custom Connectivity offers a full CPE+AP experience without a CPE.

We attempt to provide some details below on exactly how Custom Connectivity provides this functionality – and how it can be done in an interoperable multi-vendor way.

6.1 Network segmentation on shared Access Points

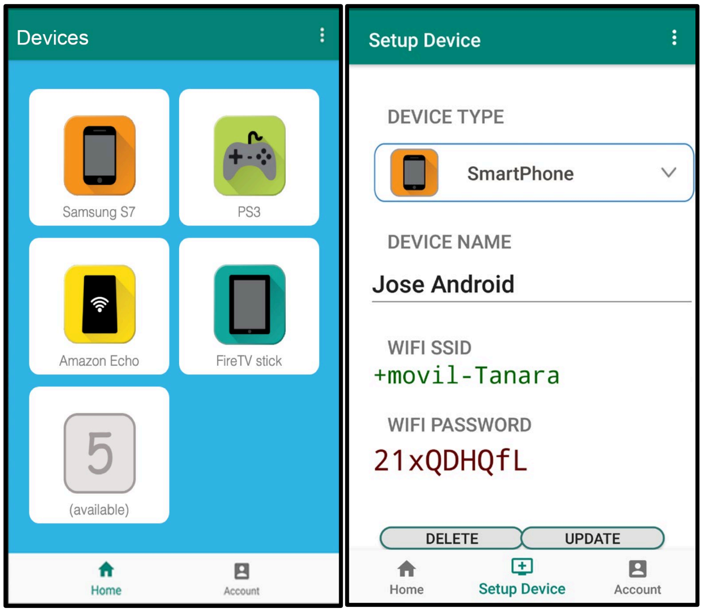
The logical segmentation of physical ethernet networks using VLANs has been a reality for decades. When Wi-Fi technology (see [2][3]) was adapted for enterprise use, capabilities were added to enable devices to be authenticated via the use of a user-associated identity/credential. Devices could all join the same SSID with each device being optionally designated for a particular VLAN. While these enterprise features require special Wi-Fi device support (that most home devices don't have) and a complicated AAA server to create/authenticate credentials, this fundamental capability for per-device credentials and VLAN association was and is present in the core Wi-Fi technology today. (see [1])

Using its unique device onboarding system, Custom Connectivity leverages the core capability present in Wi-Fi to associate non-enterprise Wi-Fi devices with an identity, encryption key, and VLAN all on a shared SSID. This means that devices cannot discover, communicate, or observe each other’s traffic without explicit policy enabling them to do so. Custom Connectivity utilizes this separation capability to group devices by household (and optionally subzones within a household) into discreet segments – each associated with a VLAN – providing the same separation for a household as one would get with a discreet in-home Wi-Fi AP and switch.

6.2 Per-device credential management

As part of the onboarding process, the Custom Connectivity system provides each device a unique passphrase which is used to provide the device access and, additionally, as a means to robustly identify the device. The process for the user is straight-forward:

1. Using a mobile app (logged into the account provided by the operator), the user selects an option to add a new device to their service (see Figure 7),
2. The user enters a couple details about the device (e.g. a name and device type,
3. The app provides an SSID and passphrase for the new device,
4. The user enters the SSID and passphrase into the device,
5. When the new device attempts to authenticate with the AP, the AP – in conjunction with the Custom Connectivity Controller – performs the necessary cryptographic logic to determine which passphrase was provided by the device,
6. The device completes authentication, and the AP associates the Wi-Fi session with the device – setting up necessary interconnects for the device and signaling the Controller,
7. The controller signals all other APs of the new device to enable interconnects and roaming.



DEVICE TYPE
SmartPhone

DEVICE NAME
Jose Android

WIFI SSID
+movil-Tanara

WIFI PASSWORD
21xQDHQfL

Figure 7: Adding a device using a Custom Connectivity-enabled mobile app

The details of how robust association of devices with unique credentials can be achieved is discussed in a previous SCTE paper, *Wi-Fi Passwords: The Evolving Battle Between Usability and Security* [1].

6.3 Roaming within the Multi-AP mesh

A single AP can only cover a limited area, so Custom Connectivity enables a large number of APs to be grouped together to form an AP group and hence cover a larger area such as a neighborhood or campus. All APs in the mesh will offer identical service, so a client may connect to any AP in the group and even move between different APs within the group at any time. Irrespective of the AP within the group that the client connects to, the client will see their own home network and all their devices connected to it. From a client's perspective, the Custom Connectivity AP mesh acts as a single large AP covering the entire area with a single SSID.

When devices which are part of the same household service are connected to different APs in a Custom Connectivity AP group, inter-device packets must be exchanged between the APs to facilitate the inter-device communication. In Custom Connectivity, this inter-AP communication is accomplished with VXLANs. When Custom Connectivity recognizes that there are devices in the same household/segment connected to multiple APs, the APs establish bi-directional VXLAN channels between the APs to facilitate the device-to-device communication over a shared AP backhaul network.

For device-to-Internet traffic the Custom Connectivity architecture enables each AP to independently egress/ingress Internet access for connected devices without any intermediate network components. See Figure 8 for an illustration of how APs setup VXLAN, inter-AP, and extender connections.

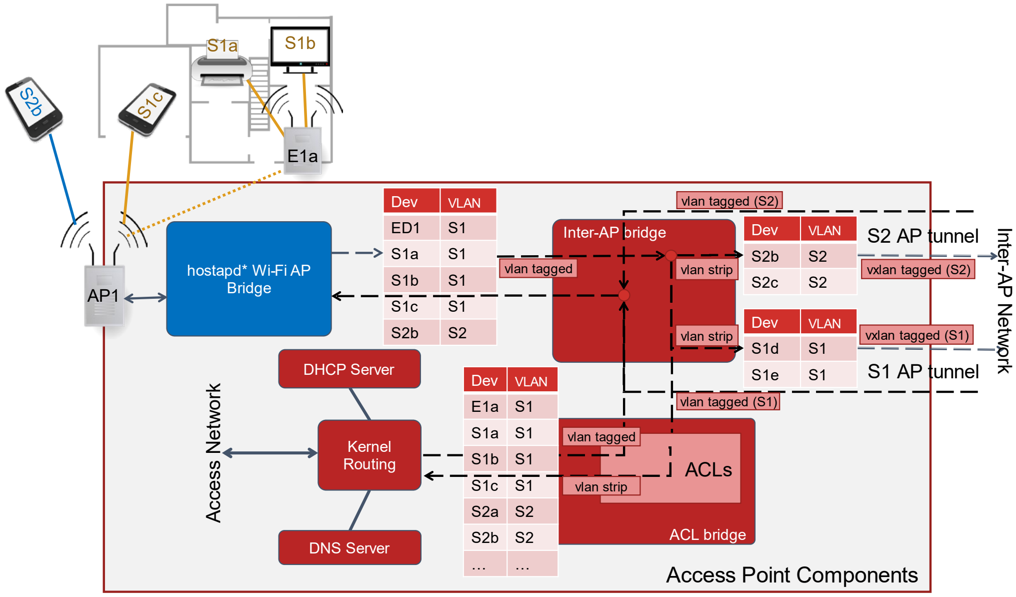


Figure 8: Inter-AP VXLAN, Extender and Access Network Interconnects

6.4 Enforcement of Service policies

Custom Connectivity's device-level identity and visibility allow for a wide variety of user-defined and operator-defined policies to be applied at both the device level and the service level.

For instance, operators likely will want to offer particular service offerings capped particular upload and download speeds. Custom Connectivity allows the maximum downlink/uplink BPS to be specified on a per-service basis – which can be specified by the operator via the Portal. As APs can independently egress traffic for a service, they share their respective egress/ingress rates to collectively enforce the limits using a distributed traffic shaping algorithm. This ensures that the subscriber's service policy isn't exceeded, irrespective of the distribution of their devices across the group.

Another example is the ability for users to assign per-device scheduling policy. Custom Connectivity allows for access hours limits to be defined and enforced more robustly than similar policy systems on other offerings. Since the policy is associated with both the identity and credentials of the device, a simple trick like changing the device's MAC address will not result in policy circumvention.

Many other policies are easily defined for Custom Connectivity – with the same ability to be tightly bound to the service and/or device identity and associated credentials.

7 Conclusion

The success of the trial allowed us to validate the capabilities of the Custom Connectivity architecture and helped us in taking one step closer to addressing the digital divide discussed in Section 3. We also learned a number of lessons from the trial that helped us refine our architecture as well some of the usability requirements.

This proof of concept helped us assert that as part of the overall evolution of cable broadband services and the build out of the 10G platform, the CableLabs® Custom Connectivity architecture provides another tool in the overall toolkit to the operators in the form of an alternate device-centric service delivery model.

8 Abbreviations

AAA	authentication, authorization and accounting
AP	access point
API	application programming interface
BSS	business support system
VLAN	virtual local area network
VXLAN	virtual extensible local area network
MQTT	MQ Telemetry Transport
OSS	operational support system
REST	Representational State Transfer
RSSI	received signal strength indicator
SCTE	Society of Cable Telecommunications Engineers
SSID	service set identifier

9 Bibliography & References

[1] Wi-Fi Passwords: The Evolving Battle Between Usability and Security; Society of Cable Television Engineers; https://scte.org/documents/3070/1742_Pratt_3216_paper.pdf
[2] WPA3™ Specification Version 2.0; Wi-Fi Alliance
[3] IEEE 802.11i-2004: *IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area network - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*; Institute of Electrical and Electronics Engineers
[4] CableLabs® Micronets; https://www.cablelabs.com/technologies/micronets
[5] Device Provisioning Protocol Version 1.2; Wi-Fi Alliance
[6] RFC 7348; Virtual eXtensible Local Area Network (VXLAN)