Towards Future-Proof Service Activation for Fiber to the Home Networks

Aditya Ganjam\(^\dagger\), Albert Greenberg\(^\dagger\), Chris Rice\(^\dagger\), Hui Zhang\(^\dagger\) and Jeff Fishburn\(^\dagger\)

1 Introduction

In open access fiber to the home networks, such as the Open Service Provider Network being built by DynamicCity for UTOPIA, multiple service providers compete to provide services to consumers over a single fiber access network. Using a common shared infrastructure, the network will support multiple types of services, which had traditionally been delivered over separate infrastructures. Though many access network challenges (e.g., limited bandwidth, channel impairments, high latency) do not exist in fiber to the home networks, management of configuration for Customer Premises Equipment (CPE), remains a key challenge, and may approach the complexity of router configuration. To offload the management of these devices from the home owner, remote service activation and device management is essential.

There are three key challenges. First, we expect rapid evolution and significant innovation in home devices and service gateways, resulting in the availability of CPEs from multiple vendors with diverse configuration options and formats. Second, open access will require rapid and cost effective service activation to support service provider choice for homeowners. Third, extremely low cost and extremely high reliable service delivery is required since existing services cannot be disrupted during activation of new services. The problem we address is to create a future-proof service definition and activation architecture, which supports potential churn in business models and end systems in the home.

We propose and have built a prototype of the solution illustrated in Figure 1. Upon request by a customer for a new service or change in existing service, the corresponding service provider requests the policy server to provision the CPE at the customer’s home (step 1). The provisioning server relays the request to a validation server to validate the request (step 2). The validation server ensures the customer’s CPE supports the requested service and will not adversely impact existing services. Upon receiving a positive response from the validation server, the provisioning server proceeds with generating the configuration and pushing it to the CPE (step 3). Finally, the policy server verifies that the provisioning event was successful (step 4).

This solution seamlessly copes with heterogeneity at two levels: First, at the service provider by implementing service activation and change through an abstract API, which enables multiple service providers to compete over a common infrastructure. Second, at the home by using a backend to generate device specific configuration files. Additional advantages are: service activation requests are authenticated, actuated and subsequently verified to ensure success. Furthermore, the system is future-proof as it can concurrently handle multiple versions of CPE and it provides a framework that can support services not currently defined. Our service activation platform accomplishes this by providing an abstract interface for service providers to specify the resources required to meet a service request, which can be extended as new services are defined. The use of configuration templates allows us to handle new devices introduces into the market.

Figure 1: System Architecture

Figure 2 depicts the devices within the home. A residential gateway serves as a media converter from fiber on the wide area to copper and as a multiplexer of different services. Both the access network and residential gateway must provide service isolation. VLANs, LSPs, CWDM and policy based layer three routing are some of the architectures that can be used to provide such isolation. Devices within the home, such as telephones, televisions or computers, connect to the residential gateway. Service specific functionality may be needed between the residential gateway and the end device. For example, video conversion functionality is needed to convert IP video to analog video that a normal TV can display. Clearly, there is opportunity to merge this service specific functionality with either the residential gateway or the end device; however, economics will determine the outcome.

We consider two models for provisioning/managing CPE devices. In the infrastructure provider model, all service activation is managed by the infrastructure provider of the access network. The infrastructure provider receives service activation requests from service providers and uses a policy server to manage the devices appropriately. The policy server allows it to maintain configuration information about all devices, yet provide an abstract interface to service providers that hides the
2 Solution Details

This section discusses details of the policy server solution, including hitless service activation, configuration guarantees and service verification.

2.1 Hitless Service Activation

Traditional service activation involves reconfiguration of the device. While operations staff may make configuration updates to fix bugs or install new policies, this is commonly done semi-manually. Since multiple services share a single device in the FTTH setting, it is critical to be able to activate services without restarting a device or affecting other services in any way. This requires devices to be able to start new services (or shut down services) without restarting and requires the policy server to generate atomic configuration to start or stop services. The policy server is able to do this by working with atomic component configuration templates and policies instead of monolithic templates.

2.2 Configuration Guarantees

The CPE have no out-of-band connectivity, unlike, for example, routers. Therefore, under no circumstances, should a configuration update to a CPE device disrupt IP connectivity. The only means of resolving such a mistake is a truck roll to the home causing a long service outage of all services sharing that device. In addition configuration updates must not affect proper functionality of other services. Static configuration rules can be used to guarantee that a configuration update does not disrupt IP connectivity or other services.

2.3 Service Verification

Provisioning events must be subsequently verified to ensure reliability of the network and services. End-to-end verification can only be reliably done by testing the service. For example, verifying a voice over IP service may entail making a phone call to the home and relaying a message that the service is operational. However, if a verification result is negative, then debugging of the service can be done automatically by probing the status of a device and static analysis of the result.

2.4 Policy Server Design

A service request to the policy server is defined using an XML data model, independent of the configuration format of any individual CPE. Each module within the CPE, such as a DHCP client, VLAN or firewall, begins with a top level XML element. Each service activation request is processed by five modules in sequence: Access Policy, XML parser, Template constructor, Presto configuration generator, and config push. In addition, two databases are used to maintain all state. The configuration database maintains records for each customer containing all values needed to create a configuration file for the customer’s CPE. This includes configuration variables, CPE types and CPE IP addresses. The template database maintains template information for each CPE type in the network. The templates are later used in conjunction with values in the configuration database to generate configuration files for the devices using the Presto configuration generator developed at AT&T. For each device type, the template database maintains separate component templates for every component that can be configured on the device. Example component templates are VLAN, IP, DHCP client, DHCP server and firewall.

3 Conclusion

Reliable service activation and management of homes in a fiber to the home will be the key challenge for these networks in the future. We propose a future-proof architecture for service activation and management where a policy server abstracts device specific configuration details from service providers and allows sharing of devices by multiple service providers. The solution copes with heterogeneity at each home where multiple services, service providers, and devices interact and at each service provider, where multiple services and homes interact.