NETWORK VIRTUALIZATION IN THE HOME

Chris Donley
CableLabs

Abstract

Networks are becoming virtualized. While there has been significant focus on virtualization in core and data center networks, network virtualization will also provide benefits in the home. From reducing equipment costs to simplifying software upgrades

CableLabs has been exploring how Network function Virtualization (NfV) and Software Defined Networking (SDN) can affect cable subscribers' home networks. This paper will present a vision for future home networks, specifically:

- *A Virtualized Home Network Architecture*
- *Virtualized Home Network Functions*
- *Virtualization Benefits to MSOs and Subscribers*

INTRODUCTION

Home networks are growing more sophisticated; customers are not. As home networks become more complicated, many customers are looking to MSOs to support these more complicated networks, and MSOs need tools to support them. Network virtualization using technologies such as Software Defined Networking (SDN) and Network function Virtualization (NfV) provides such a set of tools.

Generally speaking, SDN describes an open architecture comprising a set of APIs, and control protocols such as OpenFlow that allow for dynamic, distributed provisioning and automation.

NFV decouples network functions such as firewalls, deep packet inspection, caching, etc., from proprietary hardware so that they can be run in software on generic (e.g., x86) servers.

While SDN and NFV can be implemented independently, the benefits multiply when the technologies are combined The architecture described below illustrates a combined approach for MSO subscriber networks.

HOME NETWORKS TODAY

Home networks are evolving. Most subscribers today connect to the Internet using a router. As shown in Figure 1, subscribers are connecting additional routers to their networks to extend the reach of their wifi, or to add services such as home automation and security, IP video, and sensor networks (e.g., Internet of Things). Home routers, however, typically do not run a routing protocol, and networking these routers was challenging, and usually required multiple layers of IPv4 Network Address Translation (NAT). As customers are interconnecting devices within the home for video streaming or remote printing from tablets, these multiple layers of NAT are becoming problematic and severely hamper these in-home services.

To address these problems, CableLabs, in conjunction with MSOs and technology suppliers, developed HIPNet™, a new architecture leveraging IPv6 provisioning to automatically configure home routers into a routable network without requiring NAT on

interior routers. HIPNet functionality is becoming available on cable eRouters, and represents a significant improvement over previous technology. However, some challenges still remain. Service Discovery across routers (e.g., to allow Smart TVs to locate DLNA media sources) is challenging, and MSOs do not have an easy way to manage this proliferation of home routers on behalf of their subscribers. In addition, it is difficult to add new home network services, as they rely on the capabilities of the routers already deployed, and may require a new device to support new features.

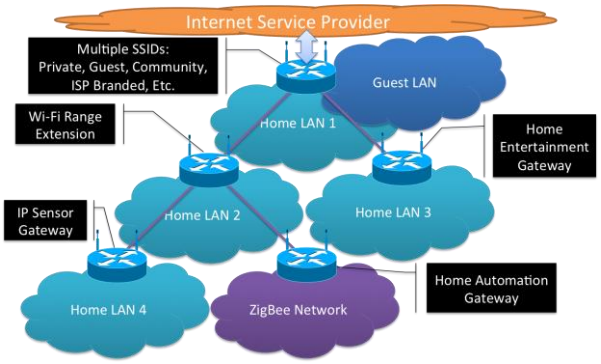

Figure 1: Evolving Home Network

A VIRTUALIZED HOME NETWORK ARCHITECTURE

One solution to the growing complexity of subscriber home networks is to virtualize the home network so that it can be managed by the MSO (or the subscriber via a self-service portal). This allows us to move beyond the device-centric architecture we use today and consider a virtualized service-centric architecture, which offers MSOs the ability to better manage subscriber networks and to understand how customers are using them, and offers subscribers a way to tailor the network to optimize their specific use cases such as gaming or video streaming.

Routing vs. Bridging

There has been a debate among home networking experts about whether to use routing or bridging inside the home. Many problems experienced in a routed home network, such as service discovery, multiple firewalls, and multicast forwarding, become simpler in a layer 2 (bridged) network. However, existing devices typically include routers. Also, some emerging services such as Smart Grid or home automation and security require routed networks for security purposes or to satisfy regulatory requirements.

In a virtualized home network, we can have the best of both worlds. First, the home network can be separated into different logical policy domains, such as for Internet access, guest access, VPNs, or in-home video sharing. See `Figure 2`. Each zone can be assigned its own firewall and connectivity policies. Next, each zone is distributed throughout the house using encapsulation techniques such as VXLAN. Finally, hosts are assigned to one or more zones. Because devices can receive multiple IPv6 addresses, it is conceivable that they will receive unique addresses for each zone. By default, they would be assigned to the Internet or Guest zone (for a Guest WiFi network), and could be assigned to different zones, as well.

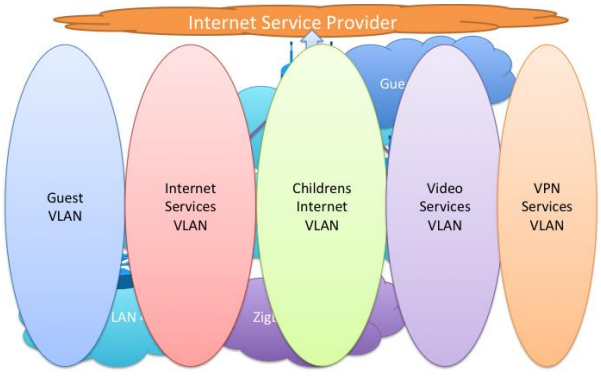

Figure 2: Virtualized Home Network

Within each zone, which could stretch across router boundaries, traffic is bridged. This would offer subscribers an improved quality of experience. No longer would

nested internal NAT functionality interfere with printing or video streaming, and link-scoped service discovery mechanisms such as mDNS would show all the devices in a particular zone, rather than just those devices on the local subnet.

Bootstrapping

When the network first comes online, it needs a basic level of automatic configuration support plus a path to reach the MSO network controller. HIPNet, included in eRouter devices, provides this level of connectivity using DHCPv6 prefix delegation to provision routers in a tree topology and establish routes to all the devices. It is optimized for Internet connectivity, and also supports host-to-host communication, but perhaps not in an optimized manner. Once network connectivity is established, the home routers can contact the MSO network controller for optimized forwarding instructions using protocols such as OpenFlow or TR-069.

To create optimized forwarding paths, the MSO network controller needs topology information from the home network devices. Home routers can collect this topology information using Link Layer Discovery Protocol (LLDP) and communicate it to the MSO controller using OpenFlow or similar protocols. The MSO controller can then use the Dijkstra algotithm (also used in routing protocols such as OSPF and ISIS) to compute optimal forwarding paths and communicate them back to the subscriber's routers. Subscriber routers can also collect and report attached host MAC and IP addresses to help troubleshoot issues that may arise in the home and to further optimize traffic forwarding.

In the event of an Internet connectivity failure, this architecture would allow the network to use a backup connectivity mechanism such as WiFi. If that is not available, the home network will continue to operate, albeit with more basic HIPNet functionality. Thus, the MSO controller provides optimizations when the service is connected, but the home has local survivability.

While a virtualized network architecture as described above can improve a subscriber's quality of experience, it is not yet sufficient to deliver on the promise of enhanced management and customizability. For that, let's explore various home network functions and how they could be delivered to our virtualized network.

HOME NETWORK FUNCTIONS

Home networking devices typically perform a number of functions on behalf of the customer. These features can be divided into two types: control plane and data plane. Control plane features look at packet headers and enforce policy on a network, while data plane features are inserted in the traffic forwarding path and affect the payload of the traffic.

While not an exhaustive list, control plane features include:

- Network Address Translation (NAT), which provides differentiation between customer space and public space and which is used to manage IPv4 address scarcity during the transition to IPv6.
- Firewall, which enforces security policy on the network
- Routing and forwarding, which identifies the optimal paths to send traffic through the network.
- Virtual Private Networks (VPNs), which provide private connectivity to remote networks such as corporate offices.
- IPv6 transition technologies

Likewise, data plane features include:

- Dynamic Host Configuration Protocol (DHCP) and Domain Name Service (DNS), which provision devices with IP addresses and provide database lookup services to identify other hosts
- Deep Packet Inspection, which looks into packet payloads and helps with Denial of Service and Parental Controls
- Denial of Service protection, which looks for traffic anomalies and block unwanted traffic streams.
- Parental Controls, which block objectionable content.

Until now, these features have generally been offered on home routers, and configured separately on each router. This has led to a sub-optimal experience for subscribers, who have looked to the teenager down the street or commercial services such as Geek Squad to configure their routers. With network virtualization techniques, MSOs can host all of these services in their data centers and offer them to subscribers as cloud services.

In addition, customers are interested in some control plane features that are not widely available today, either because they have not been possible, or because they have been difficult to implement with existing devices, but that could be delivered in a virtualized environment:

- Bandwidth on demand, where subscribers can change bandwidth levels on the fly to accommodate large file transfers (e.g., downloading a movie before a flight).
- Priority service for video or gaming services, allowing subscribers smooth delivery of entertainment content.

Recently, many in the industry have been considering virtual CPE (vCPE), an approach for moving network functions into per-subscriber virtual machines in the cloud. Control plane features such as firewalls and parental controls are obvious candidates to move into the cloud. Both can be configured via a self-service or technician web portal, with policy pushed into the home using SDN, and enforcement performed as close to the customer device as possible. See Figure 3.

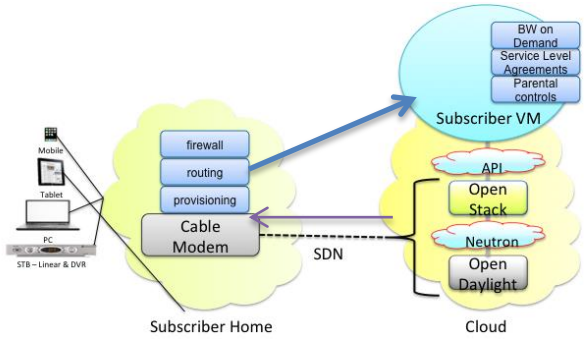

Figure 3: Virtualized CPE

Parental controls are slightly more interesting, as they also involve content filtering, and require deep packet inspection to look for objectionable content. Such a service would be far more robust than traditional DNS-based controls available on home routers. To perform these functions, the parental control function needs to be performed in-line on the data plane. Thus, the customer traffic requiring parental control will be routed through the data center and passed through parental control and other data plane network functions using service chains, a mechanism for passing traffic flows through multiple network functions on their way to the Internet or back to the home network.

Once the virtual network is in place, it allows MSOs to offer new network services such as Bandwidth on Demand or enhanced service levels for high-value content such as video streaming or gaming. Indeed, we have already taken the first steps. CableLabs has developed a PacketCable MultiMedia (PCMM) plugin for OpenDaylight that can be integrated into such a framework. OpenDaylight, combined with our PCMM plugin, provides a RESTful interface for adding, modifying, and deleting DOCSIS®

service flows. This would allow a subscriber to create a new service flow (e.g., for gaming) with defined bandwidth and DOCSIS QoS characteristics.

BENEFITS

The home network described above offers benefits for both MSOs and subscribers. MSOs benefit from reduced expenses, faster time-to-market with new services, and optimized use of deployed resources. Subscribers benefit from mass-customized services and service-centric policies (as opposed to device-centric policies today).

MSOs stand to benefit from reduced expenses, as this virtualized network architecture allows for self-service provisioning via a web portal, simplified upgrades managed by DevOps tools such as Puppet and Chef, and simplified inventory management and certification testing, as the functionality is delivered in software, rather than via specific devices. It also gives MSOs more visibility into the devices attached to the subscriber network, helping them troubleshoot and optimize the network on the subscriber's behalf. As network functions are deployed in software, this architecture offers MSOs shorter build-measure-learn development cycles that will bring new features to market faster. Finally, as virtualized network resources can be shared across multiple subscribers, it allows MSOs to optimize the use of deployed resources.

For subscribers, network virtualization offers a mass-customized Internet service. Just as we have seen with cellphone app stores, subscribers value different aspects of a service. Under this approach, they can drag and drop those features that are important to them. For example, an avid gamer might select optimized gaming service, while parents might opt for strict parental controls. As services can be tailored to individual subscriber needs, this approach offers an enhanced quality of experience over today's networks. In addition, network policies are tied to the user, and not the device. This allows subscribers to have the same Internet experience at home or on the road through Cable WiFi.

CONCLUSION

In conclusion, home networks are becoming more sophisticated, but subscribers are not. Network virtualization allows MSOs to offer subscribers a new network architecture that is mass-personalized, automated, and tailored to individual needs. This architecture includes service-(or policy-) specific overlay zones that can be extended into the MSO data center to allow delivery of MSO-managed network features. From the data center, MSO SDN controllers can push policy to individual network devices, optimizing network forwarding paths and enforcing firewall policies. These changes offer improved economics to MSOs and an improved quality of experience to subscribers.

REFERENCES

John Berg, The Future of Home Networking: Putting the 'HIP' in HIPnet, http://www.cablelabs.com/the-future-of-home-networking-putting-the-hip-in-hipnet/

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

VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, draft-mahalingam-dutt-dcops-vxlan-08.txt

Puppet: http://puppetlabs.com/

Chef: http://www.getchef.com/