Invention Title:	DOCSIS “Bring Your Own” Cable Modem provisioning improvement (via OpenFlow.)
Invention Summary:	This invention provides a model to simplify DOCSIS Cable Modem provisioning allowing Service Providers different options of how to self-provision by using the OpenFlow architecture to quarantine new devices.
Invention Description:	This invention provides a model to simplify DOCSIS Cable Modem provisioning allowing Service Providers different options of how to self-provision by using the OpenFlow architecture to quarantine new devices. See attached draft.
Invention Commercial Value/Customers:	The potential commercial value is in a self service workflow is valued in a satisfied customer and reduced OpEx for the MSO. But hidden in the mechanics of the solution is the opportunity build on value add services.
Invention Differences:	The invention was developed as part of the SDN working group’s effort of examining different MSO use cases and applying a solution involving Openflow in the DOCSIS network workflow. SDN, Openflow, and Cable is the unique use case.

INVENTION DISCLOSURE

1. Invention Title

DOCSIS “Bring Your Own” Cable Modem provisioning improvement (via OpenFlow.)

2. Invention Summary

This invention provides a model to simplify DOCSIS Cable Modem provisioning allowing Service Providers different options of how to self-provision by using the OpenFlow architecture.

3. Invention Description

Market Considerations:

Since the deployment of DOCSIS 3.0, more and more customer have been purchasing and deploying cable modems that are recommended by Service Providers to quickly upgrade to the higher speeds offered by this technology.

This process aims to design a provisioning process that empowers the customer to register his or her own service supported modem while offering several secure methods and options for authenticating and authorizing the new cable modem. This method attempts to scale the process making the identification of the new modem more reliable thus reducing the customer calls and support costs.

Technical Considerations:

The current provisioning process prone to errors and configuration errors when the only process is for the customers to call in and register the modems MAC address. The other documented process is to use a “walled garden” which is established through wildcard DNS. This method is thwarted when the CPE uses non-provider assigned DNS servers, such as, 4.2.2.6 or 8.8.8.8.

This disclosure defines the aspects of OpenFlow Controller and Switch specifics to the CMTS to achieve similar functionally.

Claims:

I. Defines a new process based on OpenFlow to identify “foreign” cable modems and offer a self-provisioning service that quarantines the modem from other production modems.

II. Defines an method which more reliably captures and redirects the “foreign” cable modem to a safe network which quarantines these modem from production modems in a reliable

Claim I:

Figure 1 shows the OpenFlow switch corresponds to the CMTS. For this proposal it is assumed the CMTS switch will support OpenFlow. An additional network is created to serve as the network to host “foreign” modems.

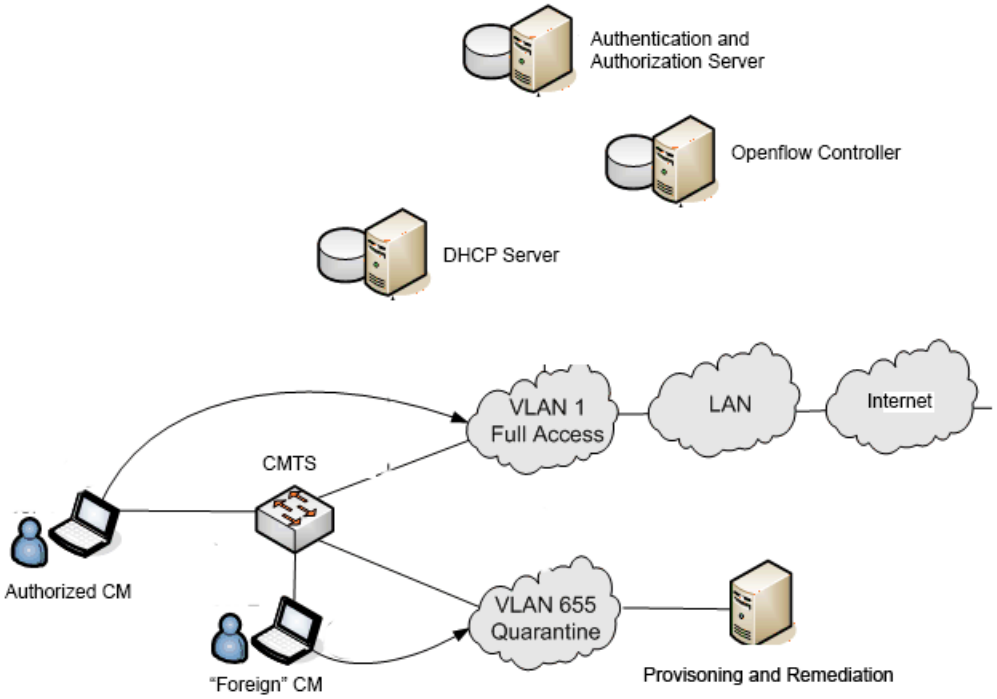

Figure 1 Openflow Components

Service Flow

1. The customer orders the high speed data service
2. The customer purchases a retail and provider supported modem
3. The customer plugs in cable modem.
4. Cable modem initializes.
5. Cable modem obtains DHCP address and TFTP server address for configuration download.
6. Cable modem contacts the authorization server to validate the MAC address
7. The MAC address is NOT found and is designated a minimal configuration file for registration.
8. Cable modem downloads configuration to establish a minimal registration.
9. The Cable modem is placed on a VLAN to preform remediation and authentication services, called “Quarantine”
10. The CPE requests DHCP address which are directed to Quarantine DHCP
11. DNS requests are intercepted and rewritten to always redirect to provisioning services.
12. The provisioning server collects the MAC address and the type of modem used via SNMP or other means.

13. The CPE is instructed to authenticate via account login, registration, account number or any combination of methods.
14. Optionally, an additional authorization step can be inserted to allow the service provider to inspect the cable modem and account association by manually approving the request and transaction. Each step of the process allows for CPE feedback and interaction. Filtered access (read: inline) is provider configurable and available to the CPE during any approval process delays.
15. Cable modem is reset to switch to production and full access.

Claim II:

Detail the DNS protocol and the use of Openflow rewrite rules to spoof or redirect DNS requests to the serving DHCP server. Additionally, provide any needed back end load balancing techniques as needed.

The critical technique that may need some explanation is Openflows ability to set a specific port–based VLAN using Openflow analogous RADIUS 802.1x Dynamic VLAN Assignment.

a) Why was the invention developed? What problem(s) does the invention solve? How is it better?

The invention was developed as part of the SDN working group's effort of examining different MSO use cases and applying a solution involving Openflow in the DOCSIS network workflow. This invention enables the customer to have a simple, automated, and user experience when purchasing a third-party a cable modem and installing it on their own, reducing provisioning time and reducing support costs.

b) Briefly outline the potential commercial value and customers of the invention.

The potential commercial value in a self service workflow is valued in a satisfied customer and reduced OpEx for the MSO. But hidden in the mechanics of the solution is the opportunity build on value add services.

4. How is this invention different from existing products, processes, and systems?

This process offers the customer a self service provisioning solution while giving the MSO an opportunity to examine new devices requesting service, the ability to intervene and remediate, and protecting their existing customers. This solution reduces operating costs and offers the ability to provide add on services, such and security diagnostics and data filtering.