Virtualizing the Home Network

Michael Kloberdans
CableLabs

Abstract

One of the areas of focus in the Cable industry has been a virtualized home network. This paper proposes a road map with an analysis and recommendations, which can assist service providers to develop their technology strategies to meet today's and tomorrow's changing needs. Specifically, this paper will address:

- *Encapsulation*
- *Control Protocols*
- *Multiple Home Routers*
- *Virtual Function Technologies*
- *Operational Concerns*

BACKGROUND

CableLabs has been analyzing how cloud-based network architectures can help service providers enhance their service offerings and provide new features with faster time-to-market and reduced costs. This paper summarizes an analysis directed towards virtualizing the home network.

TRANSPORTING DATA STREAMS

Encapsulation is a means to transport home network information across the access network as shown in Figure 1.

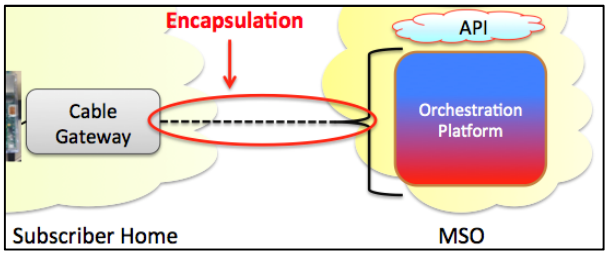

Figure 1: Encapsulation

Encapsulation requires both marking data streams at the home gateway and transporting those streams between the home gateway and the service provider cloud. Virtualization allows one to think in terms of services, and not just devices. We mark packets in order to apply a policy or service to those packets, such as VoIP, Parental Control, etc. A policy is therefore applied to a stream of packets that qualify for a specific type of service from the service provider.

One exciting opportunity offered by virtualization, is to enable new services to be applied to groups of devices in ways that are not practicable using traditional approaches. For example, a subscriber can access an MS service provider 'service portal', and define which data devices in the home should be part of a particular service group. For example, the subscriber may choose to place two tablets, an Xbox gaming unit and a printer to be gathered in the Kid's service group. Those devices would then have a specific firewall policy (e.g. allowing Xbox traffic), a specific parental control policy (e.g. time limits and restricted web access) and perhaps even specific virus protection software that excels at gaming threats. Data stream marking is critical in identifying, not only a subscriber, but also service groups that have multiple devices in each group. It is then possible to apply multiple firewalls and other services to a single residence, again, based on service groups and not just a residence location.

Data stream marking can be done at layer-2 if tunneled using VLANS, or newer approaches such as IEEE 802.1ah (mac in mac). Layer-3 can be used to identify service groups, both IPv4 and IPv6, especially if tunnel technologies are used. While one could use a single tunnel for each service group in a

home, this method doesn't scale well and is not popular with service providers. Leveraging unused or little used IP header fields in the 'inner' IP header of a tunnel is an option for classifying group data flows, however, straying from best practices always has consequences and leads to proprietary protocols, which is not the goal of virtualization.

Tunnel endpoints terminate at a layer-3 device at the edge of the home to an aggregation router in the service provider network. The home device may be an eRouter (e.g. Cable Modem and router in a single box) or it may be the subscriber's router behind the Cable Modem (CM). Another idea for marking group flows is a mapping of a pre-assigned value that is not intrinsically tied to a device and placed in a table in the service provider cloud. One could associate the value 347, as an example, to indicate that the flow requires BW on demand, VoIP support and business strength firewall. A nice benefit of a seemingly arbitrary value is the security feature of not exposing VLAN or MAC information outside the home. Below is a diagram showing all the areas discussed in this paper.

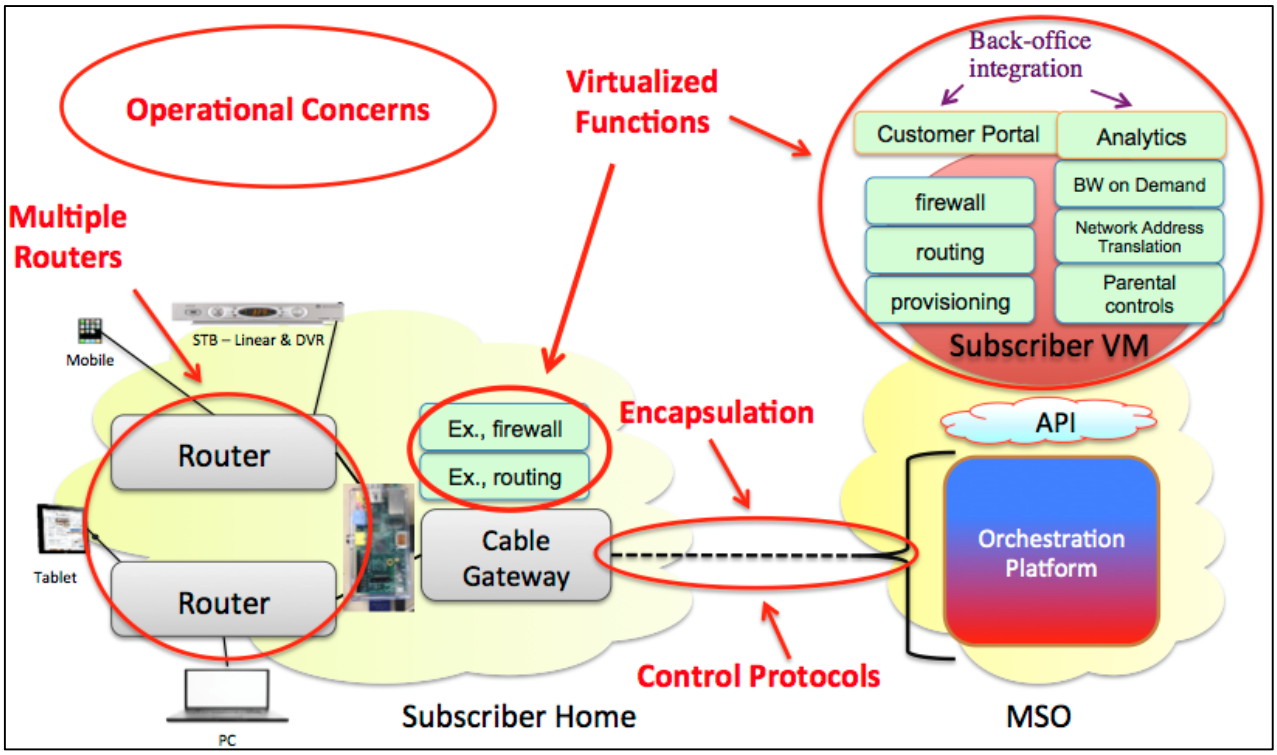

Figure 2: Challenges in the Virtualization Problem Space

Even though they may be considered individually, all areas in the problem space are interrelated. Thus, security, control protocols, latency, etc. are part of the encapsulation analysis. We've discussed marking data flows for Service Function Chaining (SFC), and now need to focus on transport protocols to complete the encapsulation analysis. As mentioned previously, there are various tunneling protocols available to transport data flows between the home gateway and the service provider cloud. Most of these tunnel protocols are well known, and there isn't need to discuss them here, other than to warn of scalability issues. Scalability is the driver to have only one tunnel to a subscriber's home.

A new protocol is also being developed by the IETF called Segment Routing. This protocol

has the advantage of 'steering' traffic from a source to a destination. While there is great promise with this protocol, it is still draft and only supports IPv6, making it unsuitable as a stand-alone solution for service providers.

CONTROL PROTOCOLS

The Cable Gateway must be both provisioned and maintained, which is the function of control protocols. The challenge here is supporting both legacy devices, which might be quite old, while embracing new devices. Because it is unreasonable to expect legacy devices to add support for new protocols, SNMP and TR-069 will continue to be used during the transition to smart devices. TR-069 is the preferred alternative to SNMP to avoid the need to support more than one legacy protocol.

MULTIPLE HOME ROUTERS

A decade ago, most homes had a single router. This device had ports that provided IPv4 addresses (DHCPv4 & NAT), switch ports, and perhaps WiFi service. Today, many homes have more than one router often merely to extend the WiFi range in their home as end devices are increasingly leveraging the ease of connectivity and mobility that WiFi provides. However, instead of buying a WiFi extender, many people have simply bought another router, not understanding the difference. Now, there may be two boxes providing firewalls (which is not optimal, but the system still works), and also NAT. Two NAT sources can often dole out private IPv4 addresses from the duplicated IP pool space of 192.168.1.x. Now there is a real chance of encountering duplicate IP addresses. Even if there is only one IP address given to a device, only one of the routers will recognize that address as being leased, and that router may not be the default gateway. This leads to network connectivity issues in the home and is difficult to troubleshoot, especially remotely.

The story gets more complicated as other routers covertly enter the home, disguised as something else, like a Chromecast or Roku USB stick. These are actually layer-3 devices. And the hardware and software used for home security is often a layer-3 device. We can now see that many 'devices' are actually L3-aware devices. Why is that an issue? In a word, visibility! We lose the visibility of important layer-2 information when a router shields it. A layer-3 device will act as a proxy for protocols such as DHCP and ARP requests. The router will substitute its own MAC address, again as a proxy, for these protocols thereby obfuscating the layer-2 information we need to see in order to troubleshoot problems. Without the visibility of these end devices, Service Providers cannot determine which devices are the cause of (for example) exceeding data caps, or help with troubleshooting when a subscriber calls with a problem. Without visibility, we cannot offer new or enhanced services.

One of the largest gains of virtualizing the home network is to enable techniques that allow ISPs to see the layer-2 connectivity information for devices in the home. This makes it possible to logically extend service groups that span multiple routers as illustrated in Figure 3.

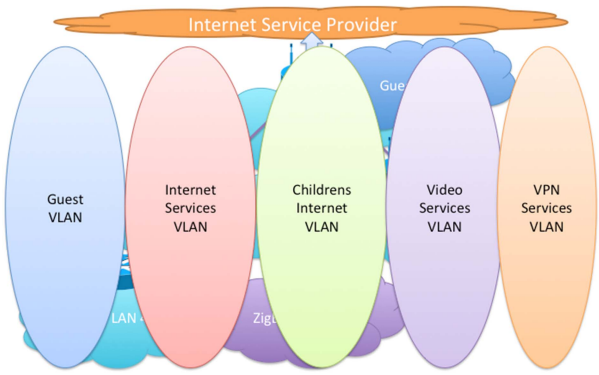

Figure 3: Example Service Groups Spanning Multiple Routers in the Home

Troubleshooting can be greatly enhanced if the service provider has information about

devices connected to the home network. For example, a subscriber calls the service provider help desk to report that a tablet cannot connect to the wireless radio on the router. The help desk technician sees that there are two tablets on the premise, and one is connected. They can know with confidence that the Router's WiFi is working and explain that the problem is most likely with the setup of the second tablet. This can also eliminate sending a service truck to the residence.

Home routers are becoming very sophisticated with new protocols such as IEEE 802.11AC, dual band radios, Service Discovery using UPnP, multiple guest SSIDs, beam forming, NAT implemented in hardware, etc. These modern routers need more features to allow the visibility needed in a multi-router home. Protocols such as GRE can tunnel layer-2 information to the service provider's virtual cloud infrastructure to enable analytics which help drive innovative new services.

Some Service Providers want to virtualize typical router functions, such as DHCP and NAT, and provide that service from the cloud. The benefit is the visibility, at layer-2 of the devices needing these services. Another benefit in providing typical home gateway services in the cloud is the time it takes to update existing, or create new services. If ten thousand home gateways rely on the ISP for DHCP services, for example, the updated DHCP function is replaced in one location in the cloud, eliminating the task of pushing out an upgrade to those thousands of devices. The speed of implementing a 'flash' upgrade is vastly reduced compared to the phased approach of delivering the change across thousands of end devices. Equally important is the time saved in testing. Because the feature is virtualized, there is no need to test the feature on multiple vendors' products, and multiple hardware and firmware versions for each of the vendor's products. Thus, a new or upgraded feature can be implemented in only a few weeks instead of typically 12 – 24 months. This results in OPEX savings, increases reliability and speed to market.

VIRTUALIZED NETWORK FUNCTIONS

A Virtualized Network Function (VNF) is a traditional network node feature that has been implemented in software with well defined, inputs and outputs instead of proprietary hardware. Common examples are NAT, Firewall, Parental Controls and other, newer features such as VoIP, bridge conferencing and WAN Accelerators. Open interfaces are required to enable the VNF module to be used in conjunction with other VNFs and management and orchestration systems originating from multiple vendors. This is the objective of industry bodies such as the ETSI NFV Industry Specification Group.

Because network node functions are now implemented in software, they are no longer restricted to the physical location of a piece of hardware. The previous section described some benefits of placing VNFs in the Service Provider's cloud. However, it is also perfectly acceptable to place the VNFs on the home gateway, for example to reduce Latency.

Latency: optimum placement of the VNF may be important for certain applications. For example, if two gamers were competing in the same residence (an extreme example), latency would be minimized if the home gateway provides the bridging or routing.

If the same function were moved to the ISPs cloud, the path between the gamers would have to extend from one gamer, to the ISPs nearest node of support and back again to the other gamer in the same home. The signal propagation through copper, or even fiber, would add latency to the path, as well as processing the signal at the ISP and again when received by the home gateway.

Operational Impact: There are significant cost and operational implications for the Service Provider to implement virtualization. Specifying and deploying VNFs requires new operational processes as well as investment to purchase the server infrastructure. Whether a network feature is provided on the home gateway or in the cloud, the feature hasn't changed for the subscriber. The subscriber has not perceived any new value even though the home hardware has changed and a sizable investment has been made in the provider's infrastructure. It is true that the subscriber now has access to a portal that lists new and enhanced services, but the basic network functions provide the same experience as the previous solution. The Service Provider reaps the benefits of faster time to market streamlined operations which should improve customer experience.

Fault Protection: If the VNFs associated with the home network reside in the service provider cloud it is important to consider what happens when the WAN link to the home goes down. Even minimal network features would no longer be available. Take for example a neighbor who visits a home that has lost their WAN link to the ISP. The neighbor brings their tablet and wants to print a picture. That simple action is thwarted because the tablet cannot get an IP address for the home network because the DHCP services are hosted in the ISP's cloud. If routing decisions are made in the ISP's cloud, then all communications between service groups (e.g. VLANs) in the home cease when the WAN link goes down. One solution to this issue is to have a latent basic set of network functions that still reside in the home gateway. They become active when triggered by some logic which determines that the WAN link has been down for a reasonable mount of time, and it is time to provide basic services in the home. Solutions are beginning to appear that address this issue.

Another promising approach is to provide a hybrid solution where basic VNFs are placed on the home gateway for fault tolerance and cost reasons, and the more sophisticated VNF functions are located in the service provider's cloud. Not all VNFs are equal in their demands for CPU and/or storage resources. A basic firewall VNF could easily be placed on the home gateway and a superior firewall offer could be service provider cloud-based. The home firewall would supply most of the everyday needs and the ISP advanced firewall could handle the tougher cases where CPU and storage demands exceed that of the home gateway. The author believes this hybrid approach is the future of VNF placement because it makes sense for the subscriber by providing fault tolerance and for the ISP because is saves costs. In this vision the service provider cloud extends into the home network with the gateway having similar capabilities to a cloud-based server albeit with a cost-sensitive approach to its' design.

CONCLUSION

There are significant benefits for service providers to reduce cost and improve customer experience by virtualizing the home network, but there are also challenges. Some of the more important challenges have been examined in this paper and are being addressed by collaborative work being undertaken at CableLabs and in conjunction with the wider industry.

REFERENCES

Chris Donley, SDN & NFV: Moving the Network into the Cloud, *http://www.cablelabs.com/sdn-nfv/*

ETSI : Network Functions Virtualisation http://www.etsi.org/technologies-clusters/technologies/nfv