Slicing Home Networks

Yiannis Yiakoumis
Stanford University
yiannisy@stanford.edu

Home Networks are becoming an essential part of each modern household. Besides traditional e-mail and browsing, we use our home network for entertainment, communications, e-commerce, file-sharing and backup, etc. But despite increasing broadband speeds and a plethora of networked devices, home networks still face systematic challenges :

- Hard to manage : The average home user lacks the technical background to manage and configure his network, which typically operates with the default settings. This results to poorly secured and managed networks, failure to integrate multiple devices, and potentially lack of functionality desired by the users.
- Hard to customize : The home network cannot be customized for the needs of specific applications, such as video streaming. It lacks the mechanism to introduce new functionality and to allow others to innovate and customize its behavior.
- Hard to share : The infrastructure to the home (last-mile connection) is inherently expensive to deploy and maintain. Nevertheless, in all cases deployment is driven by a single provider, requiring huge investments and risk, limiting user's choice and preventing other providers from using the same infrastructure to amortize the cost and share the burden among multiple parties.

Our project explores an architecture to mitigate these problems, by allowing multiple providers to co-exist over the same infrastructure. For example, a third party could provide enterprise-level network management service to the end user by setting firewall and wireless passwords, configuring QoS policies and enabling features such as parental control. Extending our view of the home network to the last-mile connection and first hop in the ISP's access network, a utility company could use the existing infrastructure for applications like smart-grid measurement collection; and similarly, a company like NetFlix could customize the network to provide better video quality. Our goal is to give users the choice on how to use and manage their home networks, and let providers reach the end-user and decide how to share the infrastructure to the home. We don't advocate any specific policy for how the network should be shared. Instead we explore a simple mechanism that allows different policies to be applied and enables their independent evolution.

We propose *network slicing* as a mechanism to share the home network among multiple providers. A user creates a "slice" and delegates control to a third-party. Each slice is isolated from others in terms of traffic, bandwidth and control. Traffic isolation is necessary to ensure that data don't leak from one slice to another. Bandwidth isolation prevents one slice from starving another; (in addition to bandwidth other resources like CPU or memory might need to be isolated). Control isolation makes sure that a slice cannot affect how another slice behaves. Besides isolation, the control logic that defines the network behavior of a slice, can be customized and modified to fit this application's needs.

We select three types of applications that motivate our work and based on these we develop a prototype to show how they can operate on top of a sliced infrastructure.

- Outsource Network Management : A home user outsources control of his network to a third-party with appropriate expertise. The service provider can remotely set firewall rules, QoS policies, configure wireless power levels and so on, while providing an interface for the user to monitor his network and apply high-level policies such as parental controls. Inferring knowledge from multiple homes, the provider could further augment his service, for example by detecting security threats and proactively secure the network against attacks [2]. In our prototype, besides being the default slice of the network, the network management provider also manages slicing. It allows the user to subscribe to services, creates the appropriate slices and delegates control to the respective providers.
- Guest WiFi : This application highlights infrastructure sharing among multiple providers. The

user creates a “Guest WiFi” slice of his network which he can share with his guests and friends, or contribute to a community or commercially crowdsourced WiFi network. Control of this slice is outsourced to a third party which provides appropriate AAA services (Authentication, Authorization, Accountability). To protect the home user’s experience and privacy, bandwidth and traffic should be isolated. Besides, the home user should still be able to secure and manage his own network as he would without the Guest WiFi service. The Guest WiFi slice itself requires individual control to be able to set firewall rules, drop packets, redirect and shape traffic etc.

- Customized Slice for Video Streaming : Video streaming is a common and popular application for home networks. Content providers like NetFlix have both the expertise and incentives to optimize the network in order to deliver better product to their users. For example, the content provider could obtain a slice with sufficient bandwidth guarantees to support the high datarates of the video stream. Further, it could customize the slice to handle packet loss and caching in a way that is optimized for video delivery, to ensure a smooth and high quality user experience. Extending the slice within the home network, the content provider can now provision video delivery in an end-to-end manner, i.e through the last-mile link and up to the end- device playing-back the video. Given the ability to modify how forwarding takes place, the application provider can implement his own routing mechanism, use replication and retransmission methods to optimize video streaming over wireless, or even implement a customized congestion control protocol. The slicing mechanism should support bandwidth and traffic isolation, as well as allow the provider to customize the slice for its own needs.

To evaluate slicing we are working on a prototype and deployment in users’ homes. Figure 1 shows our architecture. The network substrate consists of programmable network elements. These are wireless APs on the home side, and an ethernet switch on the access network. A slicing layer sits on top of the network substrate enforcing bandwidth, traffic and control isolation. For our prototype we use OpenFlow [3] and SNMP to control and configure the network elements. We build on FlowVisor [5] for the slicing layer functionality. To facilitate users to select services, a slicing manager acts as a service broker to advertise new services, control subscribtions, and translate these into low-level network semantics. Our design is sufficiently extensible to accomodate additional functional blocks like traffic classification, anonymization and aggregation. A slice is a separate control plane on top of the slicing layer. In our case we have three different slices : network management, guest WiFi and video streaming. Our current deployment spans 10 homes (on and off campus) and an access network switch at a Stanford dorm, while the control-plane for each of these slices runs at a remote server.

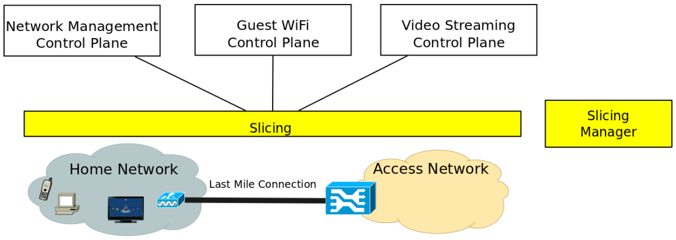

Figure 1: Slicing on a Home Network : Multiple service providers share the same infrastructure. Each provider controls a given slice, and a slicing layer enforces isolation between different slices.

Our early experience suggests that slicing is a plausible mechanism to share the infrastructure among multiple providers and enable a gradual evolution of the home network. Moving forward, we want to further experiment with applications and show the benefits of a sliced architecture into the home. We want to better understand the trade-offs between performance, flexibility, and simplicity, and see how these affect users’ experience and choices.

1. REFERENCES

[1] Telecommunications act of 1996, pub. la. no. 104-104, 110 stat. 56 (1996).

[2] N. Feamster. Outsourcing home network security. In *Proceedings of the 2010 ACM SIGCOMM workshop on Home networks*, HomeNets ’10, pages 37–42, New York, NY, USA, 2010. ACM.

[3] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74, April 2008.

[4] O’Donnell, Shawn. Broadband Architectures, ISP Business Plans, and Open Access. http://dspace.mit.edu/handle/1721.1/1513.

[5] R. Sherwood, G. Gibb, K.-K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar. Can the production network be the testbed? In *Proceedings of the 9th USENIX conference on Operating systems design and implementation*, OSDI’10, pages 1–6, Berkeley, CA, USA, 2010. USENIX Association.

[6] D. Valtchev and I. Frankov. Service gateway architecture for a smart home. *Communications Magazine, IEEE*, 40(4):126 –132, Apr. 2002.

[7] Y. Yiakoumis, K.-K. Yap, S. Katti, G. Parulkar, and N. McKeown. Slicing home networks. In *Proceedings of the 2011 ACM SIGCOMM workshop on Home networks*, HomeNets ’11, 2011.