Thèse de Doctorat de l'Université Paris VI
Pierre et Marie Curie

Spécialité

SYSTÈMES INFORMATIQUES

présentée par

Lucas Di Cioccio

pour obtenir le grade de

Docteur de l'Université Pierre et Marie Curie

Home Network Monitoring

À soutenir le 22 Avril 2013 devant le jury composé de

MM. :	Nick	FEAMSTER	Rapporteurs
	Konstantina	PAPAGIANNAKI	
MM. :	Ernst	BIERSACK	Examinateurs
	Serge	FDIDA	
M. :	Martin	MAY	Encadrant
Mme. :	Renata	TEIXEIRA	Directeur de Thèse

Thèse de Doctorat de l'Université Paris VI
Pierre et Marie Curie

Spécialité

SYSTÈMES INFORMATIQUES

présentée par

Lucas Di Cioccio

pour obtenir le grade de

Docteur de l'Université Pierre et Marie Curie

Home Network Monitoring

À soutenir le 22 Avril 2013 devant le jury composé de

MM. :	Nick	FEAMSTER	Rapporteurs
	Konstantina	PAPAGIANNAKI	
MM. :	Ernst	BIERSACK	Examinateurs
	Serge	FDIDA	
M. :	Martin	MAY	Encadrant
Mme. :	Renata	TEIXEIRA	Directeur de Thèse

Acknowledgements

As I am not the best at coming up with original acknowledgements, I will try to keep it simple. Anyway, I think that "simple" is a good-enough qualifier for me and I am a strong believer of the *KISS* (Keep It Simply Stupid) principle. I feel thankful to so many people for so many things ... such that I am afraid I will forget someone. Let's start, let's acknowledge, let's thank, let's KISS, and let's kiss.

I would like to warmly thank Renata Teixeira, my thesis advisor, for the guidance throughout these years. I would never had started, kept-up, or finished a PhD without her. I would not have started either without Christophe Diot pushing me a bit. I must also thank Jérôme Benoît from Grenouille who kind of put me in contact with Renata and Christophe. My advisor in Technicolor is Martin May, I must also acknowledge him. In particular Martin has wonderful soft skills such as cheering me up over a chat. I want to thank Dina Papagiannaki and Nick Feamster for accepting to be *rapporteurs* of this thesis as well as Ernst Biersack and Serge Fdida for being *examinateurs*. I already had multiple "this is a very good jury" comments and I will always be grateful to all of you when such a comment makes me proud.

I also thank all the people that I have been working with (either publishing or trying very hard to): Catherine Rosenberg, who I also *remercie* for hosting me at University of Waterloo for three months, Jim Kurose, and Christian Kreibich. I thank all my colleagues in Technicolor, at the LINCS, and at LIP6. These lists also includes the interns and the glorious PhD students from these places. I cannot list everyone so I'll name a few (i.e., people who got a desk next to mine) Diana, Oana, Nidhi, Simon, Srikanth, and Stéphane. Plus, Te-Yuan, Ahlem, Raphaël, Italo, and Giuseppe because they always were warm and friendly to me.

I am grateful to all those unnamed volunteers who ran HomeNet Profiler. And of course, as an open-source enthusiast, I also thank a whole community of hackers who built excellent software such as GNU/Linux, Ruby, R, and Git which were my day-to-day tools all these years. Finally, I also recommend three awesome groups to take a break and have good discussions here in Paris: the Ruby user group, the Haskell user group, and Copyleft attitude.

I want to keep the last paragraph for the most important persons. These are the persons who also receive *free kisses*[1]. My family: Thérèse, Dino, Thomas and François who supported me (and *me supportaient*) during these years even though I did not come back to Chambéry very often. But also my aunts, uncles and cousins, especially

[1] You can also use this page of the thesis a voucher for a free kiss

the Cardons who hosted me when I first crashed into Paris. A special kiss to my best friends from Chambéry, Laura & Julien, Mathieu, Alexis, and Manu. I needed all of you. I keep the last sentence for my beloved Bian Lu: without her smile every morning, you might never have seen me with one.

Résumé

Désormais, l'accès Internet à haut débit est largement répandu et de nombreux utilisateurs se connectent à l'Internet depuis chez eux. Les utilisateurs d'Internet résidentiel ne sont généralement pas des experts en informatique et leurs réseaux domestiques ne sont pas supervisés. En conséquence, les utilisateurs n'ont pas de moyen simple pour diagnostiquer les problèmes de performance. Quand un problème survient, les utilisateurs appellent leur fournisseur d'accès Internet pour résoudre le problème, même si le problème provient du réseau domestique de l'utilisateur. Cette situation est frustrante pour les utilisateurs d'Internet et engendrent une dépense importante pour les fournisseurs d'accès Internet qui doivent entretenir des centres d'appels.

Dans cette thèse, nous étudions des techniques permettant à un hôte Internet final (end-host) d'identifier si les problèmes de performances apparaissent dans le réseau domestique ou non. Les techniques de diagnostic réseau existantes ne sont pas immédiatement applicables aux réseaux domestiques à cause de l'hétérogénéité, aussi bien en termes matériels que logiciels, des réseaux domestiques. Malheureusement, peu de données sont disponibles à propos des réseaux domestiques et des problèmes rencontrés par leurs utilisateurs. Par exemple, nous ne savons pas quelles sont les configurations de dégradation des performances les plus fréquentes (ex., le WiFi est-il saturé dans les réseaux domestiques ?), ni quelles sont les options disponibles pour diagnostiquer les réseaux domestiques (ex., des protocoles tels que UPnP permettent-ils une collaboration suffisante entre tous les appareils de la maison) ?

Cette thèse développe des techniques permettant aux end-hosts de séparer les cas où un problème de performance apparait à l'intérieur ou à l'extérieur du réseau domestique. Nous montrons que la configuration de certains réseaux domestiques affecte la performance de bout-en-bout et que les techniques de diagnostic existantes ne peuvent pas toujours identifier si le réseau domestique est le goulot d'étranglement de performances. Afin d'obtenir une meilleure vue d'ensemble des réseaux domestiques existants, nous concevons HomeNet Profiler, un logiciel de mesure destiné à caractériser les réseaux domestiques. Trois caractéristiques importantes que HomeNet Profiler mesure sont : la liste des appareils actifs dans le réseau domestique, l'implémentation du protocole UPnP dans les passerelles Internet, et l'environnement WiFi. Avec notre jeu de données composé de près de 3000 réseaux domestiques, nous montrons que les réseaux domestiques, bien qu'ils soient souvent de petite taille peuvent avoir jusqu'à 20 appareils. Nous montrons que les requêtes UPnP, lorsqu'elles sont disponibles et précises, permettent de déterminer la capacité du lien d'accès, de détecter le cross-traffic dans le réseaux domestique, et de différencier les pertes réseaux dans le réseau domestique des pertes réseau dans le reste de l’Internet. Nous montrons également que l’environnement WiFi est généralement dense, ce qui induit un risque d’interférences. Afin d’exploiter et tirer profit de cette densité de l’environnement WiFi, nous concevons des techniques de mesures bénéficiant du voisinage WiFi. Ces techniques sont capables de mesurer avec une erreur faible et distinguer les délais et les taux de perte sur le lien montant de ceux sur le lien descendant ; ainsi que de diagnostiquer si le réseau domestique est un goulot d’étranglement ou non.

Abstract

Broadband Internet access is now widespread and many users connect to the Internet from home. Often, Internet users at home are not computer experts and their devices and networks at home are unmanaged. As a result, when a performance problem occurs, users have no simple means to diagnose the problem and may call their Internet service provider to fix the problem, even if the problem comes from the user network. This situation frustrates Internet users and incurs a large cost on the Internet service providers which must provision call centers.

In this thesis, we consider techniques for end-hosts to pinpoint whether performance problems occur in the home network or not. A reason why existing network diagnosis tools (e.g., Traceroute) are not immediately applicable for home networks is the heterogeneity of home networks in terms of hardware (e.g., number of devices) and software (e.g., operating system versions). Unfortunately, there is not much data available on home networks and the encountered problems. We do not know which the most common situations of performance degradation are (e.g., is WiFi crowded in home networks?), nor what the available options to diagnose home networks are (e.g., do protocols such as UPnP allow enough collaboration between home devices?).

This thesis develops techniques for end-hosts to disambiguate whether performance problems occur inside or outside the home. We show that some home network configurations affect the end-to-end performance and that existing techniques cannot always pinpoint whether the home network is the performance bottleneck. To get a better understanding of existing home networks at large, we design HomeNet Profiler, a software measurement tool to characterize home networks. Three important characteristics that HomeNet Profiler measures are: the list of devices active in the home network, the implementation of UPnP in residential home gateways, and the WiFi environment. With our dataset consisting of nearly 3000 homes, we show that home networks are often small but can have up to 20 devices. We demonstrate that UPnP queries, when available and accurate, can determine the ground-truth access link capacity, pinpoint cross-traffic from the home network, and differentiate local from wide-area losses. We also show that the home WiFi environment is generally dense and has an inherent risk for interference. To leverage and take advantage of this high WiFi density, we design neighbor-assisted diagnosis techniques. These techniques are able to efficiently detect and distinguish uplink and downlink delays and loss rates with small error and diagnose whether the home network is a performance bottleneck or not.

Contents

Chapter 1

Introduction

The last decade has seen a steep increase in the number of Internet connections from homes with the spread of broadband access [79]. At the same time, users now access the Internet via a large variety of devices. Often nowadays, every member of a household has her own personal computer, smartphone, or tablet. Other devices such as network equipment (e.g., WiFi access points and routers) are shared by all the members of a household. All these devices, once connected at home, constitute a *home network*. Devices from a same home network share a single Internet access. Figure 1.1 illustrates a simple home network consisting of one laptop, one desktop, a phone, and a TV. We call the devices that users interact with as *home devices*, in contrast with Internet routers and servers. Home devices connect to the Internet through a *home gateway*, which combines a modem, a router, and a WiFi access points. These three functions could reside in separate physical devices but for simplicity we will assume that the same device performs these three functions. Consumer electronics vendors now sell a variety of devices (e.g., phones, power meters, and health-tracking sensors) which rely on the home Internet access to connect to remote services. The link that connects the home gateway to the ISP network is the *access link*. Popular access links technologies are DSL and Cable. These wired technologies can provide a larger bandwidth than mobile data plans and at a lower price. In addition, while wired access technologies are dedicated to a single home, mobile capacity is shared.

When users experience poor Internet performance (e.g., slow file transfers, choppy audio conference), any of the networks in the *end-to-end* path (i.e., the path between the home device and the remote service) can be responsible. This thesis focuses on the contribution of the home network to end-to-end performance. Thus, we split end-

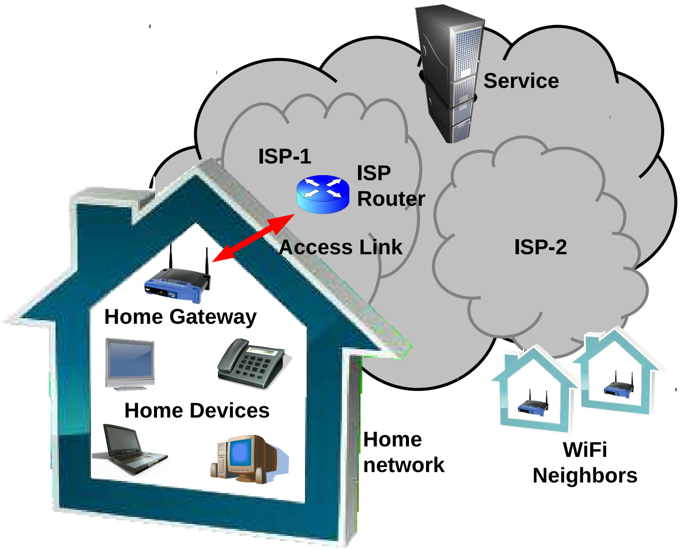


Figure 1.1: Example of home network Internet access.

to-end performance in three main components: the home network, the access link, and the rest of the Internet (including remote servers). The home network may affect end-to-end performance. Either the application or the network limits the end-to-end performance of a service. When the network limits the end-to-end performance, one or multiple links, which we call *performance bottleneck*, may limit the end-to-end performance. A reason for a link to become a performance bottleneck is congestion. For example, in Figure 1.1, a home user may start a large download on the laptop while another user is playing an online game on the desktop computer. Both applications require a large amount of bandwidth. If the access link cannot sustain streams for both applications, at least one of the two streams will suffer. In the absence of congestion, capacity determines the bottleneck. For instance, poor WiFi in the home causes losses and delays, and may also explain poor end-to-end performance [63]. While a number of studies about the performance of the access link and of the rest of the Internet exist [47, 94, 173], people are only starting to study performance of home networks and there still are little research results available on home networks.

Home users need tools to pinpoint the precise location of network performance problem. Home users are usually not networking experts and without the right set of tools they are unable to know why a given service is performing poorly. Studies show that home users often rely on simple actions such as rebooting their devices in an attempt to solve their connectivity problems [168]. If rebooting does not solve the problem, users tend to call their Internet service provider (ISP), but the ISP is not always responsible for poor end-to-end performance. Maintaining call centers and sending technicians to verify DSL or Cable lines incur a large cost to ISPs [84]. Hence, both ISPs and home users would benefit from tools that help end users diagnose their home networks, in particular tools to autoconfigure home networks and tools that can determine whether poor performance is because of problems in the home network or in the ISP network. Speed testing services such as Grenouille [71], SpeedTest [157], and Netalyzr [94] are popular among tech-savvy users. These services report path properties such as capacity, delays, or loss rates. A number of specialized command-line tools also measure the same properties [132]. However, even if these measurement services can identify performance degradation, they cannot always pinpoint whether performance degradation arises from the home network or not.

This thesis develops techniques that run on an end-host connected to a home network to pinpoint whether the home network is a performance bottleneck. We focus on techniques that run on end-hosts because it is easier for unsophisticated users to install tools on their PCs than on other home devices (e.g., home gateways). We first show with semi-controlled experiments that home networks can affect end-to-end performance. These experiments allow us to quantify the effect of different factors (e.g., when there is cross-traffic from other end-hosts or when home devices are connected in WiFi) on end-to-end performance. These experiments, however, only test a small set of home network configurations. It is hard to argue that these configurations are representative of home networks at large. In fact, there is little data about current home networks. We address this issue with HomeNet Profiler, a measurement software that retrieves home network configuration and performance. Volunteers run HomeNet Profiler on one computer in their home network. Thus, HomeNet Profiler allows us to collect the list of home devices as well as the list of services they advertise. HomeNet Profiler also measures the WiFi environment. In our results, most computers running HomeNet Profiler had a WiFi interface and the home network had a dense WiFi neighborhood. Dense WiFi neighborhoods represent an opportunity for home network diagnosis because we can connect to the same service using the home and the neighbor network. In Figure 1.1, when connected at the same time to the home network and to a neighbor network (e.g., via a guest WiFi network), a laptop can send probes to the home gateways in each network as well as send probes that cycle back through the neighbor network. These probes enable end-hosts to infer losses and delays on the parts of end-to-end paths that are close to the home network. This information allows the laptop to pinpoint whether delays and losses occur in the home network or on the access link. We design neighbor-assisted diagnosis techniques to take advantage of these alternate network paths.

The rest of this chapter provides background on the configuration of home networks, on measuring home networks, and on home network diagnosis. We then present the research contributions of this thesis and outline the rest of this thesis.

1.1 Background on home networks

As illustrated on Figure 1.1, in typical home networks, home devices often share a single Internet access through the home gateway. In France, the home gateway usually combines a DSL or Cable modem, a WiFi access point, and a router. In other countries, the home gateway is a WiFi access point and router whereas the modem is a distinct physical device. Many ISPs offer a home gateway to each of their customers. Otherwise, home users purchase a home gateway of their choice and install it at home.

The home gateway forwards Internet traffic to the ISP router via the access link. There exist a variety of access link technologies such as DSL, Cable, and fiber optics. Each technology has a different performance (e.g., transmission delay, uplink and downlink capacity) but access links are often asymmetric (i.e., the capacity is higher for download than for upload). Typical capacities that French ISPs offer are: for ADSL, 20 Mbps in download and 1 Mbps in upload, 60 Mbps/4 Mbps for Cable, and 100 Mbps/50 Mbps for fiber.

Connectivity in the home is either wired (e.g., Ethernet, MoCa, and PowerLine) or wireless (e.g., WiFi, Bluetooth). Each technology has its own characteristics: Ethernet and MoCa, which use shielded wires, provide high throughput (up to 10 Gbps for Ethernet, 200 Mbps for MoCa) and stable bandwidth but require special wiring in the home. PowerLine uses existing electricity wiring which may suffer from interference (and can offer up to 200 Mbps). WiFi is a widespread wireless technology for connecting home devices and offers rates up to 300 Mbps. One home network can use more than one technology. For example, in Figure 1.1, the desktop computer, the phone, and the TV may use Ethernet, whereas the laptop would connect in WiFi.

We call the WiFi access point (often the home gateway) for devices in the home network as *home WiFi*. The physics of WiFi propagation in the home may prevent some home devices to receive a good WiFi signal [126]. Further, WiFi does not stop at the border of the physical home, hence, home devices are generally exposed to multiple WiFi networks. A majority of these WiFi networks are home WiFis for neighbor home networks. Hence, we call these WiFi networks *neighbor WiFis*. For example, in Figure 1.1 there are two WiFi neighbors. In densely-populated areas, there may be tens of neighbor WiFis.

All WiFi clients and WiFi access points (including those from neighbor WiFis) share the air medium, either by spreading their access on frequency bands or by sharing time. Spectrum is split up into channels and a WiFi access points runs on a single channel. The home WiFi access point determines the channel for all the home devices associated to it. Hence, all home devices compete for the WiFi channel. In addition, devices and access points of neighbor WiFis also compete with the home devices if they are on the same channel as the home WiFi (or even on a channel close to the one in-use by the home WiFi). As a result, a home WiFi may have low performance in densely-populated areas with many competing WiFi networks [76].

Users subscribe to the Internet to access a number of services from home. They can access services from their ISP and more generally from the Internet. Two popular services are TV and voice over IP (VoIP). TV and VoIP are called *triple-play services* when ISPs bundle these services along with the Internet subscription. Some users also install devices to host services inside their home network (e.g., a network disk can offer a backup service and a media-server service). Installing services such as file sharing between home devices and remote control of media players requires configuration efforts. For example, computers in the home network needs to know the IP address of media servers or other services in the LAN. Protocols to autoconfigure services in home networks exist, like Universal Plug and Play (UPnP) [159] and Zeroconf (a.k.a Bonjour) [26]. Both protocols define rules to discover services via broadcast queries and rules to configure them via unicast queries. The main difference between Zeroconf and UPnP is that UPnP also specifies a set of remote-procedure call APIs. The Digital Living Network Alliance (DLNA) issues specifications, which are extensions of UPnP, for multimedia applications to discover media clips and play them on DLNA-enabled TVs. For example, the TV on Figure 1.1 may browse video clips stored on the desktop computer. Besides, UPnP and Zeroconf have different packet formats and different multicast IP addresses. In this thesis, we use UPnP and Zeroconf to discover services that users may use in their home network.

1.2 Measuring and characterizing home networks

There is a large number of techniques to measure and characterize IP networks in general. Researchers have been measuring Internet topology and performance as well as

WiFi performance. Despite the increasing interest in home networking, there is little data available on the properties of home networks (e.g., which devices and services are installed at home). Most related prior work has focused on measuring and characterizing residential access links — with active probing from servers located in the Internet [35, 47, 73, 107, 149], from clients running on end-hosts [31, 94], or on home gateways modified to support active and passive measurements [154]. Some prior studies also have deployed measurement points inside the homes of a few volunteers to record or improve the performance of home networks [50,89], to measure how WiFi propagates in homes [126], and even report on the behavior of home users when they use their home network [20, 27, 28, 168]. However, it is hard to get representative results from a few homes. Collecting measurements in home networks is challenging for a number of reasons.

Probing inside home networks from outside is hard. The lack of data on home networks is partially due to the challenges of measuring home networks at large scales. The vast majority of home networks are behind network-address translators (NATs) and firewalls, so a measurement point outside the home network normally cannot measure the characteristics of the home network itself. Hence, researchers must recruit volunteers who agree to run measurements from inside their home networks.

Volunteers are hard to recruit. The effort necessary to recruit a large number of volunteers is a hurdle in itself. Users are unwilling to commit more than a few minutes of their time to install or configure software or hardware. Similarly, only a few users would participate to a research study without strong guarantees on the privacy of the collected data [86]. Finally, a research study needs to find the right incentives to attract volunteers.

Home gateways have limited resources. When a volunteer is willing to run measurements from her home network, the particular location where to setup the measurement software or hardware is an important design choice. Measurements from inside the home can run on home gateways or on end-hosts. On one hand, home gateways are always on and they can observe all the Internet traffic of the home network [154]. On the other hand, home gateways often have limited resources [136] and there is no simple way to run arbitrary code for measurement purpose on home gateways. It is possible to provide modified home gateways but deploying hardware to a large number of users is costly. Conversely, users can install software on their own computers at no cost.

End-hosts have a limited view on the home network. End-hosts have enough resources to support a broad set of measurements. However, users may turn off end-hosts or carry them out of the home network, which prevents continuous monitoring. Further, end-hosts can only observe their contribution to the traffic flowing on the access link, which limits analyses on the data. For example, to know whether a bandwidth measurement is representative of the access link capabilities, we need to know whether other home devices introduced cross traffic.

In this thesis, we measure home networks behind NATs and firewalls in close to 3,000 homes. We reach these homes with a software that volunteers run on their end-host computer.

1.3 Diagnosing home networks

Home users diagnose network performance problems in their home network with measurement tools running on the end-host or on the home gateway. Most operating systems provide some basic network diagnostics tools. For example, *Traceroute* reports IP hops to a destination and *ping* reports whether a destination is reachable. *Iperf* measures bandwidth between hosts. There also are a number of tools, with which users can verify network stack parameters affecting network performance (e.g., the IP address of DNS servers, the MTU). In addition, some home gateways provide a web interface to perform similar diagnosis. For example, users can verify that the home gateway has an IP address, list devices connected to the home network, and even ping devices in the home network or in the Internet. These tools can help expert users infer what the problem is, but knowing the right set of tools to use and how to interpret their results is too complex for most users. A number of reasons explain why home network diagnosis is a challenging problem.

The home network affects network performance measurement tools. As we will see in Chapter 3, existing tools are not enough to pinpoint whether the home network is a performance bottleneck. For example, when a computer downloads a file, cross traffic from a second home device may reduce the file download speed. End-to-end measurement tools will observe an increased delay or a reduced bandwidth. Other reasons could lead to the same symptoms (e.g., congestion in the ISP network).

Thus, even if end-to-end measurements observe a performance degradation, there is an ambiguity on the root cause. *Traceroute*-like measurements (e.g., Tulip [106]) can identify delays and loss rates of individual network segments along an end-to-end path. These techniques however rely on ICMP messages and IP-timestamping options, which are not always supported by Internet routers [41, 140], or supported with rate-limitations [10, 91, 106]. Although Traceroute is able to identify an increased delay on the access link, Traceroute alone cannot pinpoint whether the home network is responsible for the performance hit.

There are no models of home gateways behavior. Models of home gateways behavior under cross traffic could also help in inferring the amount of cross traffic from end-to-end measurements but such models are not available.

Home networks are unmanaged. Typical home devices do not have monitoring software installed and there is no common API to query traffic statistics on home devices. Hence, a home device has no simple means to know if a second device inject cross traffic on the access link. The home gateway can observe whether there is cross traffic or not and hence can disambiguate whether the home network is the performance bottleneck or not. Unfortunately, in common deployments, users cannot query the home gateway for traffic statistics.

Access links are asymmetric. Asymmetry in residential access links makes the diagnosis of poor performance even harder. Round-trip techniques such as *ping* report a single value that couples the uplink and the downlink directions into a single delay measurement. The only method to measure each direction independently is to use servers with synchronized clocks (e.g., via a GPS signal) but such synchronization is not widely available in home devices.

In this thesis, we show how to combine UPnP queries targeted at the home gateway with end-to-end measurements to locate whether end-to-end losses occur in the home network or on the access link. We also develop techniques to distinguish uplink and downlink delays and loss rates on the access link using open neighbor WiFis.

1.4 Contributions

This thesis makes the following contributions to home network measurement, characterization, and diagnosis:

1. We show that the home network can have a significant impact on end-to-end performance with controlled experiments. For example, watching TV can double the time to download a file. We show that even a good wireless network adds variance to round-trip times. Despite its impact on end-to-end performance, most existing diagnosis tools ignore the home network when it comes to the identification of the cause of performance problems. To make matters worse, our results show that simple techniques that directly probe the home gateway cannot reliably pinpoint that the home network is the cause of performance degradation.

2. We design and evaluate HomeNet Profiler, a software measurement tool to characterize home networks. HomeNet Profiler runs on any computer connected inside a home network to collect a wide range of measurements about home networks including the set of devices, the set of services (with UPnP and Zeroconf), and the characteristics of the WiFi environment. HomeNet Profiler also embeds a user survey to collect information which we cannot measure directly. To attract a larger number of users, HomeNet Profiler runs one-shot measurements upon user demand. We evaluate this design choice against periodic measurements taken from six home networks. Our results show that a single WiFi scan is enough to observe all neighbor WiFi access points with strong signal. However, only repeated measurements of the home network can observe all the home devices. As such, HomeNet Profiler's user survey is an important complement to understand the full set of home devices.

3. We present the first large-scale study of UPnP implementation and deployment in home gateways. UPnP technology holds promise as a highly efficient way to collect and leverage measurement data and configuration settings available from UPnP-enabled home gateways in home networks. Unfortunately, UPnP proves less available and reliable than one would hope. We use data from 120,000 homes, collected with HomeNet Profiler and Netalyzr [94]. Our results show that in the majority of homes we do not observe any UPnP gateway at all. When a UPnP gateway is present, results are frequently inaccurate or simply wrong. Whenever UPnP-supplied data is accurate, however, we demonstrate that UPnP

queries can determine the ground-truth access link capacity, pinpoint cross-traffic from the home network, differentiate local from wide-area losses, and identify gateway characteristics per model.

4. With our HomeNet Profiler dataset consisting of 2,940 homes, we show that home networks are often small with between 2 and 20 devices. The broad types of devices do not vary significantly from one home to another, but the particular device model does. Diagnosis techniques for home networks will have to work on fairly diverse home network configurations.

5. With WiFi scans from 1,313 homes, we show that the home WiFi environment is generally dense. End-hosts observe up to 54 distinct WiFi networks and up to 15 on the same channel as the home WiFi. Further, in around 18% of the end-hosts running HomeNet Profiler, a neighbor WiFi has a stronger signal than the home WiFi. We also show that the high density of WiFi neighborhoods in some areas bring opportunities for diagnosis.

6. We develop methods for neighbor-assisted diagnosis to identify losses and delays. We take advantage of neighbor WiFis to diagnose performance problems. An end-host connected to the home gateway and a neighbor WiFi access point simultaneously can send out different kinds of measurement probes to infer the directional delays and loss rates on the access link. Our evaluation shows that neighbor-assisted diagnosis techniques are able to efficiently detect and distinguish uplink and downlink delays and loss rates with small error. In addition, our experiments from a real-world deployment in five homes in France show that neighbor-assisted diagnosis enables the end user and the ISP to pinpoint the location of network delays from the network's edge.

1.5 Outline of the thesis

The remainder of this thesis is organized as follows. After presenting the related work on end-to-end measurements, access links measurements, and home networks in Chapter 2, we study the effect of the home network on end-to-end performance in Chapter 3. Chapter 4 then designs and evaluates HomeNet Profiler, our tool to measure home networks at large scale. Chapter 5 describes the HomeNet Profiler dataset, as well as our heuristic to select one representative measurement per home network. Chapter 6 presents our characterization of three aspects of home networks: the implementation of UPnP in home gateways, the set of devices and services in home networks, and the WiFi environment of home networks. Our characterization shows that neighbor WiFis bring an opportunity for identifying whether or not the home network is a performance bottleneck. Chapter 7 introduces the neighbor-assisted diagnosis technique to identify network segments with high losses and high delays. Finally, Chapter 8 concludes the thesis and discusses future work.

Chapter 2

Related Work

This chapter presents the work on measurements, characterization, and diagnosis of IP networks. We first present work related to end-to-end Internet paths, we then narrow down to broadband access, and finally, home networking.

2.1 End-to-End Internet paths

End-to-end network performance determines the performance of networked applications. Hence, there has been significant effort on understanding end-to-end network performance. In this thesis, we apply to home networks some of the techniques created for end-to-end paths. We focus in this section on metrics and tools to measure individual end-to-end Internet paths; we then present the efforts to characterize Internet paths at large, as well as general network performance diagnosis techniques.

2.1.1 Metrics and tools

There has been significant work on designing and evaluating end-to-end tools to measure different properties of end-to-end paths: delays [16,33], capacity [25,55,133,143], bandwidth [69, 132, 148], loss rates [11, 144, 150, 151, 162], as well as the topology of Internet paths [9, 53, 54, 77, 78, 103]. These tools are based on active measurements, i.e., they send packet probes and interpret the results to infer a metric or a topology. The IP Performance Metrics working group at IETF [127] specifies a number of performance metrics. For example, the one-way delay is the time a packet takes to go from a source to a target destination. To measure one-way delay, the target destination must report to the source and both hosts must maintain synchronized clocks. This level of cooperation between hosts is generally not available for arbitrary pairs of Internet hosts. Instead, a source can measure the *round-trip time* (RTT) to a destination. The RTT is the total time for a packet sent by a source to reach a destination plus the time for an answer packet to reach the requester. Mechanisms built into the ICMP specification [131] enable Internet hosts to measure RTTs. The same standard also allows the measurement of Internet topology and per-hop delays using probes with a limited time-to-live field. Congestion, routing errors, or rate limitations of measurement probes in the Internet may prevent measurement probes from reaching their destination. Monitoring lost probes provide estimation of loss rates. Lost probes also motivate the need for probe re-transmission to differentiate transient losses from permanent failures [39]. Capacity and bandwidth measurement have more overhead than delay measurements because they need to measure the time dispersion of packet flows or packet trains [72, 132]. Passive measurements, i.e., measurements that only observe traffic without injecting any probe can also measure performance metrics [64, 81] as well as the topology [58] of Internet paths.

This thesis uses existing measurement techniques to measure end-to-end metrics rather than developing end-to-end measurement methods. Chapter 3 evaluates the impact of the home network on the end-to-end RTT using ping [119] and on the end-to-end bandwidth using Iperf [72] as well as the impact of the home network on the results of Traceroute [109], NDT [22], and Netalyzr [94]. In Chapter 7, we perform one-way delay and loss measurements using accurate sampling techniques from Baccelli et al. [11]

2.1.2 Characterization

There is a large body of work which used end-to-end measurement tools to characterize end-to-end paths and to build a better understanding of the Internet at large. A number of studies characterize Internet topology using Traceroute [10, 40, 120, 146]. Another active research topic is the characterization of the performance of end-to-end paths [30, 31, 104, 105]. None of these studies has characterized home networks, which is the focus of this thesis. However there are studies that have placed measurement vantage points in end-users' machines to characterize end-to-end Internet paths.

Any characterization effort running on end-users' machines faces the same issue we face with HomeNet Profiler to recruit volunteers. Characterization efforts such as Ono [30], Netalyzr [94], HomeLab [17], SatelliteLab [46], and Dimes [146] all recruit volunteers but their incentive mechanisms, when they have one, are different.

Ono holds the promise of improved Bittorrent download speeds, Netalyzr let users debug their Internet connection, and Dimes offer virtual credit to reward large contributors. Our home network characterization tool, HomeNet Profiler, provides an incentive mechanism similar to Netalyzr: once HomeNet Profiler finished running on the user machine, it opens a a report on the home network with hints on how to improve the user's network (e.g., HomeNet Profiler proposes to switch the home WiFi to the least crowded WiFi channel).

2.1.3 Diagnosis

There is a collection of tools to diagnose end-to-end Internet paths. Traceroute [109] probes network segments hop-by-hop and hence can locate where packets stop. Improvements to the original Traceroute use different types of probing packets [103], explore IP options [140] to detect delays and reordering [106], or avoid measurement artifacts from load balancers [9], MPLS tunnels [54] or path asymmetry [90]. Another technique is network tomography. Network tomography aggregates measurements of end-to-end paths (possibly originating from multiple hosts) to infer properties of network links [19,23,39,44,66–68,161]. Chapter 7 takes a network tomography approach, but applies it from a single end-host.

A number of traffic engineering practices from the ISP may appear as a performance problem to users. For example, ISPs used to throttle peer-to-peer traffic [14]. There has been work to build tools for diagnosing peer-to-peer disconnections [48] or traffic differentiation [87,156,163]. These practices only affect certain types of applications and hence are not the focus of this thesis.

None of the previous techniques can pinpoint that the home network is the performance bottleneck. As we see in Chapter 3, Traceroute could in theory attribute the problem to the access link hop but Traceroute cannot pinpoint whether the delay comes from another host in the home network or not. This thesis develops techniques to pinpoint whether the home network is a performance bottleneck. We show how end-hosts can detect the presence of cross traffic on the access link with UPnP queries. When connected at the same time to the home network (on Ethernet) and to a neighbor network (via WiFi), we show how to independently measure uplink and downlink loss rates and delays on the access link.

2.2 Broadband access links

Access link can limit the Internet performance of end-hosts in home networks. There has been a recent interest in studying broadband access performance. Prior work provide improvements or new tools for measuring access link asymmetry, for characterizing residential broadband performance and for access link diagnosis.

2.2.1 Metrics and tools

Many parties are interested in monitoring broadband access performance. ISPs have to monitor the performance of their network on a regular basis. Content providers measure the broadband performance of their users (for example, to adapt the content to the client's bandwidth). Finally, users are often curious about the performance of their Internet access.

Residential ISPs maintain their network and hence monitor access links of their broadband customers. When the ISP provides home gateways to their customers, it can use protocols (such as TR-069 [56]) to perform active measurements from home gateways. For example, ISPs monitor round-trip delays and bandwidth between home gateways and landmark servers. SNMP [80] also allows to collect passively-measured traffic statistics on network equipment. Besides, researchers have been studying the network performance of residential ISP customers with traffic traces collected on access links [29, 107, 129]. However, these techniques require privileged access to ISP equipment, which prevents us from using these techniques for our thesis.

Content providers often measure the performance of their users. For example, when users browse websites [6, 121] or when they stream videos [95]. Further, content providers sometimes report these values to their users [172]. Besides, a number of initiatives provide tools to measure access-link capacity from remote servers towards un-cooperating home gateways while taking the asymmetry of access links into account [24, 35, 36]. These tools are not strongly related to this thesis because we focus on tools for home users.

Many users want to test whether their ISP delivers the level of performance they have paid for. A number of online services propose users to test their access link performance (mainly bandwidth and latency) with active probing running on a end-host in the home network [21, 22, 71, 94, 113, 157]. This approach is easier for users but suffers from a number of caveats. For example, powerboost [12, 154], a system to speed up short-duration flows, may bias the estimation of access links capacity if measured with short flows. Also, the maximum packet-forwarding rate of home gateways may bias available bandwidth measurements [69,75]. Chapter 3 shows examples of situations where access link-measurement tools cannot distinguish if the problem is in the home or in the access network. Hence, speed-testing websites may wrongly attribute to the access link poor performance coming from the home network. To address this problem, Chapter 6 shows how to complement access link measurements with a UPnP query to the home gateway. With this improvement, it is possible to retrieve the ground truth upload and download capacity of the access link and detect the presence of cross traffic on the access link. This thesis also provides techniques to measure the asymmetric delays and loss rates on the access link. Home gateways sit between the ISP network and the home network. Thus, home gateway-based measurement alleviates the problem we study in this thesis. Expert users can install open alternative WiFi access point firmware (OpenWRT [43] and Tomato [130]) to get more control on their home gateway. Researchers deployed modified home gateways to measure access link properties without the bias of home network performance [93,153,154]. This techniques are promising but require modifications or even the replacement of existing home gateways. Hence, are not suitable for a short-term and worldwide deployment. Conversely, Dasu [142] recently integrated our work on UPnP to complement their bandwidth measurements on 13,000 hosts in more than 100 countries [141] and Fathom [45], which provides JavaScript APIs to run active and passive measurements from web browsers, also integrated a UPnP module.

2.2.2 Characterization

Monitoring broadband access performance at large scale brings valuable information to design and improve services for residential Internet users. There have been a fair number of studies on characterizing residential broadband access. Content-providers now rank ISPs [158] and rank the access speed of countries [2] using traces from video streams and from large file transfers. Previous studies observed access performance from end-hosts or home gateways in home networks [21,94,154] or from remote servers [47]. These studies compared the performance of DSL vs Cable networks and observed diurnal patterns of network performance. ISPs also monitor access links to study traffic growth of residential users [29,129]. Meanwhile, ISP customers gather measurements to expose the actual performance of ISPs [71], which is useful when selecting an ISP subscription.

This thesis complements these broadband characterization efforts by showing the importance of taking the home network into account. In particular, cross-traffic from the home network or WiFi at home may affect access link measurements. Our results in Chapter 6 show that characterization efforts that take an end-host based approach should query UPnP to remove some measurement errors coming from cross traffic in the access link as well as get ground truth on the access link capacity (Chapter 6.1).

2.2.3 Diagnosis

Diagnosing access links is important for ISPs and, to some extent, end-users. On one hand discovering that the access link is faulty is relevant for home users. On the other hand, only ISPs have a fine control on access link parameters. Thus, ISPs research methods to detect and even predict problems occurring on the access link [84, 111]. These techniques involve monitoring of access link physical parameters such as noise level of DSL lines. This topic is not strongly related to this thesis although neighbor-assisted diagnosis (Chapter 7) and other tomography techniques discussed earlier could pinpoint if a problem is shared by multiple neighbor in the same area.

2.3 Home Network

We group research conducted in the area of home networks into six broad categories: measurement techniques and services specific to home networks, efforts to characterize home networks, diagnosis systems for home networks, WiFi in home networks, user-friendly interface for home users, and finally we present propositions of new home network services. This thesis focuses on measuring and diagnosing home networks, hence we will discuss the three first categories in more details.

2.3.1 Measurement techniques

There is a growing interest in understanding home networks as they are expected to grow in complexity [57]. A number of properties capture the complexity and the heterogeneity of home networks: the set of devices and services running in home networks, the topology of the home network, and the traffic patterns between active home devices.

Two simple properties to measure inside home networks are the set of home devices as well as the set of services they offer. Network scanners (e.g., *nmap* [122] on computers or *Fing* [124] on smartphones) are a mean to detect active devices. Nmap also fingerprints each home device to identify the operating system. In Chapter 4, we implement a scan to measure active devices in home networks. Unlike nmap, our device scan does not fingerprints OSes but is simpler to embed in HomeNet Profiler. Although knowing the operating system of all home devices is valuable information, fingerprinting all home devices may take time and raise alarms on firewalls. Thus, we do not include nmap in HomeNet Profiler. We instead use the OUI field of the MAC address, which informs us about the device manufacturer. In addition, nmap enumerates open TCP and UDP ports, which informs on the services running on scanned hosts. This service discovery procedure is intrusive and time consuming. Hence, industry groups have proposed protocols to announce services in home networks (UPnP [159], Zeroconf [26], and DPWS [123]). While conceived and used for autoconfiguring devices and services, we measure the set of services in home networks using UPnP and Zeroconf. We also test the support for UPnP in home gateways of hundreds of homes. Our data show that support for UPnP and Zeroconf autoconfiguration protocols is limited in today's home networks. We do not measure DPWS services. Since DPWS is more recent, we suspect that its penetration is even lower. However, this situation may change in the future.

There is only few data available on the topology of home networks. LLDP [102] specifies mechanisms for hosts to discover and interact with network equipment (e.g., to discover VLANs). To the best of our knowledge, support for LLDP is not common in home devices. More specific to home networks, LLTD [116] provides link-layer facilities to perform active probing between home devices under the assumption that all devices speak a same protocol. HomeMaestro [89] provides a distributed system to coordinate home devices and automatically diagnose performance and configuration problems. Deploying such systems is however not practical in the short term because LLTD and HomeMaestro are not yet widely available and legacy devices will not receive updates. In this thesis, we measure existing home networks thus we cannot use these protocols.

In addition to the presence of devices and services in home networks, passive measurements also inform on their usage. Only a few studies measure the network flows of individual home devices [20, 92, 137]. Collecting such information requires users to install always-running daemon on end-hosts or home gateways as well as require root privileges. Our decision was to make HomeNet Profiler easy and fast to run so that we attract a large number volunteers and hence we cannot measure network flows.

2.3.2 Characterization

There are a few prior studies characterizing the set of devices and services in home networks. On one hand, prior work that focused on end-to-end performance or on user experience have peeked into home networks and provide valuable information on home networks. On the other hand, ISPs carried passive measurements on access networks but could not run measurements from inside home networks.

Some studies provide valuable information on home networks even if characterizing home networks was not their first intent. *How's my Network* [139] is a Java applet that collects a variety of performance and configuration metrics on end-hosts. HomeNet Profiler uses technologies similar to *How's my network* (both tools are Java applications). However, the study using How's my Network focused on end-to-end upload and download throughput and the response time of DNS servers. The home with the largest number of devices had nine devices active but their dataset only has 36 homes. In contrast, we observed up to 18 home devices in our dataset of more than 2,500 homes while users report up to 20 devices. A study of traces collected with the HostView tool [85, 86] on end-hosts in 47 homes showed that for a majority of users, the volume of Internet traffic dominates the volume of LAN traffic and that LAN traffic mainly carries DNS and networked file systems [137]. This result is consistent with our finding that the most prevalent service announced via Zeroconf and the second most prevalent service on UPnP are media sharing services. HomeNet Profiler only performs one-shot measurements but we also study how one-shot measurements compare with repeated measurements in six homes in Paris. HomeNet Profiler performs an ARP scan to discover devices and search for Zeroconf and UPnP services. These devices and services may not otherwise appear in passively-collected traces. However, we do not know how often home users actually use services in their home network.

Existing work focused on characterizing home networks studied home networks from outside. The analysis of one access network showed that in 70% of homes, fewer than two devices are active at a same time [107, 108]. This result is in agreement with our observations from repeated measurements in six homes in Paris and from HomeNet Profiler data. A study of the HTTP traffic of home networks finds that 5% of the volume of HTTP traffic comes from smartphones [59]. HomeNet Profiler's survey results show that smartphones are popular in home networks however we do not have traffic traces showing bandwidth usage to confirm the value found in this study. Since HomeNet Profiler runs inside the home network, HomeNet Profiler may observe devices which do not use the Internet connection, such as network printers. Another advantage of measuring from inside the home network is that MAC addresses contain an identifier of device maker.

All these prior studies use results from a few homes and none covers all the aspects and the diversity of homes that HomeNet Profiler measures. HomeNet Profiler also collects other properties of home networks such as the demographics of the household (Chapter 4); and reaches close to 3,000 homes in more than 60 countries (Chapter 5).

2.3.3 Diagnosis

A few previous studies tackled the problem of diagnosing configuration or web sessions problems from clients running in home networks. A challenge to diagnose home networks is the heterogeneity of devices as their support for existing protocols varies from one device to another. Researchers also recognize that the lack of continuous monitoring inside home networks is a reason why diagnosis in home networks is hard [20]. This problem spun interest on methods to combine measurements from an heterogeneous set of devices.

While our work focuses on diagnosing network performance degradation, existing work mainly diagnosed configuration or application-specific problems. NetPrints [1] aggregated device configurations from many home networks and correlated misconfigurations in homes with similar network devices. NetPrints used UPnP to get the identifier of home gateways. Our results show that UPnP is available in less than half of the homes and that the implementations often have many issues. NetPrints would benefit from further identification of home gateways (e.g., with the vendor name from the MAC address), which provide identifiers when UPnP is unavailable or inaccurate.

Previous work showed that it is possible to troubleshoot web sessions by aggregating and correlating passive measurements of users located in multiple homes [37,38]. We think that neighbor-assisted diagnosis is a good complement to correlation-based diagnosis. For example, the comparison of active measurement following distinct network paths helps in locating network failures.

Argumentation trees, an artificial intelligence technique, can also provide a framework for machines to *reason* about network performance [52]. This framework standardizes a way to combine measurement of different nature such as performance metrics and configuration information while being agnostic to the particular implementation of a given measurement. The techniques we develop to identify whether the home network or the access link are the performance bottleneck (either via UPnP or via neighbor-assisted diagnosis) are likely to improve the result of this framework.

2.3.4 WiFi

WiFi is prevalent in many home networks, some models of electronic tablets can only setup IP connectivity using WiFi. WiFi can be a performance bottleneck in home networks and there is a vast literature on WiFi. We focus our discussion on prior work on measuring and improving WiFi; characterizing WiFi deployments; diagnosing WiFi problems, which is most relevant to our goal of identifying when WiFi is the performance bottleneck. We then present work that leverage WiFi neighbors to provide new Internet services.

A number of studies measure WiFi performance or propose improvements to the 802.11 standards. An example of performance limitations of WiFi is the 802.11b anomaly [76], which explains why a single device with poor performance affects all WiFi terminals in an area. To solve WiFi performance limitations, prior work studied different schemes to increase the fairness between terminals [7, 32, 100, 128, 135] or to use existing spectrum more efficiently [51, 96, 117, 166, 174]. Rather than changing WiFi, a study also evaluated whether 60 GHz frequencies are suitable for indoor communications [5]. Meanwhile, the FCC recently argued in favor of releasing more unlicensed spectrum for WiFi [62]. Improving WiFi performance is not the goal of this thesis. Instead, we characterize the home WiFi environment with HomeNet Profiler.

Characterization of WiFi deployments has been a research topic. Prior work characterizes WiFi density in urban areas from war-driving traces [3] and software running on mobile devices [98, 165]. In this thesis, we measure the home WiFi environment from home users' computer. Inside homes, a study of device-to-device WiFi communications in three homes showed that the position of devices heavily influence the quality of WiFi links [126]. This result is in agreement with our finding that in 8% of homes in France, a second WiFi neighbor has a higher RSSI than the home WiFi. Both results indicate that the link between the WiFi access point and the end-host has poor performance. To the best of our knowledge, our characterization of the home WiFi environment as well as our evaluation of WiFi communities in France are novel.

Diagnosing WiFi problems in home networks is challenging, in part because of the lack of instrumentation providing WiFi and spectrum usage at fine granularity. There exist spectrum analyzers such as the Wi-Spy [115] that allows to finely measure the spectrum usage, however these devices are mainly meant for computer experts. Hence, researchers studied how common end-hosts could detect WiFi performance problems using commodity hardware [88, 97, 145]. Despite their promising results, these methods require specific models of WiFi adapters as well as modified drivers.

Thus, we cannot incorporate these techniques in HomeNet Profiler, which volunteers run on their own computers.

Prior work leveraged dense WiFi environments, either to save energy by turning off unused home gateways during the night or to improve the performance of network applications [70, 74, 82, 125, 134, 169]. Studies debate whether or not WiFi is a good candidate for offloading cellular networks [8, 13, 99, 101, 152]. All these applications will likely have a high overhead in terms of WiFi usage. In this thesis we use neighbor WiFis for diagnosing delays and losses on the home access link. Our diagnosis techniques only require to send a small number of small packets, hence our techniques have a low overhead. It is not always possible to use neighbor WiFis because of password but there are cases where users can get the credentials to connect. Our evaluation of neighbor-assisted diagnosis in Chapter 7 relies on WiFi communities. In WiFi communities, users open their WiFi access points to members of a same community. Researchers study the economical incentives to open WiFi to members of a community [110]. We hope that neighbor-assisted network diagnosis will be an additional incentive to increase the adoption of WiFi communities.

2.3.5 User-friendly interface

Home users are not networking experts and often get lost in managing and troubleshooting their home networks. Nowadays, users address their network problem at home by rebooting their computers or asking their friends [57, 168]. There is a fair amount of work in the human-computer interaction (HCI) community to help users control all devices in their home network [112, 118, 170]. Researchers also study the impact of exposing home network traffic usage on the social interactions within a household [18, 27, 28]. Inspired by HCI techniques, we include a user survey and a user report in HomeNet Profiler (Chapter 4).

2.3.6 New services

Given the spread of home networks, researchers and industry also propose new services or new architectures for home networks. For example, an IETF group proposes extensions to existing protocols for autoconfiguring home devices using IPv6 [155]. Besides, HomeOS [49,50] is a potential platform for building new services. The HomeOS architecture schedules and authorizes the use of home equipment (e.g., video cameras and light switches) from home devices. A study showed how to reach a similar goal with a distributed file-system [42]. Finally, virtualized home gateways [164] and software-defined networking [61, 171] are flexible approaches to incorporate new services such as security management inside home networks.

2.4 Summary

Home networks are a growing area of research spanning many topics from network performance to wireless and HCI. In this thesis, we improve on the state of the art in a number of directions. With HomeNet Profiler, we characterize close to 3,000 home networks from the inside. HomeNet Profiler measures the set of devices and services active in the home network. HomeNet Profiler also takes the user perspective into consideration so that we can have demographics on the household and be aware of devices turned off when HomeNet Profiler runs. In addition, we characterize the WiFi environment from where users actually use their computers since a user has to be present to run HomeNet Profiler. We design two sets of techniques to pinpoint when the home network or the access link is the performance bottleneck. Our first approach is to leverage UPnP in home gateways while our second approach takes advantage of dense WiFi neighborhoods common in residential areas.

The next chapter shows that the home network has an impact on end-to-end performance and that existing measurement tools cannot always attribute the performance bottleneck to the home network.

Chapter 3

Impact of the Home Network on End-to-End Performance

This chapter studies the effect of the home network on the end-to-end performance as seen by end-hosts. Internet performance may be degraded by competing traffic or bad WiFi reception in the home network. For example, triple play services (i.e., VoIP and IPTV bundled with the Internet access subscription) may compete with a video game session on a desktop computer. Due to the limited available bandwidth, at least one connection will suffer when the application bandwidth exceeds the available resources. Although there is an increasing interest in understanding residential Internet access performance [35,47,71,73,107,149,154], previous work focuses mainly on measuring and characterizing access networks (i.e., the network connecting the home gateway to the ISP router), but not the home network itself.

The study of home network performance is challenging. There are hundreds of millions of homes connected to the Internet with a large variety of network configurations and services. Thus, running controlled experiments to quantify the effect of the home network on end-to-end performance in a representative set of homes is practically infeasible. Even if we place monitoring software inside many homes (for instance, as in the Grenouille project [71] or SamKnows [93]), we cannot have full control of all devices in the home network to understand the contribution of each home device and of the quality of the home network itself to Internet performance. Further, triple-play services may require home users to use the ISP-provided home gateway, on which we cannot install monitoring software. Another option is to use analytical or simulation models of home gateways to understand how different devices and services in the home compete for bandwidth. However, packet scheduling in the home gateway depends on vendor-specific implementations that are not publicly available.

In light of these issues, this chapter uses a controlled testbed to emulate a home network connected to a DSL provider with triple-play service. This testbed (described in Section 3.1) allows us to study independently the effect of TV, phone, competing data downloads and uploads as well as the WiFi on end-to-end performance. Our main findings are:

1. We show that a home network can sometimes significantly affect end-to-end performance (Section 3.2). For example, when a user in the home is uploading a file, the RTTs of other users in the same home can increase by as much as one second and HTTP download rates reduce by half.
2. Identifying that the home network is the cause of performance degradation is not trivial (Section 3.3). Existing diagnosis tools as well as simply probing the home home gateway are not sufficient.

Section 3.4 discusses our findings and highlights the need for large-scale measurements of home networks. In particular, we need to test UPnP implementations in deployed home gateways as well as test their network buffer size. We next present our methodology and experimental setup.

3.1 Experiment description

We study the effect of the home network on end-to-end performance using controlled experiments. The complexity of the triple-play service architecture prevents us from using a completely local testbed environment. Hence, our study uses a combination of a controlled testbed to emulate a home network, a controlled distant server, and a commercial access network, which provides triple-play services. This section presents our test cases, then it describes our testbed and the metrics we use to capture end-to-end performance as seen by an end-host.

3.1.1 Test cases

We independently study the most common home services: voice, TV, data upload, and download. We test how five usage scenarios affect end-to-end performance as seen by a *probing computer*.

- *Idle* is when no other computer or application in the home uses the network. We expect to reach the best end-to-end performance in this scenario. As such, it serves as reference.

- *Phone* is when a home user performs a phone call over the Internet. During the phone call, we play music to ensure that no silence detection stops the data stream. Although realistic phone call would have alternating silence periods, here we study a worst case in terms of bandwidth usage.

- *TV* represents the scenario where a set-top-box streams a HD live video from the ISP.

- *DL* captures the case when a *competing computer* in the home downloads a file. We emulate the download with the netcat command to a remote server. We verify that changing the server location does not change the results as long as the server has good connectivity. All the computers use the same medium to connect to the home gateway.

- *UL* is like DL, but the competing computer uploads a file instead.

We emulate two common home environments:

- *Ethernet environment:* we connect the computers to the home gateway with full duplex 100 Mb Ethernet.

- *WiFi environment:* we connect the computers to the home gateway with 56 Mbps 802.11g. Prior work [126] shows that the WiFi in the home is inherently complex. Our goal is not to study extensively WiFi performance in home networks but to study whether even a good WiFi (i.e., when computers are close the access point) can already disrupt end-to-end performance.

These scenarios and environments allow us to study ten configurations independently. We next describe our testbed.

3.1.2 Testbed

Figure 3.1 presents our testbed. Our testbed has an emulated home and a controlled server connected via a commercial ADSL service. The *emulated home*, located at Technicolor in Paris, consists of a commercial home gateway (which is both a modem and a router), a phone, a TV, and two computers. The home gateway is connected to the Internet using an ADSL2+ line from France Telecom. According to its web interface,

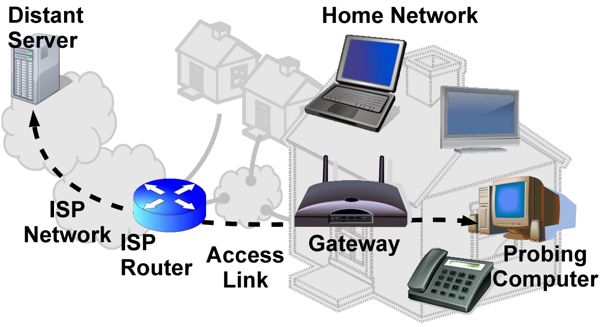


Figure 3.1: Measurement Testbed

the home gateway is synchronized at 7,650 kbps downstream and 620 kbps upstream at the time of the experiments. The first IP hop after the home gateway is the ISP router. The home gateway has two Ethernet 100 Mbps ports and an RJ11 port to plug a phone. A separate device, the set-top-box, is in charge of subscribing to and decoding television streams (hence Figure 3.1 represents the set-top-box with a TV screen). The set-top-box is connected to one of the Ethernet ports. We perform all the measurements from a commodity business computer connected to the Internet via the home gateway. We call this computer the *probing computer*. It has a dual core CPU at 1.80 GHz, 2 GB of RAM and runs Linux 2.6.32. For WiFi experiments, we use an external PCMCIA Atheros card with the ath4k driver. For UL and DL scenarios, we use a second computer. The controlled *distant server*, located at LIP6 in Paris, is the end point of our end-to-end measurements. The path between the distant server and the emulated home is 20 hops long and stable throughout the experiments. It leaves France Telecom's network and enter Cable&Wireless in Madrid, then it returns to Paris through Renater.

3.1.3 End-to-End performance metrics

We study two main metrics of end-to-end performance: the Round-Trip-Time (RTT) and the HTTP download speed. RTT captures the effect of the home on delay sensitive applications, whereas HTTP downloads represent bandwidth intensive applications. We also study jitter with the variability of RTT with the variation coefficient of the RTTs during an experiment.

We measure RTTs to the distant server with the *ping* command-line tool. We wait 500 milliseconds before each ping request. We obtain distributions from 100 pings of size 64 bytes. Our experiments with larger pings are similar. We observe no dropped packets during the whole RTT measurements.

For HTTP downloads, we use the *wget* command-line tool to download a file of 24 MB with a single TCP connection. The file contains random bits to prevent transport compression from biasing our results. We verify that the distant server actually uploads the file (i.e., no cache in the ISP network serves the file). We use large files when measuring the bandwidth to minimize the effect of TCP slow start. As a result, each measurement takes time, so we only do 20 repetitions.

When performing a measurement run, we first pick a metric and do all the experiments as close as possible in time for the different scenarios. Then, we test all cases for the next metric. Performing measurements of a metric back-to-back ensures that the conditions of the ISP network are similar, and most of the differences we observe come from the emulated home. A run for RTT measurements takes around twenty minutes, whereas it takes two and a half hours for HTTP downloads.

3.2 End-to-End performance

It is expected that the home network can impact end-to-end performance. This section quantifies this impact for RTTs and HTTP downloads under the scenarios described in Section 3.1.1.

3.2.1 Round-trip time

Figure 3.2 presents the cumulative distributions of RTTs from the probing computer to the distant server in six configurations (we omit the other WiFi scenarios because the conclusions are similar to their Ethernet counterparts). The RTTs range from 60 ms to more than 1 s, which shows that end-to-end performance of a computer in a home depends strongly on home usage. In the Ethernet/Idle scenario, all RTTs are close to the minimal value and the variation of coefficient is lower than 2%. The highest impact on end-to-end performance comes from a competing computer in the home. The RTT can reach 120 ms (and the coefficient of variation 18%) when a competing computer does a download. This impact is even higher for uploads, RTTs are never lower than 180 ms and even larger than 1 second 60% of the cases (the coefficient of variation reaches 30%). This effect is probably the consequence of "bufferbloat" in the network path [65], most likely, in the home gateway. Section 6.1.4 confirms that buffer-size strongly correlates with home gateway models. Uploads have a larger impact than downloads because of the high asymmetry of the ADSL line with a much

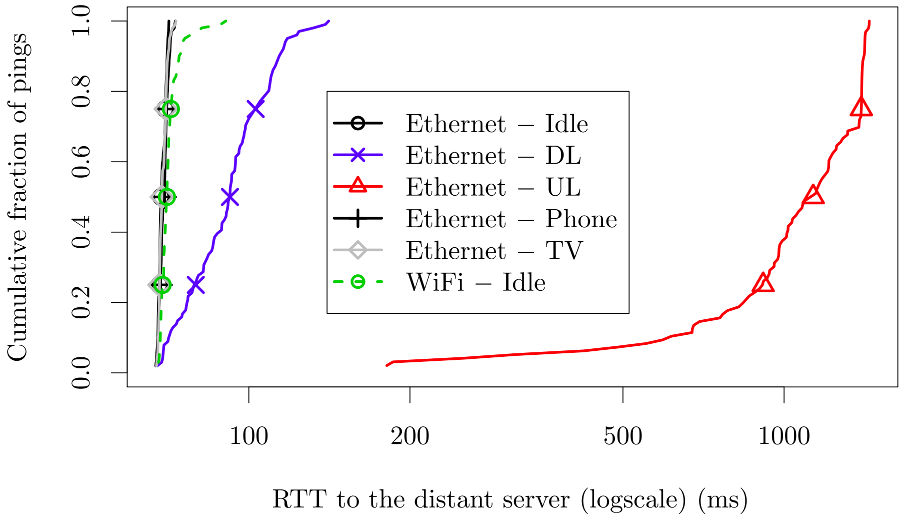


Figure 3.2: CDF of RTT to a distant server

lower uplink rate. Hence, with a fixed buffer of the same size in both direction, the draining rate is much lower and the delay becomes excessive. If we assume that the upstream capacity is in the range of the DSL synchronization rate (650 kbps), then the buffer size is around 100KB. TV and phone have a less significant effect on RTT and add no significant jitter (below one percentile point). A possible explanation for the lower importance of TV and phone on RTT is that these two services operate at a constant bitrate, without filling network buffers. These services only slightly affect the variance and do not affect the range of RTTs.

The other noticeable difference is between WiFi and Ethernet. For Ethernet/Idle, RTTs are always close to 60 ms. The effect of WiFi is unclear due to scaling effects. Hence we separately plot the WiFi/Idle and Ethernet/Idle curves in Figure 3.3. For WiFi/Idle, RTTs have more variance (the coefficient of variation of RTTs grows to 5%) and can reach larger values (up to 90 ms). Around 20% of the points have larger RTT than the maximum RTT in the Ethernet/Idle scenario. Remember that the probing computer and the home gateway are close to each other in our controlled experiments. Thus, in a real-world setup, WiFi probably introduces even more variance than our WiFi/Idle scenario.

As a result, a user with WiFi or competing flows at home may suffer long delays

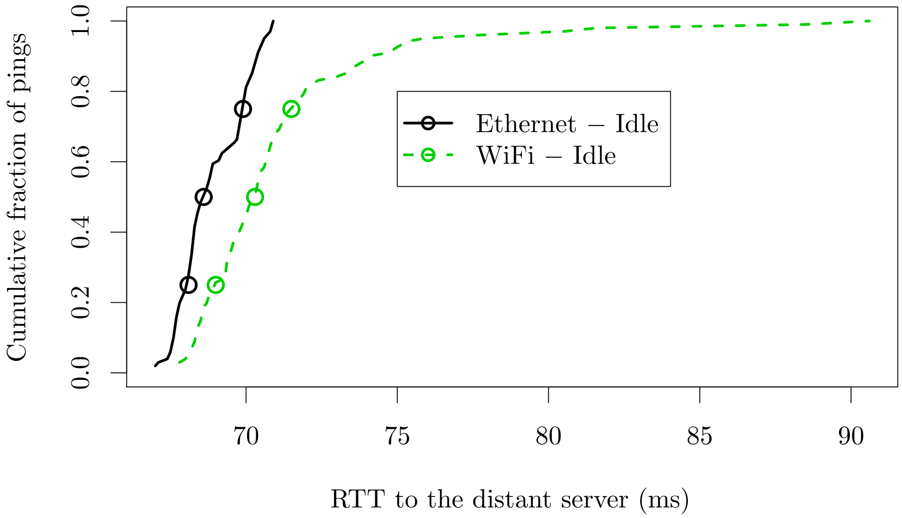


Figure 3.3: CDF of RTT to a distant server (effect of a good WiFi)

and jitter, in particular, in presence of bufferbloat in the home gateway. Applications like online games or voice may severely suffer from competing end hosts in the home network. Hence, operating systems and users need tools to detect whether such adverse situations occur.

3.2.2 HTTP downloads

Figure 3.4 shows the distribution of HTTP download rates from the distant server for several configurations (we omit the results for the phone, because it has practically no effect on HTTP downloads). The highest achievable download rate of all scenarios is 6,200 kbps, which is 10% lower than the rate that the home gateway advertises. This 10% difference is because the home gateway shows a link-layer rate, which includes the encapsulation overhead. These rates also indicate that, in the Ethernet/Idle case, the bottleneck is the access link. This observation confirms the findings of Dischinger et al. [47].

TV and competing downloads or uploads have a large effect on the HTTP download rates. Presence of TV limits the end-to-end bandwidth to 3,200 kbps, which doubles the file transfer time. This particular value reflects how France Telecom implements the service: when TV is turned on, it reserves the bandwidth. This degradation

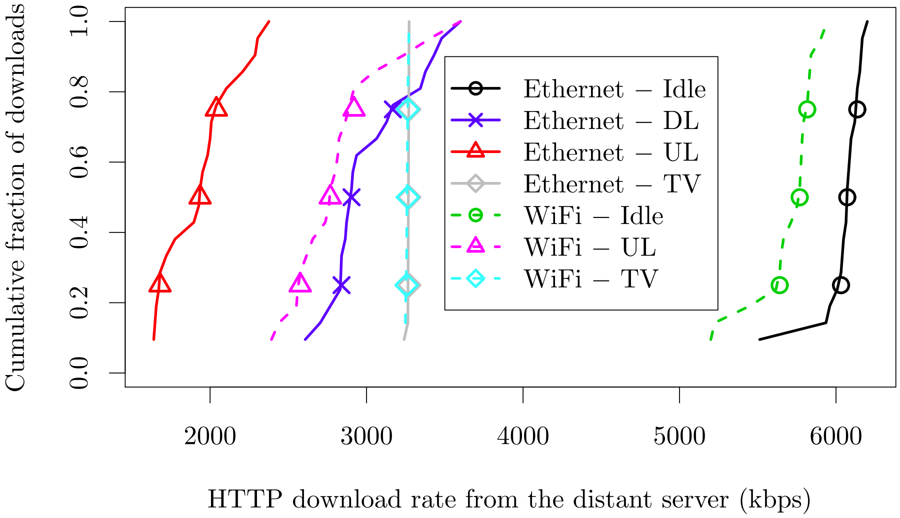


Figure 3.4: CDF of end-to-end HTTP download rates

is the same in WiFi and Ethernet (the two lines fall exactly on top of each other). Similarly to the results for RTTs, uploads from another computer in the home present the highest impact on HTTP downloads (rates are as low as 1,500 kbps). The impact of downloads is similar to that of TV but with a higher variance. Interestingly, the upload scenario has higher HTTP upload rates in WiFi than in Ethernet. We conjecture that the contention in WiFi prevents congestion on the access link. WiFi alone can reduce the bandwidth by up to 500 kbps.

In summary, our controlled experiments show that the home network can have a significant effect on end-to-end performance. Competing computers in the home are the most important source of degradation. WiFi also affects RTTs and the TV has a large impact for HTTP downloads.

3.3 Identification

This section shows that existing diagnosis tools cannot reliably identify that the home is the cause of performance degradation. Then, it shows that simply probing the home gateway does not help.

Scenario	TTL	RTT (ms)		
Ethernet				
Idle	1 (Gateway)	0.541	0.365	0.331
	2 (ISP Router)	40.1	40.2	39.4
UL	1 (Gateway)	0.498	0.577	0.349
	2 (ISP Router)	398	483	527
WiFi				
Idle	1 (Gateway)	1.78	1.12	3.48
	2 (ISP Router)	76.4	44.7	44.1

Table 3.1: Example of Traceroute output

3.3.1 Existing tools

There are many network diagnosis tools. We take two tools as example: Traceroute, which is often the first step in network diagnosis, and Netalyzr [94], which combines a number of advanced tests to diagnose network performance.

Traceroute

Traceroute sends packets with increasing Time-to-Live (TTL) to discover a path between a source and a destination host. Each router that forwards a probing packet decreases the TTL value. When the TTL reaches zero, the corresponding router drops the packet and sends an ICMP error message to the source. It is thus possible to estimate the RTT from the probing computer to each hop of the path to the destination.

We use Traceroute from the probing computer to the distant server with the default of three probes per hop. For each measurement, Traceroute discovers the same sequence of IP addresses for the first two hops: the home gateway and the ISP router. Although the values vary for different measurement runs of a given hop, we check that the general conclusions are consistent across runs.

Table 3.3.1 presents an example of the RTTs of the first two hops, for three configurations (we focus on the configurations that had the highest impact on RTTs in Section 3.2). By comparing the Ethernet/Idle case with WiFi/Idle case, we see an increased delay to the home gateway. In general, we observe higher RTTs in all WiFi experiments. In the UL case, however, the RTTs increase by a factor of ten, but between the home gateway and the ISP router, not to the home gateway. Unfortunately, both cross traffic originated at the home and at the access network can explain congestion in the hop between the home gateway and the ISP router. Therefore, our results

Env.	Scenario	Uplink (Kbps)	Downlink (Mbps)	Latency (ms)
Ethernet	Idle	530	5.9	130
	Phone	360	4.9	130
	TV	530	3.3	130
	DL	520	4.7	160
WiFi	Idle	530	5.8	140

Table 3.2: Extract of Netalyzr output

confirm the intuition that Traceroute cannot tell for sure that the origin of the problem is the home network. It can only help in cases where WiFi is responsible for performance degradation.

Netalyzr

Netalyzr [94] is a web-based diagnosis tool. It performs many tests from a probing computer with the help of a distant server and generates a report for the end-user. An execution of the tool takes several minutes to complete. Among other features, Netalyzr checks some configurations and classical security holes. It also provides many detailed hints to help the end-user interpret the tests. The reported metrics can be classified in two kinds: configuration tests (open ports, presence of HTTP proxy, etc.) and performance tests (like uplink and downlink bandwidth, or, latency). We focus here on the performance tests. To measure bandwidth, Netalyzr saturates the upstream and the downstream paths with UDP packets sent at an increasing rate.

We evaluate Netalyzr in our testbed. Note that under the UL scenario over Ethernet, the applet page always times out, and hence no result can be presented for this case. Table 3.3.1 presents the results for Netalyzr's performance tests. It shows that Netalyzr infers lower download speed in presence of TV and upload speed in presence of phone. These result confirms that the home network affects end-to-end performance. The latency measurements, however, present no significant difference when compared to the Ethernet/Idle scenario, probably because values are rounded. There are also little differences between any given Ethernet scenario and its Wireless equivalent. Interestingly, Netalyzr measures little impact in presence of a competing download, except on latency, which is in contradiction with our findings in Section 3.2. Differences in results may come from the differences in methodology: Netalyzr uses UDP where we use TCP (for bandwidth) and ICMP (for latency), and the distant servers are different. This result indicates that Netalyzr avoid bias from competing TCP traffic streams when measuring access link at the expense of a more intrusive test. However, Netalyzr cannot explicitly attribute performance degradation (either in terms of available bandwidth or increased delays) to the home network.

Similar to Netalyzr, we also tried Network Diagnostic Tool[1] as well as Network Path and Application Diagnosis[2]. Without exception, all the tools measure end-to-end performance variation between the scenarios, but they cannot identify that the performance variation comes from the home network because they do not explicitly take the home network into account. It is important to extend these tools with techniques that explicitly identify performance problems at the home network.

3.3.2 Probing the home gateway

A solution to identify that the home network is the cause of performance degradation is to combine the existing troubleshooting tools with extra probing techniques. The idea is to perform extra tests to quickly decide if the home network is the source of end-to-end performance degradation. The simplest identification technique is to directly ping the home gateway. The home gateway architecture prevents us to directly probe the set-top-box or the phone, thus, the only way to identify the presence of phone or TV is to probe the home gateway itself.

We conduct an experiment similar to the end-to-end RTT measurements of Section 3.2. The only difference is that, instead of targeting the distant server, we send the pings to the home gateway. Any delay that a direct ping experiences comes from the home network.

Figure 3.5 plots the distribution of the RTTs from the probing computer to the home gateway (we omit results for the other scenarios, because they show no significant deviation from their idle counterpart). For Ethernet, RTTs range from 0.5 ms to 1 ms, but almost all RTTs are close to 0.5 ms. For WiFi, the RTTs vary from 0.9 ms to 50 ms and we measure 20% of RTTs larger than 10 ms. In Ethernet, the curves for the UL and DL scenarios do not deviate from the idle case. Similar experiments with different packet sizes do not change the results significantly. The fact that the RTT to the home gateway does not depend strongly on the packet size indicates that most of the delay is spent scheduling and not on transmission of packets.

Consequently, direct probing of the home gateway cannot identify all instances of bad performance originated at the home, unless degradation is only due to WiFi. This

[1] `www.internet2.edu/performance/ndt/`

[2] `www.psc.edu/networking/projects/pathdiag/`

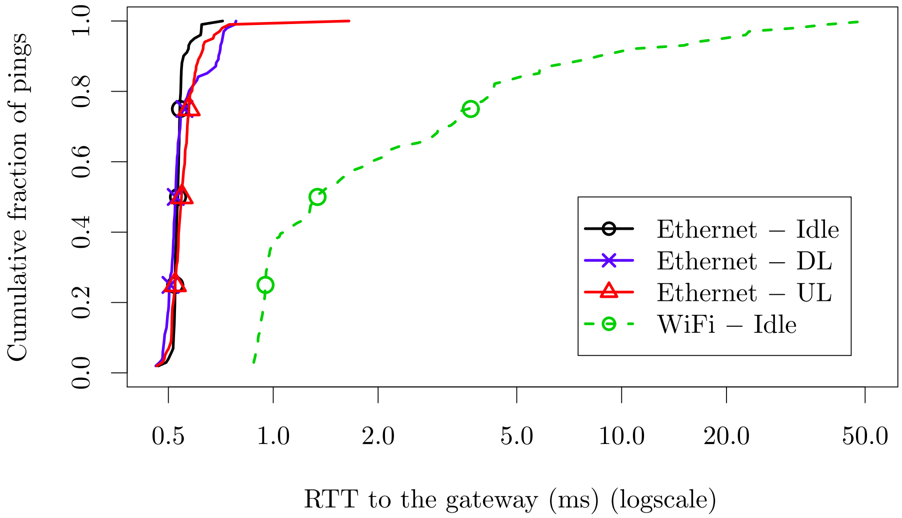


Figure 3.5: CDF of ping to the home gateway.

conclusion explains why Traceroute is not enough to identify the competing upload in Table 3.3.1, but accurately identifies WiFi.

Another solution to identify competing cross traffic is to use UPnP to query the home gateway. The UPnP WANCommonInterfaceConfig profile [160] allows an end-host to query the number of packets and bytes transferred on the WAN interface of the home gateway. In theory, with UPnP, the probing computer should be able to compare the number of bytes sent by the home gateway to that sent by its applications. If the two numbers differ significantly, it means that another device is competing for the access link bandwidth. The home gateway in our testbed supports UPnP but its support is disabled by default. We use UPnP to query the gateway for the number of packets transferred in the Phone, TV, UL, and DL scenarios. We remark that the home gateway counts all traffic from home computers properly. However, the home gateway misses cross-traffic from the set-top-box and the phone. This experiment indicates that UPnP is not reliable enough to be the only test of home performance but it can be useful when available. We report on the UPnP implementation in home gateways later in this thesis with large-scale measurements (Section 6.1).

3.4 Summary

This chapter illustrates how the home network can affect end-to-end Internet performance. We show that simple home network configurations can have a significant impact on end-to-end performance. We need data on home network configurations to know whether home users often have multiple devices active at the same time or not. Hence, the next chapter designs HomeNet Profiler, a software tool to characterize devices present in home networks. We report our findings about devices present in home networks in Section 6.2.

End-host diagnosis tools need to explicitly take the home network into account. In particular, we need better techniques to distinguish problems that arise in the home network and those that arise in the access link. This thesis explores two improvements: UPnP queries and neighbor-assisted diagnosis. Section 6.1 shows that UPnP suffer from many design and implementation issues. When UPnP implementations are correct, UPnP can pinpoint whether packet losses occur in the home or in the access link. Chapter 7 designs neighbor-assisted delay and losses diagnosis, which are method to pinpoint when large delays or loss rates occur in the home network or in the access link.

Chapter 4

HomeNet Profiler Design

This chapter designs HomeNet Profiler, a tool to measure home network configuration and performance. Although there is increasing interest in home networking [89], [20, 27, 28, 168], there is little data on current home networks available yet. Most prior work has focused on measuring and characterizing residential Internet access [31, 35, 47, 73, 94, 107, 149, 154]. The lack of data on home networks is partially due to the challenges of measuring home networks at large scales. The vast majority of home networks are behind network-address translators, so a device outside the home often cannot observe the characteristics of the home network itself. Some prior studies have deployed measurement points inside the homes of a few volunteers [50, 89, 126, 167], but it is hard to get representative results from a few homes.

This chapter first designs HomeNet Profiler and then presents our validation effort. Users run HomeNet Profiler on-demand from an end-host directly connected to their home network. HomeNet Profiler scans the local network for active devices and services advertised via UPnP and Zeroconf. HomeNet Profiler also measures the wireless environment per home. HomeNet Profiler incorporates features to help recruit a large number of volunteers. For example, it performs on-demand, one-time measurements, because many users feel uncomfortable downloading software that will run continuously in their machines. We validate this design choice with a testbed from which we periodically measure six homes in France. We refer to this testbed as the *six-homes testbed*. Our validation shows that not all home devices are active in the LAN at any given time and that a single WiFi scan is enough to observe all neighbor WiFi access points with strong signal.

4.1 Design and implementation

This section discusses the requirements of HomeNet Profiler, our design decisions, and implementation.

4.1.1 Requirements

The primary requirement for a home network data collection tool is that it **runs from inside the home**. Measurements from outside the home cannot have visibility into the home network configuration and its devices, which we want to measure. The goal of measuring a large diversity of home networks and the fact that it is not possible to collect data inside a user's home without explicit user agreement and participation imposes additional requirements:

- **Ease of use.** The tool should be simple to run, even for users who are not tech-savvy. Ideally, users can directly run HomeNet Profiler without prior installation or configuration.

- **Portability.** The tool should work for most end-host configurations and operating systems. In particular, HomeNet Profiler should adapt to the operating system and to the available libraries installed on the end-host.

- **Respect users' privacy.** Users are unlikely to run a measurement tool inside their homes if the tool collects information that they consider private or any personally identifiable information. In fact, our data collection effort has to comply with the rules of the French National Commission of Informatics and Freedom.[1]

- **Light user commitment.** We are asking home users to do us a favor by allowing us to collect data inside their homes. We cannot ask users to commit too much time or resources, otherwise only few users will participate.

- **Incentive for participation.** Some users will run research tools altruistically. However, if users can get something out of the experiment, then we are more likely to get a larger number of participants.

4.1.2 Design decisions

The design requirements outlined in the previous section lead to some high-level design and implementation decisions.

[1] Commission nationale de l'informatique et des libertés (CNIL): http://www.cnil.fr/english/.

First, HomeNet Profiler is *end-host based.* We considered two possible measurement points inside the home: the home router or gateway; or one of the end-hosts connected to the home network. Although some home users host, in their home network, routers that are dedicated to measurements [154], a hardware deployment requires a higher commitment from users than a simple software download on an end-host.

Second, HomeNet Profiler runs *on demand*. While continuous measurements would give us a more complete picture of home network performance and configuration, many users feel uncomfortable installing a permanent software on their machine for privacy concerns and because of the possible impact on machine performance. Inspired by the success of Netalyzr [94], HomeNet Profiler performs a series of measurements upon explicit user request. Users may run HomeNet Profiler as many times as they want. We evaluate one-shot measurements against periodic measurements in Section 4.2.3.

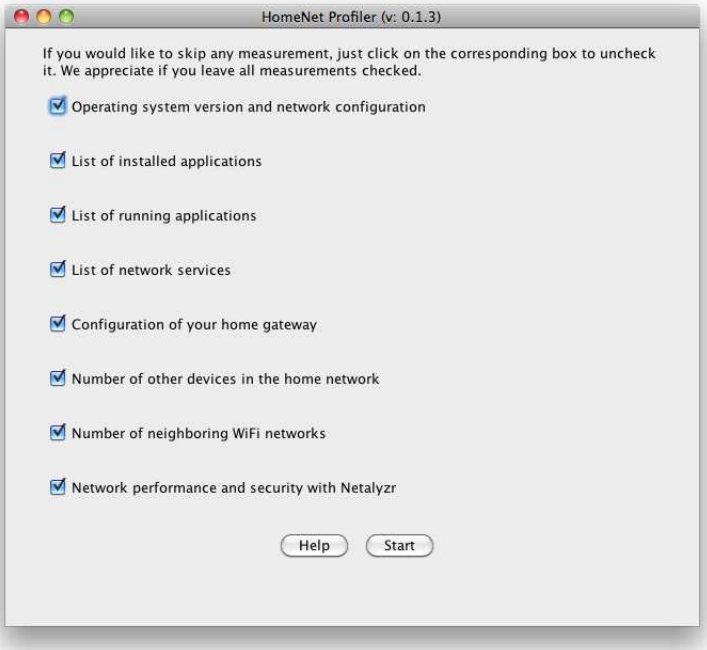
Third, HomeNet Profiler is a *Java executable JAR*. Java facilitates the deployment of HomeNet Profiler on machines with different operating systems. Ideally, we wanted to follow the Netalyzr approach and run HomeNet Profiler from a browser as a signed Java applet. Unfortunately, some of the measurements we want to collect are not possible from an applet. It is hard to load system libraries such as the Windows Native WiFi interface from an applet and we need root access on Linux, which is not possible from an applet. Instead, a Java executable JAR can collect the datasets we want and yet it is simple for users to run because there is no installation or configuration required.

Finally, HomeNet Profiler takes *user perspective* into account with a user survey. The user survey complements our measurements. It allows us to obtain information that would be hard to infer automatically from the measurements (such as finding devices which are turned off, or telling if a user has an Internet service plan that includes VoIP and IPTV). Survey results also serve to validate the measurements.

As an incentive for users to run HomeNet Profiler, users can see a detailed report of the measurements we execute once they are finished. These reports help users learn more about their home network configuration and performance.

Before the measurements start, HomeNet Profiler lets the user select which measurements it will perform. Therefore, users who are uncomfortable with some of the measurements we execute can still run HomeNet Profiler with a sub-set of the measurements. Figure 4.1 shows a screenshot of HomeNet Profiler's module selection screen. Users can also skip the survey.

System overview. We design HomeNet Profiler as a client/server application. The server hosts the HomeNet Profiler website, which users visit to run the HomeNet Pro-



If you would like to skip any measurement, just click on the corresponding box to uncheck it. We appreciate if you leave all measurements checked.

☑ Operating system version and network configuration

☑ List of installed applications

☑ List of running applications

☑ List of network services

☑ Configuration of your home gateway

☑ Number of other devices in the home network

☑ Number of neighboring WiFi networks

☑ Network performance and security with Netalyzr

Figure 4.1: Module-selection screen

filer client. Once the client finishes loading in the user's machine, HomeNet Profiler starts in a separate window. Users then complete the survey while the measurement modules run on the background. Upon completion, the client sends all collected data to the server and redirects the browser to the report page, which is also generated and stored at the server. At the end of the measurements, HomeNet Profiler only leaves a local, randomly chosen, identifier on the user's machine to track multiple runs from the same end-host. A *run* refers to one execution of HomeNet Profiler. We refer to a computer running HomeNet Profiler as an *agent*.

Next, we describe the individual measurement modules, the design of the survey and the report, and some key implementation choices.

4.1.3 Measurement modules

We select a broad range of measurements to learn as much as possible about the home network. At the same time, measurements should not take too long to execute, otherwise users might give up in the middle of the experiment. Our main goal is to discover the devices connected to the home network, the protocols they support (for instance, home devices are often expected to support UPnP [159] and Zeroconf [26]), and the services they provide as well as the network technologies connecting the home to the Internet and inside the home. When the home network has WiFi, neighboring networks may also affect the home network performance. Thus, we measure the quality of all visible WiFi networks. In addition to these direct measurements of the home network configuration and performance, we collect the configuration of the machine running HomeNet Profiler as well as the list of applications installed and running on the machine. The configuration of the machine and the list of running applications help us interpret the results (in case some configuration prevents some of our measurements or some running application interferes with our measurements), whereas the list of installed applications sheds light on the applications commonly available on end-hosts (which should help the future development of an end-host tool to diagnose problems in home networks).

The HomeNet Profiler client has the following measurement modules. To address privacy concerns and comply with French laws, we anonymize all personally identifiable information using SHA1.

Device scan: searches the home network for active network devices. This module first sends UDP packets on Port 9 (i.e., the discard port) to all IP addresses in the sub-network of the agent to generate ARP requests to populate the ARP cache. We use UDP packets because sending ARP packets directly requires root access on most operating systems and users may run HomeNet Profiler as a simple user. We impose a limit of 10 seconds to perform the scan to avoid long delays when sub-networks are too large. (Our measurement campaign confirms that the vast majority of scans finishes in less than 10 seconds.) After the cache is updated, this module reads the ARP cache to collect the vendor ID and the SHA1 hash of the MAC address as well as the IP address (when the IP is private) of each network interface on the LAN. If the IP address is public, we just record the presence of a public IP.

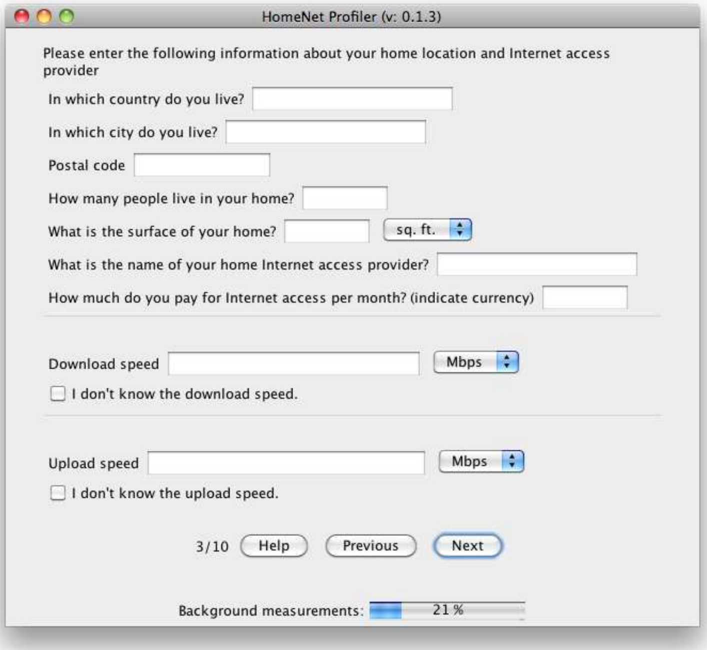
Service scan: queries two commonly-used protocols to advertise services in home electronics: Zeroconf and UPnP. We opt for querying these protocols instead of a port scan per device, because a port scan is intrusive and may take several minutes to complete. For UPnP, we package the SBBI third-party library with our JAR. We could not do the same for Zeroconf, so we use the jmdns library on MacOS and Windows and the avahi-browse script on Linux. If the end-host does not have the corresponding library, we cannot get Zeroconf results. In our tests, we also had cases where one machine in the home detected a UPnP device, whereas another machine in the same home did not. We suspect that these cases happen because the latter machine has a firewall that blocks the UPnP multicast queries or responses. Thus, the absence of UPnP or Zeroconf services is either because no device speaks these protocols or because the end-host cannot complete the queries.

Configuration of the UPnP gateway: collects (in cases where the home gateway has UPnP) the home gateway model, the upstream connectivity type and synchronization speeds (e.g. Cable 4Mbps upload, 1Mbps download), as well as the traffic counters, which reports the number of bytes and packets transferred. Chapter 3 gave anecdotical evidence with a few examples where UPnP traffic counters are incorrect either there is no response or the gateway always responds with the same value). We also perform a simple test to verify whether the UPnP traffic counter is accurate: we compare the UPnP traffic counter with HomeNet Profiler's host traffic counters (e.g. ifconfig on Linux) before and after issuing 20 pings within a 200 ms interval.

WiFi networks: collects the list of access points found with a WiFi scan. For each access point we collect the ESSID (or the network name), the BSSID (the MAC address of the access point), the channel number, and the Received Signal Strength Indicator (RSSI). For privacy reasons, we only collect the SHA1 hash of ESSIDs and BSSIDs. We distinguish between the *home WiFi*, which is the one the end-host is connected to, and *neighbor WiFis*. ESSID-BSSID pairs identify the home WiFi and distinct neighbor WiFis. On MacOS, the airport command-line tool provides all this information. On Linux, we use iwconfig, which unfortunately requires sudo rights. On Windows, we use the Win32 Native WiFi API. This library is not available on old windows XP (prior to SP3), so we can only collect WiFi information for newer Windows machines. We also observed that some Linux WiFi drivers only report information for the network the end-host is associated to.

Netalyzr [94]: performs a number of tests related to the access network configuration, security, and performance. At each execution, HomeNet Profiler downloads the latest version of Netalyzr's command-line client. Once Netalyzr finishes, HomeNet Profiler saves the report identifier. As soon as the report is available on Netalyzr's site, we parse it to extract the upload and download Internet capacity to present on the report given to the user. We also point users to the full Netalyzr report.

Computer configuration: collects the name and version of the operating system; the end-host's network configuration, including the list of DNS servers and TCP parameters; and the list of network interfaces with the corresponding IP address (if it is private, otherwise we just flag the IP as public) as well as the SHA1 hash of the MAC address and the vendor-id part of the MAC address. On MacOS and Linux we collect



HomeNet Profiler (v: 0.1.3)

Please enter the following information about your home location and Internet access provider

In which country do you live?

In which city do you live?

Postal code

How many people live in your home?

What is the surface of your home? sq. ft.

What is the name of your home Internet access provider?

How much do you pay for Internet access per month? (indicate currency)

Download speed Mbps

□ I don't know the download speed.

Upload speed Mbps

□ I don't know the upload speed.

3/10 Help Previous Next

Background measurements: 21 %

Figure 4.2: Example of survey question screen

network configuration with the sysconfig tool; on Windows, we use Win32 API, which gives less detailed information.

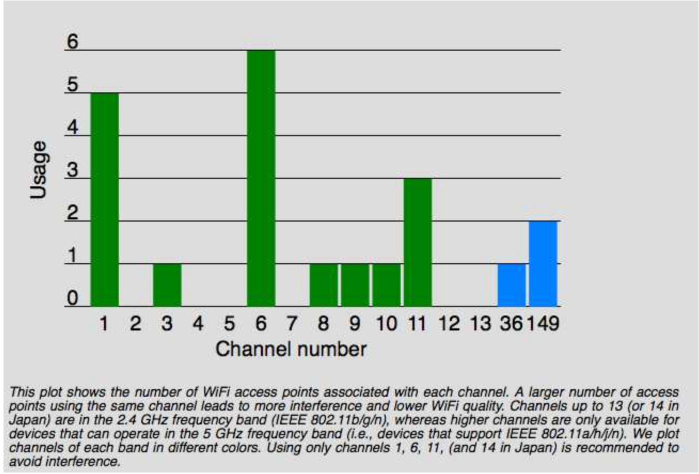
Running applications: captures the list of processes running on the end-host as well as the list of TCP ports listening for incoming connections and open UDP ports. We also collect system services in MacOS and Windows.

Installed applications: lists the applications we find on the `PATH` environment variable. It may not reflect the full list of installed applications.

Aside from these measurements taken from the client, when HomeNet Profiler's server receives the collected measurements, it maps the client's public IP address to its geographical location and AS number using the Maxmind [114] database. We discard the public IP address after this mapping. HomeNet Profiler also sends meta-data such as the duration of each module and whether the HomeNet Profiler process was running with sudo privileges.

4.1.4 Survey module

HomeNet Profiler complements and validates measurements with a user survey, which runs in parallel to the other measurement modules. We design the survey to be fast



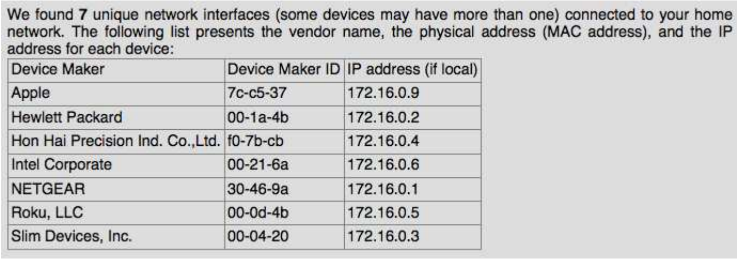
This plot shows the number of WiFi access points associated with each channel. A larger number of access points using the same channel leads to more interference and lower WiFi quality. Channels up to 13 (or 14 in Japan) are in the 2.4 GHz frequency band (IEEE 802.11b/g/n), whereas higher channels are only available for devices that can operate in the 5 GHz frequency band (i.e., devices that support IEEE 802.11a/h/j/n). We plot channels of each band in different colors. Using only channels 1, 6, 11, (and 14 in Japan) is recommended to avoid interference.

Figure 4.3: Histogram of WiFi channels' usage in HomeNet Profiler's example report

for users to complete (approximately five minutes) and easy for us to interpret the results. Hence, all questions but the last are multiple choice. The nine multiple-choice questions focus on the user (whether she is answering the survey from home, where she lives, and her level of expertise on networking), the services the user subscribes to at home (i.e., Internet plan details, the type of TV, phone, and video-on-demand service), and the types and number of devices usually connected to the home network. The free-form question allows users to give us more details about particular home network configurations or optimization that we do not ask in the multiple-choice questions. The survey is available in French and English. Figure 4.2 presents a question screen about users' Internet access plan capacities and information about their household. Similar to the measurement modules, users can skip the survey. Users can also leave any field empty if they want to skip a specific question. In particular, users who run HomeNet Profiler multiple times can fill out the survey only once.

4.1.5 Report design

As incentive for users, HomeNet Profiler presents a report at the end of the measurements with the results (also in English and French). We focus the report on a sub-set of the measurements that should be interesting to users: the wireless quality environment, access link performance, home gateway information obtained from UPnP, and the list of active network devices and services. The report provides some advice to improve home network performance (for instance, if the user's access point operates on a channel that is crowded, we suggest changing the channel). We also add refer-



We found **7** unique network interfaces (some devices may have more than one) connected to your home network. The following list presents the vendor name, the physical address (MAC address), and the IP address for each device:

Device Maker	Device Maker ID	IP address (if local)
Apple	7c-c5-37	172.16.0.9
Hewlett Packard	00-1a-4b	172.16.0.2
Hon Hai Precision Ind. Co.,Ltd.	f0-7b-cb	172.16.0.4
Intel Corporate	00-21-6a	172.16.0.6
NETGEAR	30-46-9a	172.16.0.1
Roku, LLC	00-0d-4b	172.16.0.5
Slim Devices, Inc.	00-04-20	172.16.0.3

Figure 4.4: List of active network devices in HomeNet Profiler's example report

ences to websites that give more details about each of the measurements in the report. Non-expert users can learn more about home networks from these links. HomeNet Profiler's website has an example report. Figure 4.3 is screenshot of a part of the example report. This histogram plots the number of WiFi access points found on each channel as observed from the end-users' computer. Whereas Figure 4.4 is a screenshot of the list of active network devices with their OUI and vendor name.

4.1.6 Implementation

HomeNet Profiler has two main components: the client and the server. We implement the server as a web application written in Ruby. To ensure that users can download the client, upload measurements, and see the reports without blocking on the server side, we replicate the server with eight processes: four processes handle the data collection and the other four handle the rendering of report pages (which takes longer). The data HomeNet Profiler generates is complex and may vary among clients (for example, Windows and MacOS have the concept of service, whereas Linux only has processes). As a result, we store the data in MongoDB, a flexible schema-free database instead of a SQL database.

The HomeNet Profiler client is a Java executable JAR implemented mainly in JRuby with some Ruby and Java libraries. We package JRuby with our JAR because it is usually not installed on end user's computers. When no Ruby or Java library exists (for instance, for doing a WiFi scan on MacOS), we parse shell scripts or wrap C libraries. Ruby's flexibility allows us to implement measurements quickly, whereas Java brings portability and the Swing cross-platform graphical user interface. The main drawback of embedding JRuby is that the runtime library takes approximately 9 out of the 13 Mbytes in HomeNet Profiler's JAR file. Despite the portability of Java, we had to solve a number of platform-specific issues when interfacing with low-level libraries. To help users report these problems, we added a bug-report mechanism, which uploads debug traces from the client to the server. This mechanism was particularly helpful after the larger release of HomeNet Profiler, because we do not personally know all the participants.

4.2 Validation

We validate HomeNet Profiler with a pilot study and with tests on six homes. We run a pilot study to verify the portability of HomeNet Profiler and the clarity of the survey questions. The six-homes testbed lets us validate HomeNet Profiler's one-shot measurements against periodic measurements.

This section first details our pilot study, then we present our six-homes testbed, finally we presents our validation results.

4.2.1 Pilot study

We ran a pilot study with a small group of students, colleagues, and friends from France, Brazil, Canada, and the United States. The purpose of this study was to test measurement modules in different homes and operating systems and to adjust the survey questions and report content before the larger release. During the pilot, testers ran HomeNet Profiler 152 times from 47 different agents. This pilot study allowed us to find and correct bugs on the client as well as display errors on the report pages. We also observed five users while they answered the survey. We asked these users to think out loud and ask us clarification questions. We found that a question, which was asking users to label all of their home devices, was too tedious and annoyed users. Consequently, we replaced this question with a simpler question asking users to give the number of devices they have at home for a sample of pre-selected device types (such as laptop or desktop). We ignore all data collected during this pilot study for the remainder of this thesis.

4.2.2 Testbed

In most cases, users run HomeNet Profiler once, but both the WiFi neighborhood and the devices connected to a home network vary over time. We thus complement HomeNet Profiler by instrumenting six different home networks in Paris. We distributed laptops to colleagues from Technicolor and UPMC Sorbonne Universités to deploy at home. The households have between one and three members. Each laptop runs the WiFi scan module every ten seconds using an Intel WiFi card. Every ten minutes, laptops also run the device scan module on an Ethernet adapter. We collect data from March 19, 2012 to July 31, 2012. These six homes are not representative of the population, but instrumenting a larger number of homes would represent a practical challenge. Nevertheless this six-homes testbed allows us to validate HomeNet Profiler and put collected data into perspective.

4.2.3 Validation results

We analyze the dynamics of devices connected to home networks over time to assess the completeness of device scans in HomeNet Profiler data. We then analyze the accuracy of one-shot WiFi scans.

Evaluation of the completeness of device scans

Some devices may be disconnected from the home network at the time when users run HomeNet Profiler. Hence device scans in HomeNet Profiler are likely incomplete. We evaluate whether how HomeNet Profiler's accuracy increases with the number of consecutive device scans.

Repeated device scans in our six-homes testbed observe different sets of devices. Fig. 4.5 shows the presence of a given device during the four months of data collection. The x-axis is the time of each device scan. The y-axis represents individual devices measured in each home network (identified by their MAC address). We label the y-axis with the home-id and below each home-id, the number of devices observed in that home network during our measurements. We order devices per home based on their occurrence. The most prevalent device of all six homes is the home gateway. Note that there are gaps in the data collection because of maintenance or other measurement campaigns (e.g., measurements presented in Chapter 7) running on the same six-homes testbed. These gaps are easily identified by the vertical bars with no points per home. We ignore these gaps in the following discussion.

The number of devices measured per home in four months varies between 6 and 19 depending on the home. We ask the users to manually label each device observed over the whole data collection period. We divide devices into types: *home devices*, which are those that belong to members of the household; and *visitor devices*, which belong to friends who are just using the home network for a short stay. The topmost devices of each home, those we only observed in a small fraction of the scans, correspond to visitor devices. We observe two types of home devices: always-on devices and on-off

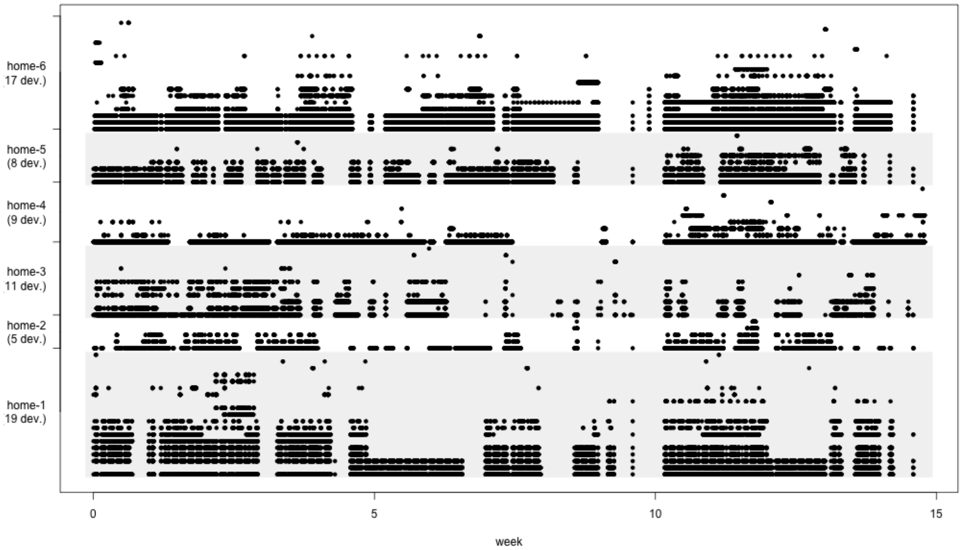


Figure 4.5: Observed devices per home network

devices. *Always-on devices* are the ones users leave on all the time after the device first connects to the home network and until the device is decommissioned. These typically include home gateways and access points/routers. In Home-6 we also observe an IP printer and an IP security camera that were always on, and in Home-1 a network disk appears just before Week 5. *On-off devices* have prevalence between always-on home devices and visitor devices. We observe two types of on-off devices: personal mobile devices (such as laptops and smartphones) that leave the house with their owners; and devices that people turn on when needed (for example, a weighing scale and a gaming console).

We compute the fraction of the home devices observed in a single scan over the number of home devices. Given that HomeNet Profiler requires at least one user in the home to run the tool, we only count device scans when at least one laptop or desktop is on. Overall, we find that a single device scan only observes a small fraction of the home devices. For example, 92% of the scans with at least one laptop/desktop observe at most half of the home devices. Nevertheless, one single device scan captures all always-on devices more than 99.5% of the time. Hence, one-shot measurements are well-suited for studies that measure always-on devices such as the study of UPnP in home gateways of Section 6.1.

We do not observe many more devices by aggregating the results of two consecutive scans (85% of pairs of scans would still observe at most half of the home devices). Only periodic measurements of the home network can observe all the home devices. We find that it takes approximately eight days on average (and a median of four days) to discover all home devices in the six homes we measured. To alleviate the lack of periodic measurements, HomeNet Profiler's survey explicitly asks users to list the devices they typically connect to their home network.

Accuracy of WiFi neighborhood characterization in one-shot measurements

The set of neighbor WiFis can vary considerably even in short time windows (of seconds) because lost WiFi beacons prevent us from inferring the presence of an ESSID-BSSID pair. We study the short-term dynamics of the WiFi neighborhood of each of the six homes in two-minute intervals; during each two-minute interval we perform 12 consecutive WiFi scans. Note that it is practically impossible to get ground truth on the WiFi neighborhood, hence we assume that the aggregate set of measured ESSID-BSSID pairs in the 12 scans represents the complete WiFi neighborhood during the two-minute interval. Then, we compute the *fraction of the WiFi neighborhood observed*, which is the number of ESSID-BSSID pairs observed in the first scan of a two-minute interval divided by the number of ESSID-BSSID pairs of the WiFi neighborhood in this interval.

Intuitively, the probability of a WiFi scan to observe an ESSID-BSSID pair will be lower if the pair has low RSSI. To better understand this effect, we group the ESSID-BSSID pairs into ten *RSSI bins* based on the mean RSSI of each pair during a two-minute interval. We pick bin boundaries at every 10th-percentile of the distribution of mean RSSI per two-minute interval for all ESSID-BSSID pairs to ensure that every RSSI bin has 10% of the points. Fig. 4.6 shows the boxplot of the fraction of the WiFi neighborhood observed. The x-axis presents the RSSI bins (note that the x-axis is not linear). Boxes represent the inter-quartile range of the distribution of the fraction of the WiFi neighborhood observed for ESSID-BSSID pairs in a given RSSI bin; the solid line inside the box is the median, the whiskers represent the minimum and maximum values. The 802.11 standards do not specify units for RSSI and each vendor may use a different scale. All six machines we distribute have the same hardware and software. Hence, we can aggregate RSSIs from the six machines.

Fig. 4.6 confirms our intuition that ESSID-BSSID pairs with stronger signals are easier to observe. For example, the leftmost bin shows that half the time, a single WiFi scan observes no more than 34% of the ESSID-BSSID pairs with RSSI lower than -87, whereas a single scan is sufficient to observe all ESSID-BSSID pairs with RSSI higher

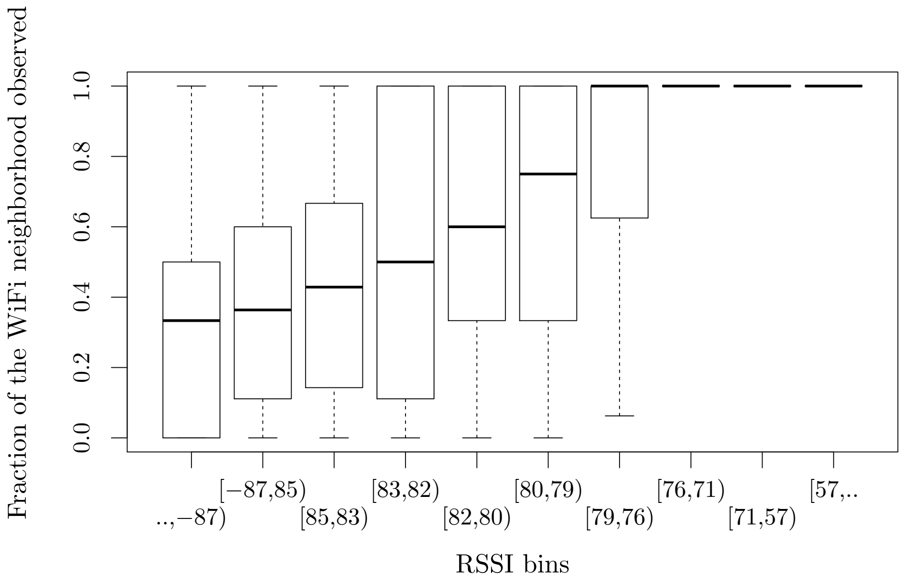


Figure 4.6: Fraction of the WiFi neighborhood observed with one scan for different RSSI bins

than -71. The lower the RSSI, the more scans we need to observe all the ESSID-BSSID pairs. In summary, one scan is enough to collect all the ESSID-BSSID pairs with strong RSSI and to frequently get a large fraction of those with lower RSSI. This result validates HomeNet Profiler's approach of performing a single WiFi scan to speed-up the data collection. ESSID-BSSID pairs with strong RSSI are more likely to interfere with the home WiFi and are also the ones that home users could potentially use for backup connectivity, for instance.

4.3 Summary

We design HomeNet Profiler, a software tool that users run on a desktop or a laptop to measure home networks. HomeNet Profiler scans the local network for active devices and services, observes the WiFi neighborhood, and complements measurements with a user survey. We design HomeNet Profiler as a one-shot measurement tool. We validate HomeNet Profiler with a pilot study and with tests in six homes. Our results show that one-shot measurements capture practically all always-on devices, but only a small fraction of on-off devices. As a result, HomeNet Profiler's survey is an important complement to understand the full set of home devices at a large number of homes. In addition, our results show that one-shot measurements are sufficient to capture all WiFi neighbors with strong signal and a significant fraction of neighbors with lower signal. WiFi neighbors with strong signal are more likely to interfere with the home WiFi or to be useful as backup links. Hence, HomeNet Profiler captures an essential part of the WiFi neighborhood. The biggest advantage of our one-shot approach is that it requires little effort/commitment from users and hence allow us to reach a large number of users. We next present the dataset we collect with HomeNet Profiler as well as heuristics to select one representative per home network.

Chapter 5

Measurement Campaign and Dataset Description

This chapter describes the dataset we collected with HomeNet Profiler. Starting on April 4, 2011, we sent emails advertising HomeNet Profiler to family, friends, and colleagues as well as mailing lists of networking researchers. On April 18, 2011, we posted an announcement on the grenouille.com website, which is a community website that tracks the performance of access ISPs in France. Until November 20 2012, 3,056 unique agents ran HomeNet Profiler 4,125 times. In this chapter, we first report on HomeNet Profiler deployment — which measurement modules users chose to run and the duration of each module. Then, we describe our method to pre-process the collected data to get a single representative run per home. Finally, we discuss the user population in our data from the 2,940 distinct homes. We also describe the type of access link technologies as well as the triple-play services that home users subscribe to.

5.1 Measurement popularity and duration

We evaluate how HomeNet Profiler performs and which measurement modules are most popular among users. Table 5.1 shows the total number of runs and agents that ran HomeNet Profiler and how many users ran each measurement module (this table also presents the number of homes for later reference). We see that 26% of the 3,056 agents skipped the user survey. The survey is the only module that requires active user participation, so it is natural that some people prefer to skip it. Besides the survey, some users are also uncomfortable with collecting the list of running and

Module	Runs	Agents	Homes	Duration		
				Median	5%	95%
Survey	1820	1726	1598	3 min.	1 min.	9 min.
Computer conf.	3980	3021	2395	0 s.	0 s.	3 s.
Installed apps.	3583	2707	2127	2 s.	0 s.	10 s.
Running apps.	3688	2793	2209	0 s.	0 s.	3 s.
Service scan	1978	1572	1391	10 s.	10 s.	20 s.
UPnP Gateway	2844	2210	1956	14 s.	10 s.	38 s.
Device scan	4003	3015	2388	1 s.	0 s.	11 s.
WiFi	3983	2991	2373	10 s.	0 s.	11 s.
Netalyzr	3956	3002	2389	4 min.	54 s.	7 min.
Total	4125	3056	2940	3 min.	40 s.	7 min.

Table 5.1: Popularity and duration of measurements.

installed applications. Interestingly, different users chose to skip different types of measurements (only in 55% of the 4,125 total runs, users chose to run all measurement modules). This value suggests that to attract a larger number of users, it is important to give users the flexibility to customize data collection.

Table 5.1 also shows the median, the 5th percentile, and the 95th percentile duration of each module. All modules run within a few seconds, except for Netalyzr and the user survey. It is natural that these two modules take longer. Netalyzr performs more than ninety different tests, most of them connecting to hosts that are outside the home network. The survey time depends on user participation. The median time to complete the survey is 3 minutes, which is relatively short and reflects our desire to make the survey easy and quick to answer. In 26% of the runs when users answer the survey, the background measurements complete before the survey. Thus, users get the report right after they finish the survey. For the majority of runs when measurements end after the survey, users only wait for a few minutes and the report comes up automatically after the results are uploaded. The median waiting time after completing the survey is 1 minutes. Overall, the duration of a run varies considerably across users, but for the vast majority of users it takes less than 7 minutes.

5.2 Data pre-processing

Users may run HomeNet Profiler in networks that are not home networks and users may also run HomeNet Profiler multiple times from the same home. These two situations may bias our analysis. Hence, we select a single representative run per home. We face two main issues to select a single representative run per home. First, although

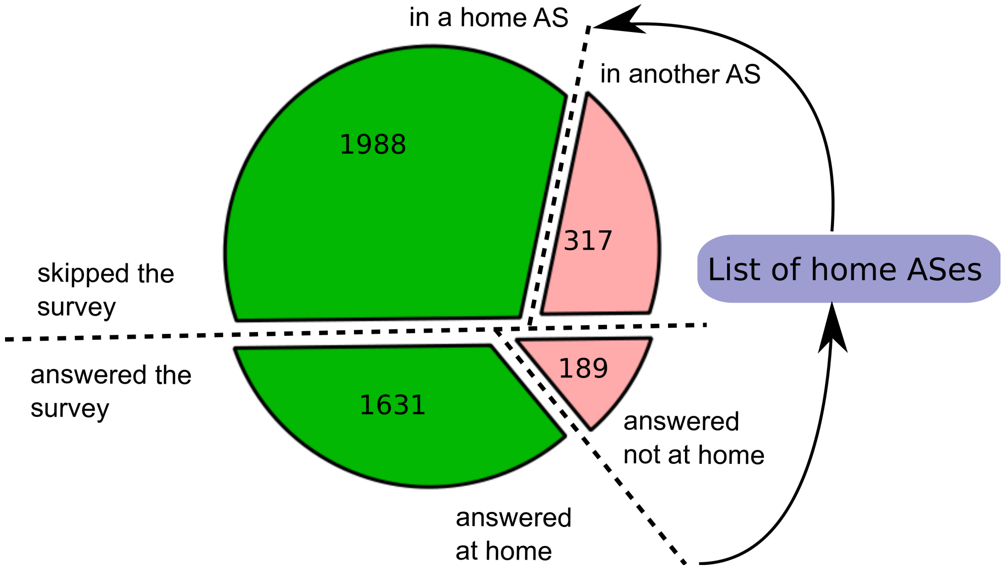


Figure 5.1: Heuristic to identify runs from homes

we ask people to run HomeNet Profiler from home, some people miss or ignore this request. Thus, we need to eliminate all runs from machines that are not connected to a home network. Second, people may run HomeNet Profiler multiple times in the same home. To avoid biasing the results towards any single home, we need to identify the set of different runs from the same home network and select a single representative run per home. We do this in three steps.

5.2.1 Step 1: Identifying runs from homes

One of the survey questions explicitly asks users whether they are running HomeNet Profiler from a machine connected to their home network. Unfortunately, users may not answer the survey. Users answered the survey on 1820 runs and they claimed to be at home on 1631 of these runs. We develop a heuristic to identify runs from homes based on the assumption that we can label ASes as residential versus not.

Our heuristic works as shown in Figure 5.1 and described as follows. Every run has a corresponding AS number, which we collect at the server. For each AS number, we increment a counter when a user reports to be at home and we decrement this counter when the user reports otherwise. We then label every AS that has a strictly positive counter as residential. We say that a run is from a home if the corresponding AS is labeled as residential. When there is only one run from an AS, this heuristic will just label the run according to the user's response (if any). Our manual verification of

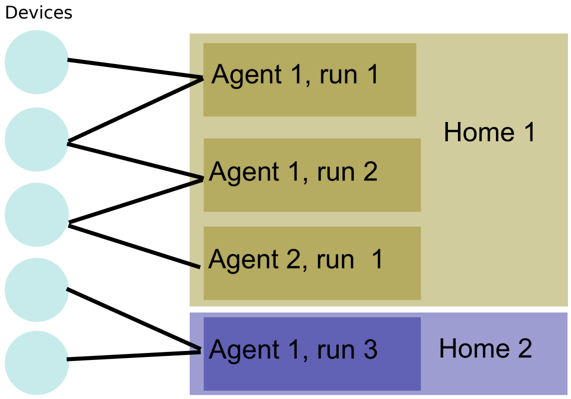


Figure 5.2: Heuristic to group runs from same homes

the list of residential ASes found rare cases of mislabeled ASes (a user that claims to be at home, when connected to a research network). We manually removed these runs. Although this heuristic may misclassify some runs from small business as residential (some residential ISPs also offer services to small businesses), it will filter out ASes that only connect academic/governmental institutions and large enterprises.

5.2.2 Step 2: Identifying multiple runs from the same home

The random identifier that HomeNet Profiler leaves in the user's computer identifies multiple runs from the same machine, but users may also run HomeNet Profiler from different machines in the same home. We detect that two runs from different machines are in the same home with the results of the network scan module. As shown on Figure 5.2. If we find network interfaces with the same hashed MAC address in runs from different agents, we say that they are from the same home. We find 290 such network interfaces, measured by 423 different agents. Our inspection of these interfaces showed that some of them correspond to virtual machines (e.g., the vendor-id is VMware or Parallels). In some cases, we also measure the same MAC address from agents in different cities but in the same AS. Some ISPs seem to configure multiple home gateways with the same MAC address, maybe to facilitate management. To address these cases, we add an extra constraint to our filter and only consider that two runs are in the same home if they are in the same city. After applying this filter, we have 365 homes with more than one agent. For runs where the user skipped the network scan, we consider that they come from different homes.

Run number	Module		Analysis		
	A	B	A	B	$A \cup B$
0	√	√	.	.	.
1	.	√	.	.	.
2	√	√	.	T	T
3	√	.	T	.	.

Table 5.2: Heuristic to select one run per home.

5.2.3 Step 3: Selecting one run per home

Our analysis only considers one run per home. When there are multiple agents in a home, we select the first agent to run HomeNet Profiler. When there are multiple runs from an agent, we select the last valid run for any given analysis. For example, if an analysis only requires the results from one measurement module, we only consider the latest report for this module. When we consider reports from different modules, we take the reports from the latest run with all these modules. Table 5.2 gives a fictional example of which run our heuristic selects in a home with four runs. We only show two modules A and B. The first column gives the index of the run (the larger this value, the more recent the run is). The second and third columns have a marker when the user decided to run a module and a dot otherwise. The remaining columns present the decisions of our heuristic: we mark a T in the line for the run selected when an analysis requires only A, only B, or both A and B.

The selection of a single valid run per home also ensures that in case a user runs HomeNet Profiler on the same laptop in different homes, we will only study one of the home networks. This step does not discard a large number of data point because the vast majority of agents (96%) have runs in a single home. Our manual inspection of the reports from agents with runs in multiple homes indicate that these cases mainly happen for runs without device scans and runs with device scans with a single device (e.g., the user may have changed her home gateway and/or ISP). After applying Step 1 and 2, we infer that our data comes from a total of 2,940 distinct homes. For the rest of this thesis, we only study valid runs from these 2,940 home networks. The number of homes varies for the different analysis depending on the measurement modules we study (Table 5.1 presents the number of homes per module).

Beginner	Intermediate	Expert	No Answer	Total
4 %	30 %	64 %	2%	1596

Table 5.3: User expertise.

Win.XP	Win.7	MacOS	Linux	Other	Total
25 %	50 %	16 %	7 %	2 %	2107

Table 5.4: Operating system of HomeNet Profiler agents.

5.3 Dataset description

We first present some high level characteristics of users running HomeNet Profiler and their home networks.

User Expertise. Table 5.3 describes the expertise of the users answering the survey. The survey asks users to rate themselves as Internet users but who don't know much about the technology behind (beginner), users with basic knowledge of Internet technology (intermediate), or users who understand Internet technology well (expert). The majority of users are self-declared experts in computer networking. This high-number of expert and intermediate users is due to our recruiting method (even the grenouille.com site is mostly read by people who are in general curious about ISP performance). Ideally, one would involve sociologists and use statistical sampling techniques to select a representative set of homes for this analysis. Unfortunately, such recruiting method would represent a significant enterprise, which is not realistic in an academic environment. Instead, we take the approach of most measurements of residential Internet performance, where users volunteer to participate. Even the United States Federal Communication Commission relied on volunteers for their measurements of residential broadband Internet [60]. Expert users are more likely to have more sophisticated home networks with the latest gadgets. Hence, our results are not representative of the population at large. This bias may be an advantage, because expert users might be some years ahead of market and the home networks we measure may be a better representation of the trends in home networking.

Operating Systems. Table 5.4 presents the split of our agents according to the operating system of the end-host. The vast majority of end-hosts run some version of Windows, which is expected from market shares. Linux may be over-represented because

Country	Homes	AS
France	1686	33
United States	307	62
Canada	61	11
Italy	58	5
United Kingdom	55	9
Overall	2424	209

Table 5.5: Homes and ASes per country.

AS Name	Country	Access Technology	Triple play			Homes
			TV	VOD	VoIP	
Free	France	ADSL / Fiber	392	260	525	802
France Telecom	France	ADSL / Fiber	82	76	144	302
Numericable	France	Cable / Fiber	28	30	102	192
SFR	France	Cable / Fiber	62	49	85	176
Bouygues Telecom	France	ADSL / Fiber	34	27	61	95
AT&T	United.States	ADSL / Fiber	2	1	1	47
Cegetel	France	ADSL	11	5	15	38
Verizon	United.States	ADSL / Fiber	6	6	5	30
Telecom Italia	Italy	ADSL	2	1	2	29
Comcast	United.States	Cable	2	1	3	25

Table 5.6: Top ASes.

our dataset also has a majority of expert users. The operating system with the largest amount of platform-specific code is Windows, fortunately the bug-report mechanism allowed us to correct any issues that arose as more people ran HomeNet Profiler.

Geographical spread. Users ran HomeNet Profiler from home networks in 44 countries and 208 different ASes. Table 5.5 shows the number of home networks and ASes we measure overall and for the top-five countries in our data. France dominates our data, mainly because of the announcement on the Grenouille website. This table shows that we obtain measurements from a fair number of different ASes in the top five countries.

Internet Access Plans. Table 5.6 lists ASes for which we have at least 25 homes together with the access technologies they provide as reported on their website. HomeNet Profiler's survey includes three questions about which technologies home users have to receive phone, TV, and video on demand (VoD) at home. Table 5.6 also includes the number of users who answered that their Internet plan includes VoIP, IPTV, or VoD service (which are commonly referred to as triple-play services). The majority of homes in French ISPs have triple-play services, but these services are not as common in other countries.

The survey also asks users to pick the type of Internet access technology they have at home from a multiple choice list. In a number of answers to this question, users claim to have cable or Ethernet, when the ISP only offers ADSL or fiber connections. Clearly, some of the questions in our survey are too technical for some users. The questions about the technology of Internet, TV, phone, and VoD access are particularly challenging. In fact, some users contacted us by email expressing concern about the answers to these questions. In the rest of this thesis, we focus on the survey answers that are easier for users such as the number and types of devices they have at home.

5.4 Summary

In around two years and a half since HomeNet Profiler first release, users ran HomeNet Profiler 4125 times from 3056 distinct agents. Only 55% of HomeNet Profiler measurements runs have results for all measurement modules. Hence, data analyses using data from different modules will also have a different number of data points. Users may run HomeNet Profiler when they are at work or in any network. Hence, we filter our dataset in three steps to select a single representative run from home. After this filtering, we infer that our data comes from close to 3,000 distinct homes. Our recruiting strategy bias our dataset towards expert users and home networks in France.

The next chapter characterizes three aspect of home networks with HomeNet Profiler data: the implementation of UPnP in home gateways, the set of devices and services in home networks, and the WiFi environment of the home networks.

Chapter 6

Characterization of Home Networks

This chapter analyses the HomeNet Profiler dataset for the set of devices, services, and the WiFi environment of different home networks. Our results should guide efforts to model home networks and the development of future home network technologies. We identify two opportunities for improving home network troubleshooting: on one hand, we show how querying UPnP-enabled home gateways help infer cross traffic in the home network. On the other hand, we evaluate WiFi communities as auxiliary vantage points for network performance diagnosis.

We first explore whether it is possible to query home gateways with UPnP to diagnose home networks (Section 6.1). UPnP technology holds promise as a highly efficient way to collect and leverage measurement data and configuration settings available from UPnP-enabled devices found in home networks. Unfortunately, UPnP proves less available and reliable than one would hope. We use data from 120,000 homes, collected with the HomeNet Profiler and Netalyzr measurement suites. In more than half of the homes, we could not collect any UPnP data at all, and when we could, the results were frequently inaccurate or simply wrong. We identify seven different problems with the UPnP implementations observed in our dataset. Whenever UPnP-supplied data proved accurate, we demonstrate that UPnP provides an array of useful measurement techniques. UPnP can help inferring home network traffic and losses, identifying home gateway models with configuration or implementation issues, and obtaining ground truth on access link capacity.

Second, we study the devices and services present in home networks using Home-

Net Profiler data (Section 6.2). We find that the set of devices in home networks varies across homes. The total number of end devices connected that people usually connect to their home networks varies from 1 to over 20, with low correlation to the number of people in a household. In addition, only a few of these devices are active at any given time. Our data show that there are no significant differences across countries. We further find that the deployment of auto-configuration protocols such as UPnP and Zeroconf is limited.

Finally, we examine the WiFi environment of home networks measured from an end-host in the home network (Section 6.3). The quality of home WiFi networks is often good compared to neighbor WiFis. Interestingly, around 15% of the end-hosts we measured in France detect a neighbor WiFi with a stronger signal than the home WiFi. We find that WiFi communities are prevalent in France and that more than 60% of end-hosts in our dataset observe at least one WiFi community.

6.1 Leveraging UPnP in home gateways

The network measurement community increasingly focuses attention on measuring and characterizing broadband Internet access and home networks. For example, a number of measurement efforts infer the speed of residential Internet access networks from different vantage points: servers in the Internet [47], end-hosts connected to home networks [15, 94], or home gateways [154]. Some research groups advocate instrumenting home gateways for measuring both access network performance and properties of home networks, because all traffic between the home network and the Internet traverses the home gateway [20,28,154,167]. On the other hand, measurement suites such as Netalyzr [94] and Ono [15], which run on the end-hosts, face a lower start-up cost and have demonstrated the potential to reach a large number of homes.

With UPnP, a tool running on an end-host connected to the home network can directly query the home gateway, which is a great opportunity for home network measurements. For instance, the tool can obtain the manufacturer and the model of the home gateway to then pinpoint devices that suffer from particularly oversized buffers. As another example, end-hosts can obtain the capacity of the access link and the volume of traffic traversing the gateway, which can help explain measured link speeds. Despite UPnP's promises, the few measurement studies that have leveraged UPnP to date have focused on only a handful of home gateways [1], and so the general degree of UPnP adoption and the usability of its implementations has so far remained unclear.

This section evaluates UPnP implementations in home gateways using data collected with Netalyzr and HomeNet Profiler. We first describe our measurement methodology and our dataset. We then present the measurement artifacts that appear due to broken UPnP implementations or specific home topologies such as homes with multiple UPnP-enabled home gateways. Finally, we show how UPnP can help in measuring home networks to get ground truth on access link capacities, infer cross traffic, or detect models of gateways with large buffers.

6.1.1 Measurement method

We base our analysis on measurement data collected by HomeNet Profiler and by the Netalyzr test suites. Both run on end-hosts, generally within a home network, and perform a series of measurements when prompted by the user. To get a common baseline for buffer delays, up/downlink capacities, and round-trip times both tools execute the same code because HomeNet Profiler runs Netalyzr via its command-line API. The main Netalyzr paper [94] presents the details of these measurements.

While developing HomeNet Profiler, we discussed our results about the effect of the home network on end-to-end performance with Netalyzr authors and proposed them to add UPnP queries into Netalyzr. In the following we describe UPnP's basic operation, and detail the UPnP measurements in Netalyzr and HomeNet Profiler.

UPnP protocol. UPnP provides mechanisms for LAN-level discovery and control of a wide range of services specified by the UPnP standards. Discovery employs multicast UDP requests in order to contact peers matching a specific service class, expressed in HTTP header-like plain text. The responses, if any, contain HTTP URLs via which the client may obtain a device's full description, expressed in XML. This description contains a list of APIs the client may subsequently invoke via the HTTP SOAP protocol. The UPnP standard specifies security levels for the APIs to limit the threat of rogue clients accessing sensitive APIs. We employ only non-sensitive APIs.

UPnP measurements. Given our focus on services offered by home gateways, we first discover any 'WANCommonInterfaceConfig' services. We then retrieve the device description from responding devices, and collect four non-sensitive gateway configuration parameters: (1) the device model name and version, (2) the device's WAN interface type (e.g., DSL, Cable), (3) the physical connection rate (e.g., 10 Mbps/1 Mbps), and (4) unidirectional byte/packet counters maintained by the gateway. To test the accuracy of these counters, we retrieve them immediately before and after sending known-size packet trains to a server in the Internet. Hence, we can compute the amount of cross traffic during the experiment provided that traffic counters are accurate. Netalyzr's packet train consists of UDP bursts making up its bandwidth test. Comparing the actual before/after counters to the expected values allows us to gauge cross-traffic. Note that HomeNet Profiler also obtains traffic counters from the local system to account for other cross-traffic from or to the local host.

In addition to the client-side measurements, Netalyzr's server logs the client's AS number and geographical location based on the public IP address that reports the measurements. Netalyzr also includes a survey that explicitly asks users whether they ran the tests from their home. We use this information to identify runs from home networks as opposed to tests conducted from public or office networks. We apply a heuristic similar to the one we use in HomeNet Profiler (cf. Section 5.2) to select only Netalyzr runs from end-hosts in home networks.

6.1.2 Dataset

We employ three datasets, summarized in Table 6.1. The HomeNet Profiler dataset ("HNP") included UPnP measurements from the beginning. Netalyzr added UPnP measurements incrementally. The first version with UPnP, which we call "Netalyzr-1," performed only the device identification. The recent version, "Netalyzr-2," implements all UPnP measurements discussed in Section 6.1.1. The UPnP column refers to the percent of homes with UPnP gateways.

Dataset	Start date	End date	Homes	UPnP	Countries	ASes
HNP	4/4/2011	12/15/2011	2423	53%	44	208
Netalyzr-1	3/23/2011	8/29/2011	95417	22%	131	1373
Netalyzr-2	8/30/2011	12/15/2011	30243	47%	114	949

Table 6.1: Dataset description

The table indicates that we only obtain UPnP measurements in 35% of all homes. An explanation for the differences in the fraction of homes with UPnP gateway may come from the population bias of each dataset. HNP is biased towards France, Netalyzr-2 towards Germany, whereas Netalyzr-1 is more balanced. This value does not necessarily mean that the home gateways do not implement UPnP. We identify three possible reasons for failing UPnP measurements, which we cannot distinguish in the data: (1) some gateways do not actually implement UPnP; (2) others implement it, but keep UPnP disabled by default; (3) host-level firewalling prevents the end-host from issuing UPnP's multicast discovery query or seeing the responses. The rest of this section analyzes the homes in which at least one gateway responded to the service discovery query. We first discuss measurements artifacts and how we eliminate them from our dataset, then we present the results with the rest of the data.

6.1.3 Measurement artifacts

When the client manages to receive UPnP responses, the reported values may still be misleading or simply wrong. This section discusses the issues we encountered in practice and explains how we clean the dataset from these measurement artifacts. We first discuss the challenge of interpreting UPnP data correctly without additional information about the home network configuration. Then, we report UPnP specification and implementation problems.

Misleading home network configurations

We report two misleading home network configurations.

Gateways connected over Ethernet. We find 27% of homes with UPnP where the gateway reports Ethernet WAN connectivity. While some homes might connect to the Internet via Ethernet, only few ISPs offer this kind of service. In fact, the top ISPs with gateways that reported Ethernet connectivity in our measurements were Vodafone, Verizon, and Comcast, which do not provide this type of connectivity. We thus believe that most of these cases correspond to homes where the UPnP gateway connects to a modem via Ethernet and the modem connects to the ISP. The reported synchronization rate is then the speed of the Ethernet link between modem and UPnP gateway (e.g., 100 Mbps), which does not reflect the access link speed. When comparing UPnP link speeds with measured link capacity, we therefore eliminate all cases where the gateway claims Ethernet connectivity.

Homes with more than one UPnP gateway. We detect that 3% of the homes with UPnP have more than one UPnP gateway in Netalyzr-2 and 4% homes in HNP. Such configurations occur in large homes, where it becomes necessary to install multiple access points to cover the entire place. In these deployments, the primary gateway connects to the access link and the others connect to this primary gateway via Ethernet. Since our data cannot reveal the actual primary gateway (Netalyzr runs a Traceroute from the server, which stops at the home gateway), we remove these homes from the rest of the analysis. In Netalyzr-1, we only have UPnP queries to the first device that responded as a gateway. Hence, Netalyzr-1 may contain outliers. Given the number of homes with multiple gateways is small, this artifact should not significantly bias our results.

UPnP design and implementation issues

We report five UPnP design and implementation issues.

Inconsistent UPnP discovery. HomeNet Profiler uses two distinct queries to discover UPnP services: one query searches explicitly for gateways (as described in §6.1.1), the other queries for any UPnP service with a wildcard option. We compare the number of UPnP gateways found by these two queries as a sanity check. Among the 2188 homes with both measurements, the two queries agree in 85% of the homes; in 14% of the homes, the gateway only answers to the specific search, and in 1% of the homes the gateway only answers the wildcard search. We found no correlation between the gateway model or the ISP and these inconsistent responses, so if the differences stem from implementation errors, these problems only manifest rarely. Lost query packets could likewise offer an explanation for the differences. In the rest of the section, we only analyze data from devices we discovered via explicit requests for gateway devices.

Incomplete identifiers. UPnP provides two fields to identify devices: name and model. In practice, these fields are not always specified. In some cases, we only get the device name, but not the model. In others, the device name has the UPnP profile name or a vague description such as "Wireless Router" and not the device name.

Inaccurate connection type. We find 23% of homes in the French ISP SFR where the gateway reports Cable connectivity. This ISP does not offer cable Internet. In addition, the same homes all report a symmetric synchronization rate of 4.2 Mbps, which the ISP does not actually offer. We conjecture that some SFR's gateways have a hardcoded UPnP configuration. We find a similar configuration in other models but at a lower frequency.

Inaccurate synchronization rates. We identified three cases of access link synchronization rates reported inaccurately. First, in 1% of homes, the synchronization rate is reported in wrong units. The gateway reports a synchronization rate lower than 64 Kbps, even for ADSL or Cable users. Given the values, we believe that these UPnP implementations report values in Kilobits/s or KiloBytes/s, instead of bits per second (as specified in UPnP specification). This problem affects 30 models by three distinct vendors. Second, in 7% of homes, the gateway reports a synchronization rate of zero in both directions, which clearly cannot be the case given we could contact servers outside the home. Most of these inaccurate values occurred with Sagem and Fritzbox gateways. Finally, some ISPs configure the gateway to report a hardcoded synchronization rate, which often corresponds to the rate the ISP advertises commercially and not the rate negotiated between the modem and the DSLAM or CMTS. In particular, almost all customers of the French ISP Free have the exact same synchronization rate.

Inaccurate traffic counters. The UPnP gateway does not respond to the traffic counter queries in 22% of the homes of Netalyzr-2 and HNP datasets. We observed this behavior with 46 models, mainly D-Link, DIR, and, Freebox. In 4% homes, UPnP gateways answer the query for traffic counters, but always report the exact same value. We found 185 gateways models that answer with hardcoded values, most often from Sagem, Thomson, and SpeedTouch.

We remove all inaccurate reports (on connection types, synchronization rates, and traffic counters) from the relevant analysis in the rest of this section.

6.1.4 Analysis

This section illustrates four practical examples where UPnP queries help enhance end-host based measurements.

UPnP link capacity versus measured capacity

We compare the upload and download capacities measured by Netalyzr with the capacity reported by UPnP. Figure 6.1 presents the measured upload rates versus the reported upload rates per home. Most points in this figure fall on a straight line with slope 0.86 and zero intercept (72% of the points are within a 5% interval). This linear relationship comes from the protocol overhead of PPP encapsulation. UPnP reports the raw rates, whereas Netalyzr measures IP rates. We observe a cluster of points with upload rates around 1.2 Mbps, which is a common commercial uplink limitation. Measured upload rates are consistently close to the 0.86 line, which indicates that the uplink is the bottleneck in the end-to-end path and that there is little cross-traffic from the home competing for uplink bandwidth.

Figure 6.2 compares the measured download rates with the download rates UPnP reports per home. Again, we see few points above the $Y = 0.86X$ line, indicating the

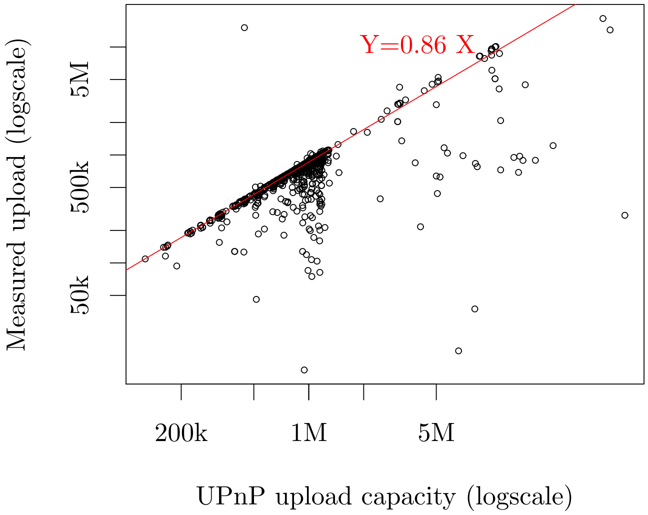


Figure 6.1: UPnP reported uplink capacity versus active measurements (1,084 homes)

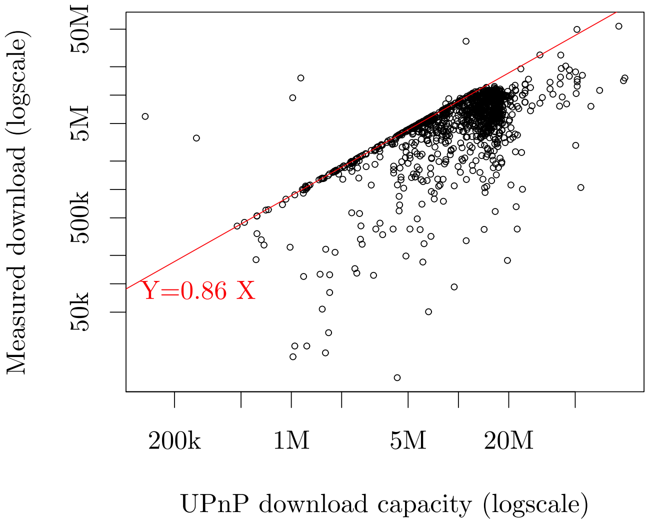


Figure 6.2: UPnP reported downlink capacity versus active measurements (1,084 homes)

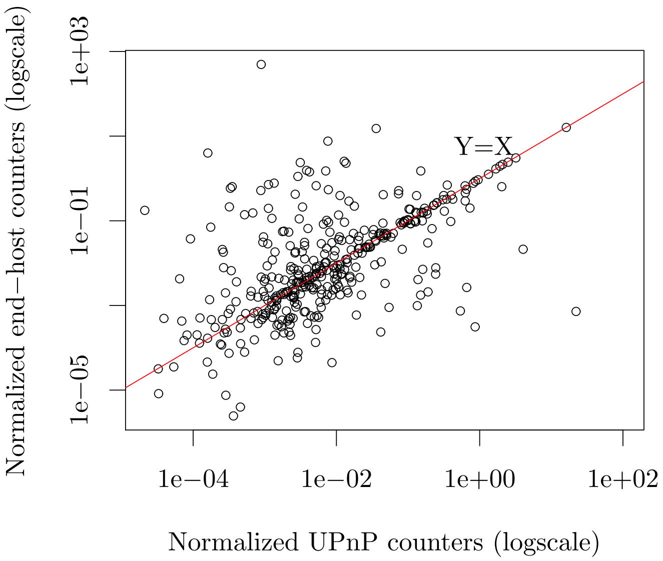


Figure 6.3: Access link uplink usage from the localhost and at the gateway (This figure presents results for 461 homes in HNP)

same overhead as for uploads, and clustering along the line. However, download rates exhibit more variance than upload rates. In general, most Internet applications (such as web surfing or media streaming) consume more downlink than uplink bandwidth. The higher variance in the downstream direction thus suggests that cross-traffic may affect downstream bandwidth measurement accuracy more than in the upstream direction, despite upstreams frequently possessing smaller available bandwidths. This result reaffirms previous measurements of residential broadband Internet access in the United States [154].

Inferring cross traffic

A measurement tool running on an end-host inside the home can estimate the cross traffic from other hosts connected to the home network by querying the gateway's UPnP traffic counters. We study traffic counters in the HNP dataset, because it logs both UPnP counters and traffic counters in the local host. In this dataset, we obtain realistic traffic counter measurements in a total of 462 homes. Homes in the dataset have different access link capacities and the amount of cross traffic for a given amount of time may vary from home to home. We want to estimate the fraction of the capacity that cross traffic uses during our measurements. Hence to compare results across homes we normalize the number of bytes observed by the gateway (computed from UPnP counters) by Netalyzr's measured uplink capacity; we perform the same normalization to the number of bytes sent by the local host.

Figure 6.3 plots the normalized traffic observed at the gateway on the x-axis versus the normalized traffic sent by the host in the y-axis. When x=y, the gateway and the host observe the same traffic, which implies that there is no other traffic in the home network or to the Internet. For points below the diagonal line, the gateway saw more traffic than the end-host, which indicates that other devices in the home network were sending traffic to the Internet. For points above this line, the host was sending traffic to other local destinations (note that the UPnP counter only reports traffic to and from the WAN interface). This plot shows that in most of the homes there was mainly local traffic (from the host to other devices in the home) during our measurements. This case accounts for 53% of the points in Figure 6.3, whereas the case with cross-traffic from other devices to the Internet represents 38% of points. It may seem surprising to have more traffic to the local network than the Internet. This result is just an artifact of our measurement methodology. When users run HomeNet Profiler or Netalyzr, they often just wait for the results instead of running other Internet applications on the side. In this scenario, the background traffic in the home network (of protocols such as DHCP) composes most of the cross-traffic. In fact, the volume of local cross-traffic is less than 18 KB in 90% of HomeNet Profiler's test.

Quantifying loss in the home vs. the wide area

The UPnP traffic counters also prove useful for distinguishing packet loss in the home network from that in the wide area, a use case often mentioned by proponents of gateway-driven measurements. We can conduct the same measurement with a passive UPnP-enabled gateway by extending Netalyzr's bandwidth test, as follows. The test consists of UDP packet round-trips from the client to Netalyzr's servers and back. Small upstream packets with large downstream responses measure downstream bandwidth and vice versa. The measurement records the number of packets sent by the client (P_c), received by the server (P_s), and responses received back at the client ($P_{c'}$). The packet counters provided by UPnP gateways (P_g) add an extra loss tracking point, which allows locating dominant loss directionally: for the uplink, $P_c \gg P_g \sim P_s$ indicates loss in the home, while $P_c \sim P_g \gg P_s$ reflects loss in the wide area. The downlink follows analogously. This inference could misreport if the local network drops packets

		WAN	
		No loss	Loss
LAN	No loss	4 %	42 %
	Loss	32 %	22 %

Table 6.2: Location of losses (6,887 homes in Netalyzr-2)

while traffic from another home device to the Internet increments the UPnP counters. To avoid false identification, we only consider cases with at least 5% packet loss.

Table 6.2 breaks down the location of packets losses in Netalyzr-2. We have correct traffic counter measurements for 11508 homes. We keep 6887 homes for which UPnP traffic counters report cross-traffic less than 10% of the estimated uplink capacity. There was no loss in only 4% of tests. This result is expected because Netalyzr's capacity test sends a high rate of packets to fill the pipe, which induces packet losses. In 42% of tests, losses occur in the wide-area (possibly at the access link, but we cannot pinpoint where in the wide-area exactly). In total, we observe losses in the home network in 32% of tests. It is expected that well provisioned local networks will have less losses. In our future work, we will study whether these losses correlate with wireless home networks.

Buffer sizes

The effects of over-sized buffers, so-called "buffer bloat", have recently received renewed attention by the measurement community [4, 65, 83, 94]. Common wisdom holds that most end-to-end buffering occurs at the gateway, but many different places could introduce buffering, for example the operating system on the end-host; wireless access points; or other equipment in the access link. We use UPnP's gateway model information together with Netalyzr's upload capacity and RTT-under-load measurements to infer the buffer sizes of individual gateway models. To avoid any bias in our inferences because of buffering happening on the wireless link, we only conduct this analysis for homes where our measurements run over a wired link. For each home, we infer the amount of buffering from the RTT under load and the measured upload capacity. We then plot the probability density function of these buffering values for all homes with a given gateway model. We take the point of highest density in this plot as the inferred buffer size for this gateway model. In most cases, we see one clear spike in the density function. The consistency of the gateway buffer measurements for all homes with a given model confirms that most current gateways have a fixed buffer size, irrespective of the uplink capacity. Ideally, the buffer size should be proportional to the uplink capacity, which determines the buffer draining rate.

Model	Homes	Buffer size (KB)	Median (KB)
FRITZ Box 6360	264	370	367
Actiontec IGD	285	252	286
Linksys Series Router E1200	59	223	259
DIR 615	447	209	242
Freebox ADSL	113	147	147
Inventel UPnP	79	139	145
PK5000	70	134	142
Sagem Livebox	555	138	141
N Plus Wireless Router	92	120	70
FRITZ Box Fon WLAN 7390	1542	49	45

Table 6.3: Buffer sizes in KB of UPnP models, Ethernet only

Table 6.3 presents the inferred buffer sizes and the median buffering values for gateway models that appeared in at least 30 homes. For conciseness, we only present one model per vendor if several models from the same vendor have similar buffer sizes (for example, other models of Fritzbox have similar buffer sizes to the Fritzbox 7390). Buffer sizes vary from 22 to 365 KB. For a typical uplink rate of 1.2 Mbps, any buffer larger than 150 KB will introduce more than one second delay under load, which is prohibitively large for interactive applications. This delay would increase to 2.3 seconds for a 512 Kbps uplink.

6.2 Diversity of in-home network devices and services

We investigate how home networks vary in terms of devices and services using the home network dataset.

6.2.1 Number of devices

We use the HomeNet Profiler data to study the devices that connect to home networks. We infer the *number of active devices* at the time HomeNet Profiler runs in a home network by counting MAC addresses present in the device scan. We remove devices with a MAC address belonging to a virtual device. In our dataset, the OUI for virtual machines are VMWare, Hyper-V, and Parallels. As seen in Section 4.2, one-shot device scans often miss some devices. Given we only have one-shot measurements, we take the answers to the survey as ground truth for the *total number of devices*. Although

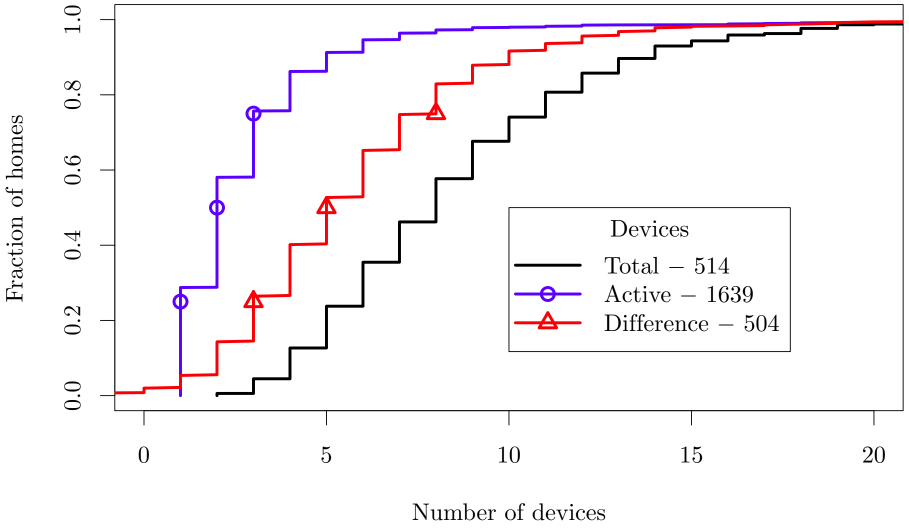


Figure 6.4: Number of active devices versus the total number of devices per home.

users may misrepresent the number of devices in their home, we expect most users to answer this question correctly.

Fig. 6.4 shows the cumulative distribution of the number of active devices and the total number of devices across measured homes as well as the difference for homes where users selected both measurements (i.e., the number of total minus active devices for each home). The number in the legend represents the number of homes included in the respective curve. The total number of devices per home ranges between 2 to 29, presenting a much wider spread than what we observe in our six-homes testbed. HomeNet Profiler's larger scale measurements are essential to capture this wider spread of home network sizes. The range of the number of active devices, however, is smaller than that of the total number of devices. Approximately 75% of homes have at most four active devices during our measurements. This result is in agreement with our validation that shows that just a small fraction of home devices are on at any given time. The 'difference' curve confirms that many home devices are not connected when HomeNet Profiler runs.

The size of each household (i.e., the number of members living in a household) may explain the number of devices in a home network. However, some devices such as printers serve all members of a household. For the 498 homes for which users re-

Country	Desktop	Laptop	Smartphone	Printer	Console	Phone	TV	Homes
France	87%	88%	59%	53%	40%	63%	39%	511
USA	81%	90%	63%	55%	41%	17%	15%	78
Canada	81%	85%	56%	48%	30%	19%	4%	27
Brazil	83%	100%	54%	13%	25%	8%	4%	24
Italy	95%	95%	62%	43%	29%	14%	10%	21
Overall	84%	90%	61%	50%	38%	48%	31%	747

Table 6.4: Types of devices based on the survey.

ported the size of their household, we find that the number of active devices and the size of the household have a Pearson correlation coefficient of only 0.40. The coefficient increases to 0.45 when considering the total number of devices and to 0.51 when considering only laptops and desktops. These results imply that the size of a household does have a moderate positive correlation with the total number of devices and hence the size of the household should be considered to model the total number of devices in the home.

6.2.2 Types of devices

We study how often different types of devices are present in home networks. HomeNet Profiler has two mechanisms to identify the types of devices. First, the survey asks users the number of devices of each type. Second, the device scan stores the OUI of each device, which can give some indication on the type of device (for example, Linksys makes WiFi access points).

Table 6.4 presents the percentage of homes with each type of device considering the answers to the user survey; the last column presents the total number of homes with answers to this question. We only show devices that appear in at least 30% of homes overall. As expected, desktops and laptops are the most popular devices. Users report at least one desktop computer in 84% of the homes and at least one laptop computer in 90% of the homes. Interestingly, laptops are consistently more popular than desktops. Smartphones are also popular (61% of the homes have at least one). These numbers reflect market trends [34, 138]. Tablets, however, have not yet been popular when the bulk of HomeNet Profiler dataset was collected (in 2011). Only 18% of homes have a tablet. Home networks also often have printers (50%) and gaming consoles (38%). The percentages of users with IP phones and TVs are much higher in France than in other countries. Given that most French ISPs offer triple-play services, we conjecture that these users got confused when answering the question. They declare to have an

AS	Most popular vendors			Homes
Free	Freebox (83%)	Apple (10%)	Asustek (10%)	732
France Telecom	Sagem (69%)	HP (11%)	Apple (11%)	265
Numericable	Netgear (52%)	Hon Hai (16%)	Apple (15%)	166
SFR	SFR (84%)	Netgem (30%)	Netgear (12%)	165
Bouygues Telecom	Sagem (60%)	Thomson (34%)	Apple (12%)	97
Cegetel	SFR (71%)	Netgem (21%)	Intel (18%)	38
AT&T	2Wire (42%)	Apple (26%)	Linksys (21%)	38
Verizon	Actiontec (58%)	Motorola (29%)	Intel (29%)	31
Comcast	Apple (52%)	Linksys (36%)	Netgear (16%)	25
Telecom Italia	Pirelli (38%)	Netgear (19%)	Apple (14%)	21
Deutsche Telekom	AVM (33%)	Arcadyan (19%)	Asustek (19%)	21

Table 6.5: Most frequent device vendors found in device scan.

IP phone when in fact their provider delivers VoIP to a regular phone. The same error happens for answers about TV technologies.

We also study the vendor for all devices that are active during the device scan measurements using the OUI. Table 6.5 shows the three most frequent device vendors for every AS with more than twenty homes (the last column shows the total number of homes with these measurements). The numbers in parenthesis are the percentage of homes with at least one active device from a given vendor.

As seen in Section 4.2.2, device scans captures all always-on devices and only a fraction of on-off devices. Hence it is natural that the most prevalent device vendors are home gateways and WiFi access points vendors. We see a clear correlation between equipment names and ASes. For example, the Freebox is the home gateway of Free, and hence we only see it in home networks that subscribe to Free (similarly, for Pirelli in Telecom Italia's network and Actiontec in Verizon's). In these cases, the home gateway comes with the subscription to the Internet access service. Other popular vendors are standard WiFi access point vendors such as D-Link, Linksys, and Netgear. These vendors are present in almost all countries. Apple is popular both in AT&T and in Comcast. Apple makes access points, computers, smartphones, and tablets. We cannot distinguish these different types of devices from the vendor OUI alone. Overall, no vendor dominates the market. The device vendors that we observe in home networks are fairly diverse.

6.2.3 Types of network services

We characterize the types of services available in home networks. Although users may access some devices directly (for instance, access a printer via its USB port), we only focus on services that are available via the home network. HomeNet Profiler collects the list of services advertised via both UPnP and Zeroconf. Although we study extensively UPnP in home gateways in Section 6.1, more devices support UPnP. This section studies any type of UPnP services. Note that the service scan module in HomeNet Profiler does not verify whether the service is actually implemented. An exhaustive verification may look like a network attack, especially for users who run HomeNet Profiler in a company or a university network.

We have 2,378 reports from distinct homes for the service scan module. We find devices that advertise any type of UPnP services in 1,226 homes and Zeroconf services in 477 homes. The number of homes with at least one Zeroconf device is low, because we could not find the Zeroconf library in 1,709 homes (mainly on Windows machines). In the remaining 192 homes, HomeNet Profiler found no Zeroconf services in the home network. Although we ship the UPnP library with HomeNet Profiler, there are some cases where we cannot find UPnP-enabled devices, because the configuration of the end-host blocks the queries (as discussed in Section 4.1.3). Moreover, in the service scan module we use the UPnP wildcard query to find any UPnP service available. Some devices may implement UPnP, but not answer the wildcard queries as we see Section 6.1.

Irrespective of the cause, the fact that we can only discover the available services automatically with UPnP in approximately 50% of the homes and in less than 25% of homes for Zeroconf shows that the adoption of these services is moving slowly. For the automatic discovery and configuration of services to work both the device offering the service and the end-host have to support the protocol. In all the cases where we have no UPnP nor Zeroconf, we can safely infer that the particular end-host we measured from would not be able to access these services.

Next, we examine the types of UPnP and Zeroconf services we find for the homes where our measurements were successful. We find 205 different services via Zeroconf and only 39 via UPnP. Table 6.6 presents the top-ten UPnP and Zeroconf services. Many popular Zeroconf services are specific to Apple (for example, Apple File Sharing, Sleep Proxy, and Airport). This result is not surprising because Apple started Zeroconf. Other popular Zeroconf services are remote access services (SSH and Remote Frame Buffer) and services to share printers (IPP) or files (SMB, SFTP, and DAAP). HTTP is also used for sharing personal web pages in MacOS.[1] UPnP is mainly used for advertising devices such as Internet gateways, media servers, and WiFi access points.

[1] http://docs.info.apple.com/article.html?path=Mac/10.5/en/8236.html

Rank	Zeroconf	UPnP
1	Apple File Sharing (47%)	Internet Gateway Device (47%)
2	HTTP (36%)	Media Server (29%)
3	SMB (35%)	WiFi Alliance Device (8%)
4	Sleep Proxy (27%)	Media Renderer (5%)
5	IPP (26%)	Printer (2%)
6	SSH (26%)	Set Top Box (2%)
7	SFTP (26%)	Remote UI Server Device (1%)
8	RFB (25%)	Basic (1%)
9	Airport (24%)	WiNAS (1%)
10	DAAP (21%)	Synchronization Server (1%)
Homes	571	1362

Table 6.6: Most frequent Zeroconf and UPnP services.

6.3 Residential WiFi networks

This section first describes how to interpret HomeNet Profiler WiFi measurements and then presents our findings on the density of the WiFi neighborhood of home networks, the received signal strength of home WiFis vs neighbor WiFis, and on WiFi communities in France. We will use WiFi communities in Chapter 7 to help diagnose high losses and delays.

6.3.1 Methodology

HomeNet Profiler successfully collects WiFi results in 1,313 homes. The machine running HomeNet Profiler had a WiFi network interface in only 1,645 homes. Other end-hosts either do not have a WiFi interface or lack support from the OS to run the WiFi scan. Further, some WiFi access points may broadcast ESSID-BSSID pairs for more than one network, for example, a guest network. In addition, WiFi access points often create a virtual BSSID for each of the ESSIDs they announce. Consequently, HomeNet Profiler cannot tell which ESSID-BSSID pairs originate from the same WiFi access point. In our analysis, we consider that all ESSID-BSSID pairs other than the home WiFi are neighbor WiFis. In total, aggregating home and neighbor WiFis, we study 8,405 distinct ESSID-BSSIDs (i.e., those for the home WiFi plus those for neighbor WiFis). We find only 8,116 distinct BSSIDs because some access points use BSSIDs that are not universally unique. The number of unique ESSIDs is even lower (only 5,505 distinct ESSIDs), which implies that many WiFi networks have the same name (e.g., ‘NETGEAR’ or ‘linksys’) or WiFi communities such as ‘FreeWifi’.

Country	Channel						Total
	1	2 to 5	6	7 to 10	11	12plus	
France	19%	8%	18%	10%	40%	5%	4573
USA	21%	11%	27%	8%	26%	0%	739
Canada	14%	13%	26%	15%	29%	0%	261
UK	30%	5%	24%	7%	28%	3%	170
Brazil	20%	11%	32%	18%	16%	0%	166
Italy	35%	5%	27%	1%	25%	2%	121
Germany	34%	9%	17%	18%	15%	7%	82
Overall	21%	9%	20%	10%	34%	4%	7745

Table 6.7: Percentage of ESSID-BSSIDs on each channel for the 2.4 GHz band.

6.3.2 WiFi neighborhood

We find only 4% of home WiFis that operate on the 5 GHz band. Either the home WiFi operates only on the 2.4 GHz band or end-hosts lack support for 5 GHz. Since we cannot disambiguate these two possible outcomes, our results are not representative of the actual use of 5 GHz band. We focus our results on the 2.4 GHz band. When two neighbor WiFis operate on the same or close channels, they might interfere. We say that two neighbor ESSID-BSSID pairs are *overlapping* if they are on channels where numbers differ by 4 or less. The worst situation happens when ESSID-BSSID pairs are on the same channel.

Table 6.7 presents the percentage of ESSID-BSSID pairs on each channel in the 2.4 GHz band. This band contains 14 channels. Channels 1, 6, and 11 are the non-overlapping channels in the 2.4 GHz band and hence are recommended for use. We merge other channels for the 2.4 GHz band into ranges. In our measurements, 19% of the ESSID-BSSID pairs operate on non recommended channels. We also notice a predominance of ESSID-BSSID pairs on Channel 11 in France . Our analysis of the vendors of the access points in France shows that some specific ISP-provided access points use channel 11 by default. We believe that these ISPs should upgrade their access points so that they can perform better channel selection.

WiFi neighborhoods are generally crowded. Figure 6.5 plots the cumulative distribution of the number of neighbor ESSID-BSSID pairs across all measured homes. We present three distributions: for all neighbor WiFis; for ESSID-BSSID pairs that overlap with the home WiFi; and for ESSID-BSSID pairs on the same channel as the home WiFi. Overall, the number of ESSID-BSSID pairs of the WiFi neighborhood varies considerably across homes (from 1 to 54 neighbor WiFis) and more than 75% of homes

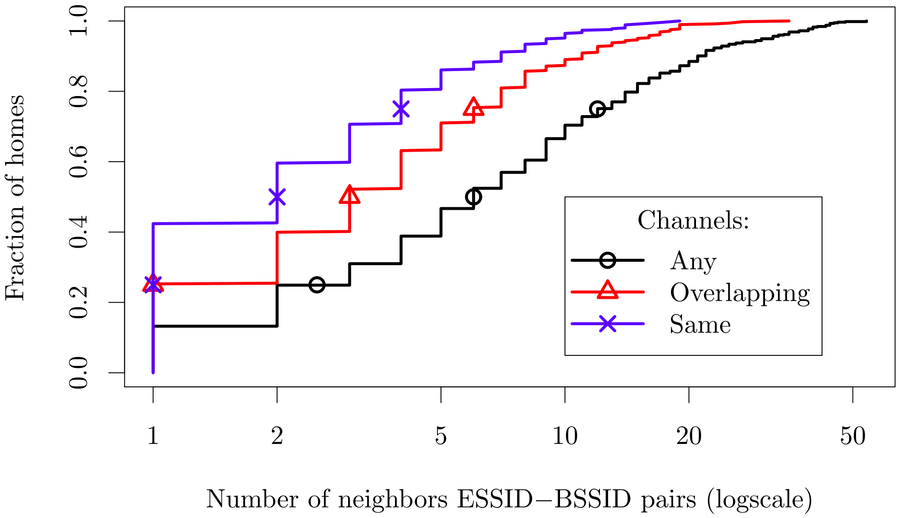


Figure 6.5: CDF of the number of neighbor ESSID-BSSID pairs

have at least one overlapping WiFi neighbor. The actual number of WiFi neighbors is likely larger because HomeNet Profiler misses some WiFi neighbors with low RSSI.

6.3.3 WiFi received signal strength

The quality of the home WiFi also depends on the strength of the received signal. Since end-hosts have different WiFi adapters, their RSSI measurements are not directly comparable. Thus we only compare RSSIs of different ESSID-BSSID pairs measured on the same end-host rather than comparing RSSIs taken from different end-hosts. We compare the RSSI of home WiFi to the RSSI of neighbor WiFis using the *RSSI-rank* metric, which we define as the index of the home ESSID-BSSID pair in the ordered list of ESSID-BSSID pairs according to RSSIs. A home ESSID-BSSID pair has a RSSI-rank of one when the home ESSID-BSSID has the highest RSSI in the WiFi scan. We have high confidence on the RSSI-rank measurement because our six-homes testbed validation shows that we always observe ESSID-BSSID pairs with strong RSSI and here we are only studying the strongest ESSID-BSSID pairs. Home WiFi access points that also broadcast a guest network (e.g., a WiFi community) may bias the RSSI-rank because both the home WiFi and the guest network will have similar RSSI. In France, we compare the RSSI-rank with and without WiFi communities.

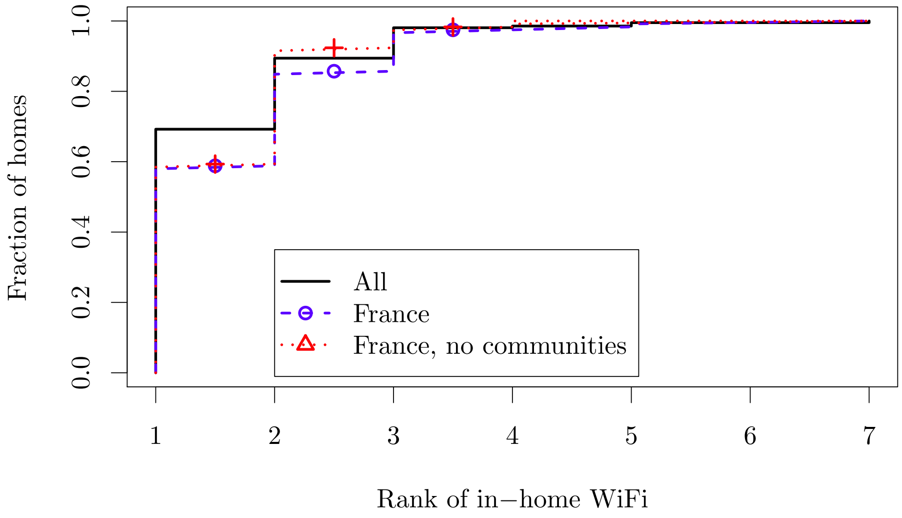


Figure 6.6: CDF of the rank of home RSSI

Figure 6.6 presents three cumulative distributions of RSSI-rank: one across all homes, one for homes in France counting all neighbor ESSID-BSSID pairs and one obtained by removing ESSID-BSSID pairs of known French WiFi communities. We only consider ESSID-BSSID pairs on the same channel as the home WiFi. In general, the RSSI-rank of the home ESSID-BSSID is small: 95% of homes have an RSSI-rank of at most three when considering only the same channel as well as considering overlapping channels. Most end-hosts run HomeNet Profiler closer to their home WiFi access point than to neighbor WiFis however, more than 34% of the home WiFis rank worse than one neighbor WiFi on the same channel. This percentage increases to 42% when considering overlapping channels.

In France, WiFi communities explain part of this phenomenon: the fraction of homes where the home WiFi ranks first increases from 0.57 to 0.87 on the same channel after removing the eight WiFi communities we identify in the next section. Only 8% of the end-hosts running HomeNet Profiler receive a stronger signal from a neighbor WiFi than from their home WiFi on the same channel. The same value increases to 14% for overlapping channels.

6.3.4 WiFi communities in France

We now study WiFi communities in France. Most major access ISPs in France deploy a WiFi community, where customers of an ISP receive credentials to connect to WiFi access points of other customers of that ISP. Hence, customers can benefit from "free" WiFi access in most of France. We first examine the prevalence of different WiFi communities; we then present results of a focused experiment where we test which set of diagnostic measurements the two most common WiFi communities allow.

Prevalence

We evaluate the prevalence of WiFi communities with the data from the 710 homes in France with successful WiFi results. In particular, we study the most common WiFi communities in France: 'FreeWifi', 'FreeWifi_secure', 'freephonie', 'orange', 'Bouygues Telecom WiFi', 'Neuf WiFi', 'SFR WiFi Public, and 'SFR WiFi Mobile'. Freephonie, FreeWifi, and FreeWiFi_secure are three communities of the same ISP called Free. Freephonie and FreeWiFi_secure only share the access link for phones whereas FreeWifi provides Internet service. Similarly, SFR WiFi, SFR WiFi Mobile, and Neuf WiFi belong to SFR. We refer to access points advertising one of the WiFi communities as *community access points*.

Figure 6.7 plots the cumulative density function of the number of community access points observed per home. We present three curves: 'Any community' corresponds to the total number of community access points each home observes; 'Home ISP communities' only counts community access points advertising the WiFi community of the home ISP; and 'Other ISP communities' counts all community access points, except those corresponding to the home ISP. We distinguish the communities of the home ISP from others because we cannot directly identify if home users running HomeNet Profiler has enabled the WiFi community in their access point. Thus, in the 'Any community' and 'Home ISP community' curves we may be counting the home access point itself, which wouldn't help in neighbor-assisted diagnosis. The 'Other ISP community' curve represents a lower bound on the number of community access points that one could potentially use for neighbor-assisted diagnosis.

Figure 6.7 shows that HomeNet Profiler observes community access points in 62% of all measured homes in France and even if we only consider other ISP communities we observe at least one community access point in approximately half of the measured homes. The number of community access points per home presents strong linear correlation with the total number of neighbor access points (0.93). Intuitively, denser

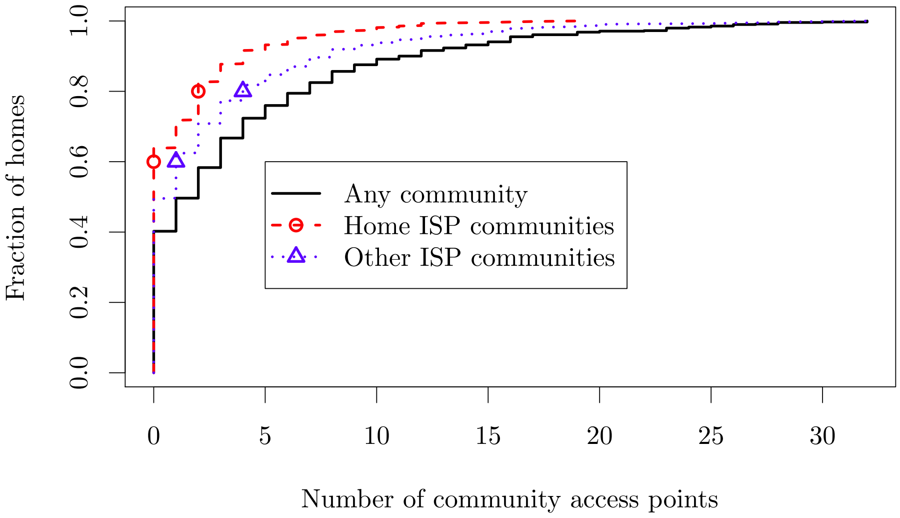


Figure 6.7: Cumulative density function of community access points per home in France

WiFi neighborhoods are more likely to have more access points enabled to participate in WiFi communities as well. This large fraction of community access points suggests that neighbor-assisted diagnosis could be performed today in many French homes.

Measurement capabilities

We next consider to which extent the two most prevalent WiFi communities support network measurements. The two most prevalent WiFi communities in the HomeNet Profiler data are FreeWifi and SFRWifi. ISPs restrict the type of traffic and bandwidth used by guest hosts connected to a community access point. Thus, a community access point is not necessarily a candidate vantage point for issuing network measurement.

We determine the measurement capabilities of FreeWifi and SFRWifi (i.e., which kinds of measurements can a guest host perform when connected to these community access points) from two homes in Paris. From each home we connect to different FreeWifi and SFRWifi access points. We use Netalyzr [94] to perform a complete test of the capabilities of each community access point. We repeat each test twice and found that our results are consistent over time.

Community	Test	Comments
FreeWifi	IP	Public IP or Private IP
	Protocols	All protocols allowed (public IP) No DNS to arbitrary servers (private IP)
	Ping	Allowed
	Traceroute	Allowed
	Download	Shaped at 1 Mbps
	Upload	Not Shaped
SFRWifi	IP	Private IP, no port forwarding
	Protocols	Only: DNS, HTTP, HTTPS, SSH, SIP
	Ping	ICMP to the gateway only
	Traceroute	ICMP blocked after the gateway
	Download	Not shaped
	Upload	Shaped at 256kbps

Table 6.8: Measurement capabilities of WiFi Communities

Table 6.8 summarizes the measurement capabilities of FreeWifi and SFRWifi. On FreeWifi, the guest host obtains a public IP address half of the time. Otherwise, the guest host obtains a private IP address. We didn't identify patterns that might explain when the guest host receives a public or a private IP address. When receiving a public IP address, the guest is able to receive incoming connections, can perform *Traceroute*, and experiences no port-based protocol filtering. When the guest host obtains a private IP address on FreeWiFi, however, it cannot send UDP probes to arbitrary IP Internet addresses. On FreeWifi, the guest host bandwidth is capped at 1 Mbps for download; the upload bandwidth is not capped (it is hence limited by the WiFi connectivity and the access link). Although we didn't identify any pattern of bandwidth shaping over SFRWifi, a guest host connected to SFRWifi has many more limitations than when connecting with FreeWifi. The guest host can only obtain a private IP address and hence it cannot easily receive incoming connections. In addition, SFRWifi filters many protocols. For example *Traceroute* is blocked past the SFRWifi access point (i.e., the guest host only receives the response for the first hop; no other responses are forwarded to the guest host).

6.4 Summary

This chapter provides a characterization of home networks. We show the potential of UPnP as a tool to complement end-host measurements in home networks. UPnP queries can determine the ground-truth access link capacity, pinpoint cross-traffic from the home network, differentiate local from wide-area losses, and identify gateway characteristics per model (as we did for the buffer size). The caveat is that in the majority of homes in our datasets, end-hosts fail to discover an UPnP gateway. To make matters worse, UPnP gateways respond with answers that are sometimes hard to interpret and other times simply wrong.

Our characterization of devices at homes shows that home networks generally connect less than a dozen of devices. Further, only a small fraction of these devices are on at a given time. We find that the total number of devices in home networks correlates moderately with the number of members of the household. The complexity of home networks arise from the heterogeneity of device vendors and the limited support for autoconfiguration protocols like Zeroconf or UPnP.

WiFi scans collected in more than 1,313 end-hosts show that the WiFi neighborhoods also vary considerably from one home to another. The number of neighbor ESSID-BSSID pairs varies from 1 to 54. We find that 14% of the end-hosts from France detect a neighbor WiFi with a signal stronger than the home WiFi on an overlapping channel. In areas with dense WiFi networks, neighbor WiFis could also serve as backup connectivity or as extra vantage points to perform measurements. A way to access these neighbor WiFis are WiFi communities. In France, more than 60% of the end-hosts detect WiFi communities. We evaluate how two of these WiFi communities (FreeWifi and SFRWifi) can support measurement studies. FreeWifi permissible policies when hosts obtain a public IP address are ideal for running network measurements; but we can also use SFRWifi and FreeWifi with private IP address as long as we can adapt our probing techniques to work under the constraints of the policies of the WiFi communities.

The next chapter uses WiFi neighbors to introduce the concept of neighbor-assisted diagnosis and we leverage WiFi communities in France as prototyping and evaluation platforms.

Chapter 7

Neighbor-Assisted Network Diagnosis

This chapter builds on the idea that an end-host can leverage neighbor WiFis to diagnose home networks. A home user may be able to access the Internet not only through its contracted ISP, but also through separate and distinct (typically wireless) networks. Hence, a end-host connecting to a neighboring home network via wireless benefits from a second vantage point "for free" and which is useful for troubleshooting. For example, if the neighbor home network has a different ISP than the home network, one can detect if an outage is limited to a single ISP or not. Another use for a second vantage point is to send probes between the two interfaces, such that we can infer one-way properties of the access link. We call such techniques *neighbor-assisted network diagnosis*.

In this chapter, we explore neighbor-assisted network diagnosis where an end-host sending probes between a network interface attached to the home network and another interface attached to a neighbor network. We develop techniques to measure the latency and the transmission rate of the home network and of the access links. For each of these two metrics, we study the equation system arising from the analysis of the measurements that the end-host can perform. We discuss the hypothesis needed to solve these equation systems.

We evaluate our techniques with both controlled experiments and real-world experiments. Our testbed for controlled experiments includes a DSLAM access network and multiple Ethernet home networks. Here, we introduce artificial delays and losses in the home network as well as in the access network. We verify that our techniques

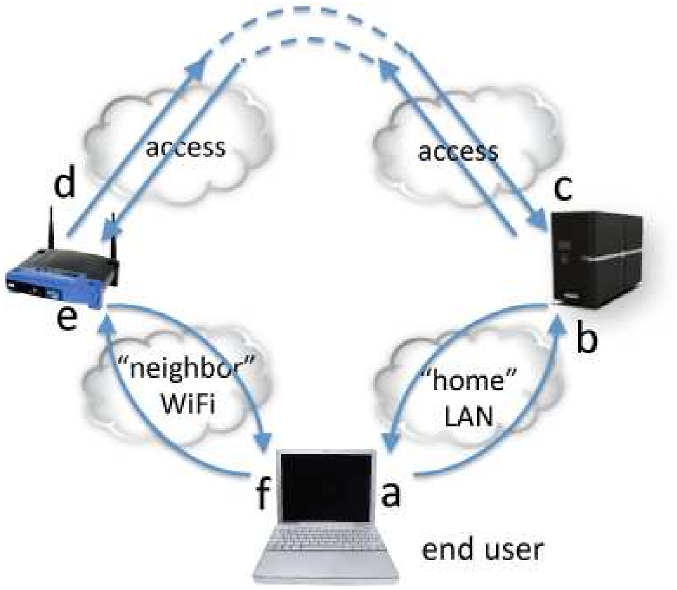


Figure 7.1: Notations for NADD

are able to detect and distinguish the delays/losses occurring in each of the segments, and the upstream/downstream direction in which these delays occur.

Our real-world experiments re-use our six-home testbed of six laptops with which we evaluated HomeNet Profiler (Section 4.2.2). We leverage FreeWiFi and SFR WiFi communities to connect to neighbor networks. Neighbor-assisted diagnosis is also applicable when neighbor WiFi access is available through other means (e.g., when neighbors exchange their WiFi password or in presence of open WiFi networks). Our results from this deployment indicate that neighbor-assisted network diagnosis delivers accurate results and can be deployed in real homes today.

7.1 Network settings

The network setup used throughout this chapter is the following. Each end-host is connected to two distinct networks through two different network interfaces (one typically being its own home network, and one being a neighboring wireless network).

Figure 7.1 illustrates our network setting. A user has a primary connection to the Internet through its home network. An interface on the end-host (labeled a in Figure 7.1) connects via its home network to an interface on its home gateway router (b) which then connects via interface c to the access network and from there to the larger Internet. A user experiencing congestion (e.g., as manifested in high delay) is interested in *where* this delay occurs - is the delay in the home network or in the access network, and does this delay occur in the upstream or downstream direction? The user's ISP is also interested in this information, particularly when the user calls the ISP to report poor performance and to demand a diagnosis.

In order to perform this diagnosis, neighbor-assisted network diagnosis leverages the fact that a WiFi neighbor with Internet connectivity is available. In this case, the end-host connects via interface f to interface e in the neighbor network, and from there to the larger Internet. Neighbor-assisted network diagnosis requires the ability to send packets from interface f to interface a. Hence, both interfaces must be connected at the same time. As discussed in Chapter 6, this second connectivity is often available (particularly in urban settings) when a user has access to a WiFi community network. The home network itself may be wired or wireless although in the wireless case, the user would require two separate wireless network interfaces to run test (which is not often available). For simplicity and maximal applicability, we consider here the case where the a-to-b network is wired Ethernet and the f-to-e network is wireless. However, the general techniques behind neighbor-assisted network diagnosis are independent of connectivity type.

We next study how to measure delays in the framework of neighbor-assisted network diagnosis.

7.2 NADD: neighbor-assisted delay diagnosis

We describe NADD: neighbor-assisted delay diagnosis. NADD allows the user to determine not only where the delays occur (e.g., in the home network or in the access network) but also whether those delays are experienced in the upstream or downstream direction. We then present our evaluation method and our evaluation results.

7.2.1 Analysis and implementation

We begin by describing a simple (but as we will see, often inaccurate) ping-based approach for pinpointing the location of delay. We then describe NADD, discuss the technical challenges when implementing this approach, and detail our measurement implementation.

Estimating delays via landmark pings

Perhaps the simplest way to estimate delays is to use a tool such as $traceroute$ or $ping$ or their variants to measure the round-trip delay from the end user to a landmark and assume that delays in the upstream and downstream directions are symmetric. Using this technique, for example, the user can ping the path aba and measure the round trip delay $\hat{d}_{aba}$. Here we use the hat notation to indicate a measured value and use the subscript to indicate the path measured. Assuming symmetric upstream and downstream delays, i.e., that the a-to-b delay, denoted d_{ab}, equals the b-to-a delay, d_{ba}, these delays are then simply estimated as $d_{ab} = d_{ba} = \hat{d}_{aba}/2$. Given the estimates $\hat{d}_{aba}$, the user can then measure $\hat{d}_{abcXcba}$, where X is a next-hop router or another landmark, and assuming $d_{cX} = d_{Xc}$, can estimate $d_{cX} = (\hat{d}_{abcXcba} - \hat{d}_{aba})/2$.

Neighbor-assisted delay diagnosis

NADD exploits the fact that hosts with two network interfaces have a cyclic topology with three segments (six directional segments, ab, cd, ef, fe, dc, ba), as shown in Figure 7.1, and can send probe/measurement packets from one interface to another through these segments.

Given the ability to send probe/measurement packets along a directional path (e.g., along path $abcdef$), it is tempting to use IP timestamp options to directly measure directional delays at each hop along the path. Prior studies [41,140] document the relatively sparse implementation of IP timestamp options in wired backbone routers, particularly when the option request is to record a timestamp at a given IP interface en route to a final destination. Indeed, our own measurements (see Table 7.2 in Section 7.2.3) indicate that fewer than 10% of the packets sent along the cyclic path $abcdef$ or $fedcba$ in five different home network settings actually completed the cycle with the requested timestamp. Thus, the use of timestamps for delay diagnosis in edge networks appears even more problematic than (the already rather bleak situation) in wired backbone networks.

Given that individual, per-hop delays are not directly measurable with IP timestamp options, is all hope lost of determining these per-hop delays and thus pinpointing and diagnosing delays? Fortunately, the answer is no! NADD provides a methodology for measuring round-trip and cyclic delays in a setting such as Figure 7.1, and then *inferring* these per-hop delays.

NADD Delay measurements and per-hop delay inference

Let's again consider the setting in Figure 7.1. Although individual per-hop directional delays can not be directly measured by the end-host, the host can make a number of useful measurements:

- **RTT estimates to local gateway interfaces, via ping.** The host can individually ping interfaces b and e, obtaining measurements $\hat{d}_{aba}$ and $\hat{d}_{fef}$.
- **RTT estimates to the public (i.e., Internet) interface of the local gateway via ping.** For example, to ping the public interface of the home network gateway, a ping can be sent via the community WiFi interface along the path $fedc$, yielding the RTT measurement $\hat{d}_{fedcdef}$. Note that to do this, the end user must first discover the IP address of interface c.
- **Clockwise and counter-clockwise full cycle probes.** The host can send *itself* a probe message that traverses a cycle (either clockwise or counter-clockwise) beginning and ending at the host itself. For example, by sending a probe on outgoing interface a addressed to its own interface f, the host can directly measure the counter-clockwise cyclic *one way* delay $\hat{d}_{abcdef}$. The clockwise cyclic delay $\hat{d}_{fedcba}$ can similarly be measured.

As we discuss in Section 7.2.3, these measurements can vary even in short periods of time. Hence, we estimate these values by sending a train of probes and taking the minimum value. Note that in each of these cases, the measured multi-hop delays are composed of various combinations of the (unknown) per-hop delays $d_{ab}, d_{ba}, d_{cd}, d_{dc}, d_{ef}$ and d_{fe}. Given the topology in Figure 7.1, these relationships can be represented by the following system of linear equations:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} d_{ab} \\ d_{ba} \\ d_{cd} \\ d_{dc} \\ d_{ef} \\ d_{fe} \end{pmatrix} = \begin{pmatrix} \hat{d}_{aba} \\ \hat{d}_{abcdcba} \\ \hat{d}_{fedcdef} \\ \hat{d}_{fef} \\ \hat{d}_{abcdef} \\ \hat{d}_{fedcba} \end{pmatrix} \tag{7.1}$$

This system of six equations has six unknowns. Unfortunately, the rank of the matrix is four. In order to solve this system, we will thus need either to reduce the number of unknowns or to increase the number of equations. One way to do this is to *assume* symmetric delays in the local networks (i.e., $d_{ab} = d_{ba}$ and $d_{fe} = d_{ef}$). Prior work [147] shows that this assumption is reasonable unless many WiFi nodes use VoIP at the same time; moreover, local network delays are typically smaller than access network delays given link transmissions speeds. We do not assume that access links are symmetric, as this is generally not the case with residential Internet connection. Assuming symmetric local network delays reduces the number of unknowns to four, yielding six measurement equations with now four unknowns.

With more equations that unknowns, we now have a choice of which set of measurement equations to use. One reduction uses both one-way measurements (i.e., $\hat{d}_{abcdef}$ and $\hat{d}_{fedcba}$):

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} d_{ab} \\ d_{cd} \\ d_{dc} \\ d_{fe} \end{pmatrix} = \begin{pmatrix} \hat{d}_{aba} \\ \hat{d}_{fef} \\ \hat{d}_{abcdef} \\ \hat{d}_{fedcba} \end{pmatrix} \tag{7.2}$$

A second reduction uses an RTT measurement to a public gateway interface instead of a one-way cyclic delay measurement. Specifically, replacing the last equation above yields:

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} d_{ab} \\ d_{cd} \\ d_{dc} \\ d_{fe} \end{pmatrix} = \begin{pmatrix} \hat{d}_{aba} \\ \hat{d}_{fef} \\ \hat{d}_{abcdef} \\ \hat{d}_{fedcdef} \end{pmatrix} \tag{7.3}$$

Depending on which equations are actually used to solve for these four unknowns, NADD will give slightly difference performance estimates, a topic we'll investigate in detail in Section 7.2.3.

Measurement implementation

Network address translators (NATs) significantly complicates our measurement technique. End-hosts generally receive a private IP address (for example, in the 192.168/16 sub-network) and connect to the Internet through a NAT. End-hosts must first discover the public IP addresses of the gateways before probing the gateways. We gather the public IP addresses of home gateways with the support of a remote web server that returns the requesting-IP-address of a web client. Hence, a web client behind a NAT, can retrieve its public IP address, which can then be used in issuing the four ICMP ping measurements to the home gateways.

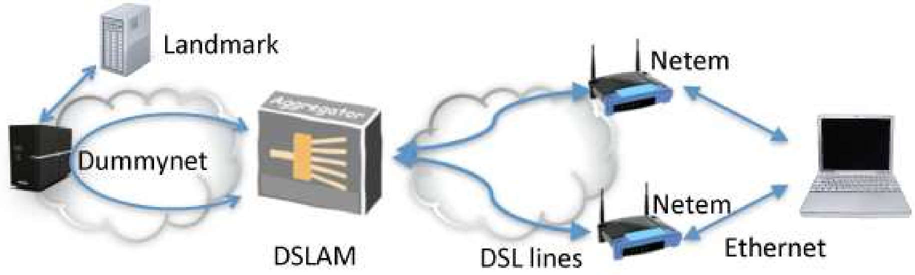


Figure 7.2: Testbed for controlled experiments

NAT also introduces complications into the one-way cyclic delay measurements. Here, the problem is that a NATed host must be able to *receive* packets on one of its interfaces. In order for the incoming measurement packets to punch through the NAT, the NAT must support port mapping for incoming packets. To accomplish this, NADD automatically configures a port-mapping between a port on the home gateway and a port on the measurement laptop using UPnP; NADD accomplishes this without user-intervention. Our deployment maps port 53 (DNS) because both FreeWiFi and SFR WiFi allow UDP packets to be sent to this port. We have found that the community access points do not support UPnP port-mapping. Consequently, we can only initiate cycle measurements from the WiFi interface in a clockwise direction in Figure 7.1. Our measurement implementation requires little support from the home gateways. Both gateways must reply to ICMP pings and the home gateway must support port-mapping configuration via UPnP.

We next evaluate our delay identification technique with controlled experiments and with a prototype deployment.

7.2.2 Evaluation method

This section describes our method to evaluate NADD. We combine controlled experiments using a testbed that emulates home networks connected to one residential access ISP with a deployment in five homes in Paris. The controlled experiments allow us to evaluate the accuracy of our delay inferences under different scenarios, whereas the deployment allow us to experiment with real delays and delay variations.

Controlled experiments

Testbed We setup a fully-controlled testbed that emulates two home networks connected to an access ISP (one home network represents the home where our measurement host is connected to and the other represents the neighbor). Figure 7.2 illustrates our testbed. We emulate the gateways of each of the homes with two Linux computers each with an ADSL interface to emulate the access link and an Ethernet interface to emulate the home network. The measurement host, which is another Linux computer, connects to both gateways over Ethernet. Even though in the real-world deployment the link between the host and the neighbor gateway will be a wireless connection, we connect the measurement host to the neighbor gateway using Ethernet to have better control of the measured and introduced delays. We add delays in the home network with $netem$ running on each gateway. The ADSL interface is connected to an ADSL2+ DSLAM. Each home gateway sets up an Internet connection with PPP over an Ethernet tunnel over ATM to a FreeBSD server. This server runs $dummynet$, which allow us to introduce delays on the access link.

Parameter settings We can add delay to the access link and the home network in each direction independently, giving us four parameters to set. We have two choices for each parameter. For the home network, we add either 0 or a constant 30 ms delay; for the access link, we add either 0 or a constant delay of 100 ms. We pick 30 ms and 100 ms to validate our techniques because these values are large compared to typical delays inside the home network or in access links, respectively. Our goal is to evaluate whether our techniques can accurately infer the delays in the home network and the access link in each direction both in situations when delays in a given link are symmetric and not. Sweeping all the settings for these four parameters leads to a total 16 test scenarios. We run each scenario 100 times.

Error metric For each scenario, we know how much delay we are adding to each network segment as well as the *baseline delay*, which is the delay we infer for each network segment in the scenario where we add no delay. The baseline delay for a network segment plus the added delay represents the ground truth. We can then obtain the absolute error of each technique by subtracting the ground truth delay from the delay inferred by NADD. Netem and dummynet may introduce random errors when delaying each packet. Hence, our ground truth may have small errors. To account for this, we repeat each test 100 times and present the median absolute error out of the 100 runs.

Deployment

We also evaluate our techniques using a small-scale deployment. We re-use our six-homes testbed with which we evaluated HomeNet Profiler (Section 4.2.2). Recruiting volunteers in Paris is desirable because WiFi communities are particularly prevalent in Paris. We use a server at UPMC, which is also in Paris, to control the measurement hosts and collect measurement reports. The control server also assists measurement hosts to discover the public IP addresses of the home and the neighbor gateways. Each measurement host connects to neighbor access points advertising both FreeWiFi and SFR WiFi every ten minutes, not to overload the volunteer's network. We develop scripts to automatically log into the FreeWiFi and SFR WiFi authentication portals. The measurement hosts are configured with the credentials to connect to both of these WiFi communities.

For each successful connection to a WiFi neighbor, we perform a measurement round that consists of a number of tests with different parameters. Each test sends six trains of probes to estimate each of the six delays used in NADD in the following order: $\hat{d}_{fef}$, $\hat{d}_{fedcdef}$, $\hat{d}_{aba}$, $\hat{d}_{abcdcba}$, $\hat{d}_{fecdba}$, $\hat{d}_{abcdef}$. First, we send a train of probes back-to-back to estimate $\hat{d}_{fef}$, we wait up to five seconds to receive all the responses, then we send the next probe train to measure $\hat{d}_{fedcdef}$, wait up to five seconds, and so on. We configure probe trains with different types of probes, probe sizes, and number of probes per train. We set the number of probes in a train to either 3 or 20; and the probe size to 64 bytes (i.e., a small packet) and 1400 bytes (a large packet). We measure full cycle probes with UDP and RTT estimates with ICMP. For the full cycle probes, we measure with and without requesting the IP timestamp of the home gateway and the neighbor gateway. A measurement host first performs the test with eleven trains of small probes per delay measurement (ten trains of 3 probes and one of 20 probes), then eleven trains of large probes (again ten trains with 3 probes and one with 20 probes). We then run the same 22 trains with the IP timestamp request.

We run repeated measurement rounds from the five homes for nine days in July 2012. We collect a total of 408 measurement rounds in this period. Each measurement host successfully connects to between two and six different neighbor WiFi networks. The median duration of a single test is 12 seconds and 99th-percentile is less than 46 seconds (the tests take longer when the majority of probes times out). The median time of a measurement round is 510 seconds. What is important for us in practice is the time of a test, because this corresponds to the time NADD would take to perform all the necessary measurements. Here, we perform multiple tests in one round to evaluate which parameter settings will work best in real homes.

Added Delay	Technique	Error (ms)			
		Access		LAN	
		dc	cd	ba	ab
$ab = ba = 30$ ms	NADD	-0.1	-0.2	1.0	1.0
	Landmark	-0.3	-0.3	1.0	1.0
$cd = dc = 100$ ms	NADD	-0.9	-1.0	0.0	0.0
	Landmark	-0.7	-0.7	0.0	0.0
$ab = 30$ ms	NADD	15.4	-16.3	-13.9	16.1
	Landmark	-0.3	-0.3	-13.9	16.1
$cd = 100$ ms	NADD	-0.4	-0.3	0.0	0.0
	Landmark	-50.4	49.6	0.0	0.0

Table 7.1: Absolute error of NADD and landmark ping under symmetric and asymmetric delays

7.2.3 Evaluation results

This section first evaluates the accuracy of NADD with controlled experiments and then discusses how to address issues such as lost probes and measurement consistency that arise in real deployments.

Validation

We use the testbed described in Section 7.2.2 to evaluate NADD's accuracy in a fully controlled setting. We evaluate NADD using the five different possible reductions to the system of linear equations in Equation 7.1. Our results show that NADD infers the same delays for all reductions in all scenarios within a range of 5 ms. Given that the different versions of the equation system lead to similar results, we only present results using the system presented in Equation 7.2, which uses the two one-way cycle measurements.

Table 7.1 presents the median absolute error out of 100 measurements for NADD and landmark pings in four representative scenarios in our controlled testbed. Results for other scenarios are similar. During these controlled experiments, we add delays into network segments ab, ba, cd, dc (refer back to Figure 7.1 for a description of link notation). The first four rows in Table 7.1 correspond to cases where delays in the upstream and downstream direction of each link are symmetric, whereas the last four rows correspond to asymmetric delays in the LAN or the access link. We present the absolute error of NADD and landmark pings to estimate delays in the LAN (d_{ab} and d_{ba}) and in the access link (d_{cd}, and d_{dc}). When delays are symmetric, both landmark pings and NADD perform well. The absolute error is less than 1 ms in all cases in the first four rows of Table 7.1.

Not surprisingly, when we violate NADD's assumption of symmetric delays in the home network (row labeled ab = 30 ms), NADD performs poorly. The absolute error is approximately +/-15 ms for the access and the LAN. This error corresponds to half of the delay difference between the upstream and downstream directions of the LAN, so in networks with higher asymmetry we expect larger absolute errors. Landmark pings have the same +/-15 ms error in the LAN, but practically no error in the access.

We do not expect highly asymmetric delays to occur in practice in home networks, since these networks are implemented with Ethernet, WiFi, or Powerline, which have equal upstream and downstream capacity and high transmission rates. Even if WiFi contention or buffering at the end-host or gateway creates some asymmetry, in practice this asymmetry will be small. As we'll see in the next section, typical home network delays (or $\hat{d}_{aba}$) vary between 1 ms and 5 ms, while access network delays (or $\hat{d}_{abcdcba} - \hat{d}_{aba}$) are an order of magnitude higher. Hence, even if there is asymmetry in the home network, the absolute error should be small. We are currently investigating a method to detect that NADD's assumptions are violated. The idea is to perform NADD's inferences periodically and search for large (negative) variations in the time series of the inferred delay of each network segment. The inference of such a negative delay would indicate that our assumptions are likely violated.

NADD shines when delay asymmetry occurs in the access network (for example, when $cd = 100$ ms in Table 7.1). NADD infers correct delays with less than one millisecond of error. Meanwhile, the landmark ping technique incorrectly attributes half of the delay to each direction. We expect this scenario to be the most common in practice, because most residential Internet access plans offer higher downstream than upstream capacity and because buffering at the gateway (which can sometimes introduce seconds of delay [65, 94]) will affect access network delays rather than LAN delays.

The controlled experiments evaluate NADD's accuracy in an ideal case. In practice, however, NADD will experience measurement noise — instances when measurement probes are lost or when measured delays vary considerably between two consecutive probes. We study these issues in the next section.

Effects of measurement noise

To evaluate the measurement noise that NADD must handle in practice, we analyze the measurements obtained from our deployment described in Section 7.2.2. Our analysis of the different parameters of probe trains show that small probes (of 64 bytes) in

Probe type	Probed segments	Success rate
ICMP	fef	87 %
ICMP	aba	100 %
UDP	$fedcba$	67 %
UDP	$abcdef$	67 %
ICMP	$fedcdef$	27 % (62 %)
ICMP	$abcdcba$	66 %
UDP (timestamp)	$fedcba$	9 %
UDP (timestamp)	$abcdef$	9 %

Table 7.2: Probe success rates in the deployment

trains of three probes represent a good tradeoff between probing overhead and probe success rate. Hence, the rest of this section presents results for trains of three probes of 64 bytes. Our conclusions are similar with other parameter settings.

Probe success rate

Probes or their responses may be rate-limited, blocked, or lost in the network. Without valid responses to probes, NADD cannot infer delays. Table 7.2 presents the success rate of the six types of probes that NADD uses in 339 distinct measurement rounds. The names of probed segments are shown in Figure 7.1. We define the *success rate* as the fraction of transmitted probes for which the measurement host receives a response. We compute the success rate over thousands of probe trials for each measurement. ICMP probes measure round trip delays, whereas UDP probes measure one-way delays. Although we don't use probes with timestamps in NADD, we also present the success rate of these probes for reference.

The success rate depends on the probe type and the measured segment. Probes with timestamps are often dropped or blocked. Only 9% of the probes transmitted with timestamps yielded a response. As discussed in Section 3, this result prevented us from incorporating probes with IP-options timestamping in NADD. The most successful measurement is the ping to the home gateway ($\hat{d}_{aba}$). This result is expected given that measurement hosts are directly connected to their home gateway. Other measurements have success rates between 66% and 87% with the exception of the ping to the home gateway from the neighbor WiFi ($\hat{d}_{fedcba}$). Our inspection of the traces shows that this higher loss rates happen as a result of two independent issues: SFRWiFi blocks ICMP probes and one home gateway dropped all ICMP ping requests to its public interface. After removing these erroneous measurements, the success rate of $\hat{d}_{fedcba}$ is 62%.

These results suggest that NADD can already be applied in practice. Even though some of the probes are blocked in the deployment, NADD is still able to solve the linear equations in many cases, because it only requires four out of the six probes to be successful. Out of 339 measurement rounds, the measurement host has enough measurements to solve the linear equations in 178 measurement rounds. It has all the six measurements in 84 rounds. Moreover, these results only reflect the current configuration of these community access points. If NADD were to be widely deployed, ISPs would have incentives to configure their network policies to allow these types of measurement probes.

Consistency of measured delays

NADD assumes that different probes traversing a given network segment will experience the same delay. In practice, however, consecutive probes measuring the same set of network segments may lead to different delay estimates, because of transient congestion. We study the consistency of measured delays by computing the delay variability over a train of ten probes issued back-to-back to a given set of network segments. We define the *delay variability* as the delay difference between the probe in the train that inferred the maximum delay and the one that inferred the minimum delay. If the delays experienced at a set of network segments are consistent, then delay variability will be close to zero.

Figure 7.3 presents the cumulative density function of delay variability for three different sets of probed segments. The left-most curve corresponds to the LAN segment (aba). In approximately 80% of trains the delay variability in the LAN is less than 1 ms, and the maximum variability in the LAN is 6.5 ms. Under such consistent delays NADD's inference should be the most accurate. The two other curves, however, show that the delay variability in the WiFi ping ($\hat{d}_{fef}$) and the cycle ($\hat{d}_{fedcba}$) are rarely less than 10 ms. The delay variability in these two segments can be as high as 900 ms. The distributions of delay variability of the WiFi ping and of the cycle are strikingly close. This observation leads us to believe that most of the delay variability in our deployment happens in the WiFi segment.

The high inconsistency in different delay measurements of one given segment implies that we can not assume that different probes that traverse the same segment will experience consistent delays. To address this issue, NADD uses the minimum delay out of ten probes to populate the equation system. The minimum delay is usu-

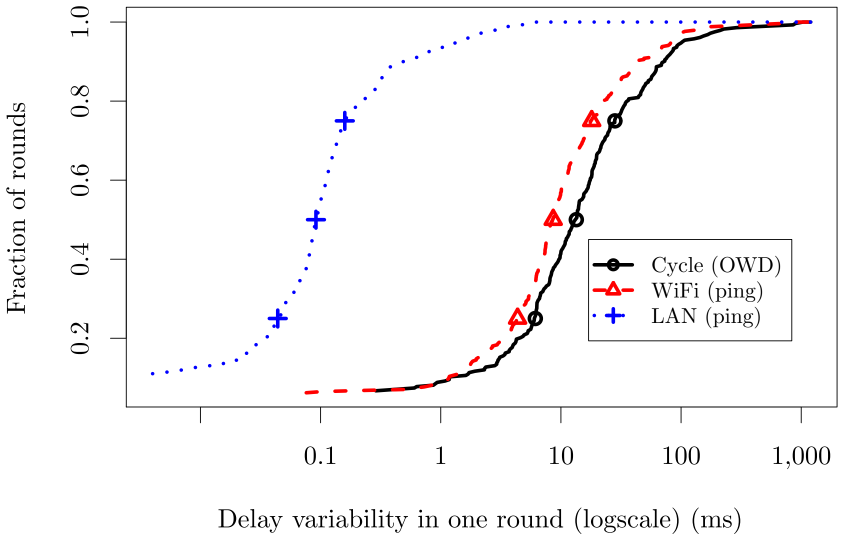


Figure 7.3: Delay variability in the deployment

ally more stable, because it avoids variability introduced by short-time-scale, transient congestion episodes.

Next, we study how the violation of the asymmetry assumption in the LAN or in the WiFi impacts the accuracy of NADD. Figure 7.4 shows the cumulative density function of raw estimates of $\hat{d}_{aba}$ (LAN), $\hat{d}_{fef}$ (WiFi), and $\hat{d}_{abcdef}$ (Access) using the minimum delay of ten probes. LAN delays are always below one milliseconds and hence can be neglected. The WiFi delay is larger. We notice two strong modes around 3 ms and 22 ms. These values most likely correspond to different WiFi rates. The measurement rounds in each of these two modes belong to measurement rounds on different neighboring WiFi networks, with different signal strength. Finally, the measurement crossing the access link range from 29 ms to 53 ms. These values are is in the same order of magnitude as WiFi delays with low signal strength. Hence, we conclude that the asymmetry in the WiFi or in the LAN should not introduce significant error, except when the end-host connects to a WiFi neighbor with a low signal strength.

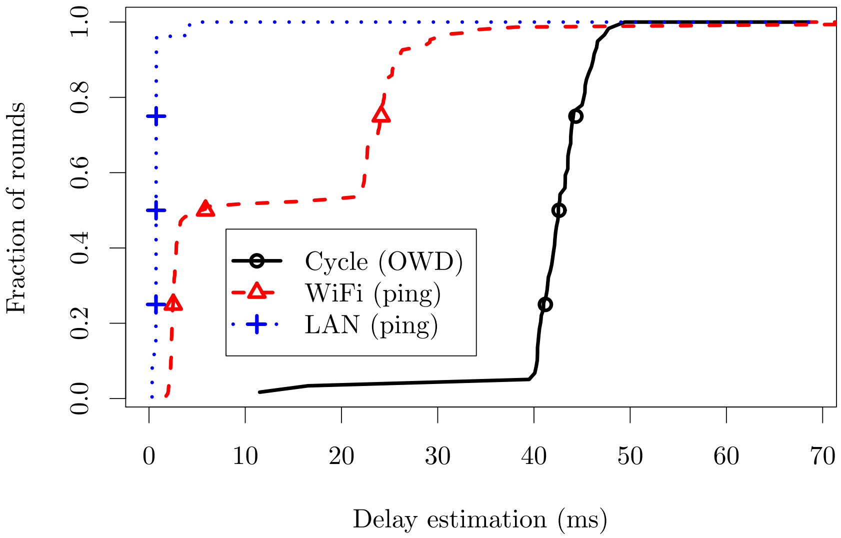


Figure 7.4: Raw delay estimations from measurements

Consistency of inferred delay

In 84 measurement rounds where we receive responses to all six measurements required in Equation 7.1, we infer delays of each network segment with each of the five possible reductions. We then compare whether the inferred delays of each network segment are consistent across the different reductions. We measure consistency with the delay variability computed as the delay difference between the maximum and the minimum inferred delay for a network segment out of the five inferred delays.

NADD's inferred delays are consistent in our deployment. All solutions infer the same value of d_{ab}, since the single measurement $\hat{d}_{aba}$ is itself sufficient to compute d_{ab}. The same argument applies to d_{ef}. The delay variability of d_{cd} and d_{dc} are strongly correlated (the Pearson coefficient of correlation is 0.94). The median delay variability of d_{cd} and d_{dc} is 1.7 ms and the 95th-percentile is 6.7 ms. In our dataset, we found only two distinct neighbor access points out of 10 where NADD inferred delays in the access segment with delay variability higher than 10 ms. These inconsistent delays indicate that inferences may be incorrect. We can avoid such inconsistencies by selecting only those neighbor access points with high signal strength. In our specific case, the measurement host indeed had other WiFi neighbors that delivered consistent results.

While delay is an important metric for troubleshooting end-to-end performance, applications also suffer from packet losses. We next apply a similar technique to pinpoint losses occurring close to the end-hosts.

7.3 NALD: neighbor-assisted loss diagnosis

We next present NALD, a neighbor-assisted network diagnosis technique to diagnose network losses which occur close to the end-host. NALD builds on the same idea as NADD, i.e., leverage a second vantage point to measure access link characteristics. We present NALD's equation system and we discuss the assumptions we use for NALD. We then describe our evaluation method for NALD and present our evaluation.

7.3.1 Analysis

We re-use the network settings from NADD. The main difference between NALD and NADD is that NALD measures losses on each paths instead of delays. Under the assumption that link loss rates on each segment are independent, link transmission rates (i.e., the complement of loss rates) multiply along a path. Hence, the logarithm of transmission rates accumulate along paths (like delays do) and we can use a system of equations analogous to NADD to compute the loss rate on each network segment. It is not clear whether or not the assumption that link loss rates are uncorrelated holds in practice. However, if loss rates are small, the error introduced by the correlation is negligible. We test whether the loss rates that we observe are correlated in our real-world evaluation.

Using a notation similar to the one for NADD, we note T_{ab} the transmission rate on the link between the interfaces a and b, and $\hat{T}_{aba}$ the overall transmission rate from a to b and back to a. We have $log(T_{aba}) = log(T_{ab}) + log(T_{ba})$ for strictly positive transmission rates. A transmission rate of zero means that there is no link between a and b. In practice, we observe transmission rates of zero for a perfectly-working link if the policy of the network is to block some probes (e.g., ICMP pings are blocked for SFR WiFi). Therefore, implementations of NALD must take these specific cases into account. The topology in Figure 7.1 yields:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} log(T_{ab}) \\ log(T_{ba}) \\ log(T_{cd}) \\ log(T_{dc}) \\ log(T_{ef}) \\ log(T_{fe}) \end{pmatrix} = \begin{pmatrix} log(\hat{T}_{aba}) \\ log(\hat{T}_{abcdcba}) \\ log(\hat{T}_{fedcdef}) \\ log(\hat{T}_{fef}) \\ log(\hat{T}_{abcdef}) \\ log(\hat{T}_{fedcba}) \end{pmatrix} \tag{7.4}$$

Like NADD's equations, NALD's equations are not linearly independent. Hence, we assume that loss rates are symmetric (or that the asymmetry is negligible) in the home and on the WiFi link to the neighbor home gateway. This assumption is reasonable for wired technologies such as Ethernet in the home network. However, some WiFi configuration may invalidate this assumption. An example of such a configuration is the hidden terminal effect, where two WiFi nodes can communicate with a same WiFi access point but where they cannot hear each other. In that case, the risk of collision is larger on the uplink than on the downlink. Under the symmetric loss rates assumption, we can reduce NALD's system of equation in Figure 7.4 to five reduced equation systems. Since NALD's matrix of equation is the same as NADD's matrix, the rank of the matrix is again four and the reduced equation systems for NALD are also the same as for neighbor-assisted network diagnosis. We next present our evaluation methodology.

One loss rate measurement consists of multiple probes. Each measurement will experience different realization of the loss process. Hence, even with a fixed link loss rate, variability in the measurement process will hamper the accuracy of NALD. Intuitively, to get the best estimate of loss rates, we should use as many measurements as possible. Since each reduced equation system for NALD uses only four distinct measurements out of six, we reduce the variability coming from the sampling process by averaging the inferred loss rates estimates for every reduced-equation system.

7.3.2 Evaluation method

We evaluate NALD with the same testbed and the same real-world deployment than NADD. We justify our loss rate estimation technique.

Loss estimation technique Measuring losses is more challenging than measuring delays. On one hand, we cannot directly estimate small losses with short probe trains like we did for delays. On the other hand, sending probes of back-to-back packets may generate self-induced congestion and hence bias loss rates estimations. We avoid these shortcomings by sending probes spaced in time according to a Gamma process.

Gamma processes estimates loss rates without bias and with low variance [11]. We estimate delays, both in the controlled experiments and in the six-homes testbed, with 300 probes of 64 bytes. Delays between two probes follow a Gamma process of shape 14 and a scaling factor such that we send packets at a mean rate of 2 packets per second. Thus, a measurement of a single path (e.g., $\hat{T}_{abcdef}$) takes around two and a half minutes.

Controlled experiments We study NALD results for various loss rates in different links of the testbed. We tune our experiment to the case where there is a significant amount of losses. When we add losses on a WiFi link (symmetric or not), we add 20% of losses; whereas we add 10% of losses on the access link (symmetric or not). We execute one repetition of NALD for each scenario. We otherwise assume that there is no loss on the link (i.e., the loss rates that we inject are the ground truth). Under this assumption, we can directly compare the inferred loss rates to the ground truth with no baseline measurements.

Correlation of loss rates in the deployment We verify whether NALD's assumption of independence between link loss rates are reasonable. We cannot observe all links independently, however we can study the correlation between loss rates of the measurement probes. We use the Pearson coefficient of correlation as a measure of correlation between loss rates. Probes may be lost because of a broken link or because of policies. These losses are measurement artifact and may bias the computations of loss rates. Hence we remove all occurrences where all packets for a given probe are lost. In our evaluation, this constraint limits our evaluation of NALD to the FreeWiFi WiFi community. After removing these lost probes due to broken link, we compute the full correlation matrix of loss rates of different probes.

We next present our NALD evaluation results.

7.3.3 Evaluation results

We first verify that the loss rates inferred in our controlled experiments match theoretical results. Second, we verify that the loss-rate measurement of NALD probes are not correlated in our six-homes testbed. Finally, we study where NALD infers losses in the wild.

Controlled experiments

We compare NALD to a solution with landmark pings in four representative scenarios similar to our analysis on delays. Table 7.3 presents the absolute error for a realization

Target Losses	Technique	Error (percentile points)			
		Access		LAN	
		dc	cd	fe	ef
$fe = ef = 20$ %	Landmark	-1.4	-1.4	0.8	0.8
	NALD	1.0	-1.5	0.8	0.8
$cd = dc = 10$ %	Landmark	0.1	0.1	0.0	0.0
	NALD	0.0	0.0	0.0	0.0
$fe = 20$ %	Landmark	-0.1	-0.1	9.9	-10.1
	NALD	-11.3	10.1	9.9	-10.1
$cd = 10$ %	Landmark	-5.1	4.9	0.0	0.0
	NALD	0.0	0.2	0.0	0.0

Table 7.3: Absolute error (in percentile points) of NALD and landmark ping under symmetric and asymmetric loss rates

of NALD and a realization of landmark pings with 300 packets per loss-rate measurement. Each row corresponds to a measurement scenario where we introduce symmetric losses (four first rows) or asymmetric losses (four last rows) in the links. The four last columns give the estimation error on loss rates in percentile points. For example, when we set the loss rates on the link fe to 20%, the landmark solution infers a loss rate of 20.8%. Both landmark pings and NALD perform well under symmetric loss rates. Both techniques infer the correct loss rate within less than two percentile points.

Unsurprisingly, both NALD and the landmark ping have trouble when we deliberately inject asymmetric losses in the link to the neighbor gateway. In that scenario, NALD infers a negative loss rate on the dc link. In practice, we can leverage this artifact to detect violations of the assumption that loss rates are symmetric on the WiFi link. When injecting asymmetric losses in the access link NALD properly infers the correct loss rate with small error. The landmark ping cannot pinpoint losses occurring on the uplink versus losses occurring on the downlink.

Summarizing, NALD behaves as we expect from the theoretical analysis. NALD has the same drawbacks and the same advantages than NADD.

Correlation of measured losses

We measure 1,191 rounds of measurement (i.e, 300 probes for the six individual path measurements). We compute the Pearson correlation coefficient between each pair of measurements. The most correlated pair of measurements are $\hat{T}_{fedcba}$ and $\hat{T}_{fedcdef}$, which have correlation coefficient of 0.45. This value indicates a moderate correlation

	Access		LAN	WLAN
	dc (Downlink)	cd (Uplink)	$ba = ab$	$ef = fe$
Occurrence of losses	4	18	4	16
Negative losses	18	9	0	0

Table 7.4: Location of losses in the six-homes testbed deployment

between the lost probes. This result support the fact that NALD assumptions are realistic in practice.

Location of inferred losses

We solve NALD systems of equations for 240 rounds where we have the six measurements and where we received at least one packet for each segment. We observe packet losses in 73 of these rounds. When we observe packet losses, loss rates are often small: there are only 27 rounds for which NALD infers loss rates larger than 1% in at least one link. Table 7.4 reports, for these 27 rounds, the number of time we infer some losses on each segment as well as the number of time NALD infers negative loss rates (i.e., when the measurement probes experience variability or asymmetry).

We observe four measurements with losses in the LAN. Laptops in the six-homes are connected in Ethernet, hence we expect even lower loss rates. Manual inspection of these four rounds shows that although on link has significant loss rates, loss rates in the LAN are below 1%. There is a significant amount of losses in the WiFi link. This results is consistent with the fact that neighbor WiFis may have a weak signal and suffer from heavy losses. We also observe losses on the access link, with a clear bias towards losses on the uplink. This result is consistent with the fact that access links uplink often are performance bottlenecks. Finally, there are 18 rounds with a significant asymmetry (we suspect on the WiFi link). Another explanation from the observed asymmetry is our current implementation of NALD: we perform the six measurements consecutively. Each measurement sends 300 probes, which takes more than two minutes. The network conditions may vary during the time to run all six measurements. We plan to improve our implementation of NALD to distribute probes on the six measurements uniformly so that all measurements experience similar network conditions.

7.4 Summary

We introduce neighbor-assisted diagnosis, a set of techniques for diagnosing home networks. A novel aspect of neighbor-assisted diagnosis is its use of WiFi neighbors (e.g., through WiFi communities) for the purpose of delay and loss diagnosis. We use neighbor WiFis for troubleshooting purposes, allowing probes to be sent to the public side of the home network gateway, and clockwise and counter-clockwise cyclic probes to be sent between multiple end-host interfaces.

We believe that neighbor-assisted diagnosis represents an important addition to the arsenal of network diagnostic tools, allowing end users to now pinpoint the location of delays and losses at the network's edge. Neighbor-assisted network diagnosis illustrates an important advantage of multi-homed end users – the ability to launch new types of measurement probes and perform new measurement diagnostics given multiple vantage points into the network. In the long term, multi-homed hosts may also be able to use their multiple points of connectivity to adaptively respond to changing network conditions – conditions that can be monitored using new tools such as NADD and NALD.

Chapter 8

Conclusion

We summarize the research contributions of this thesis and present future work.

8.1 Summary of contributions

This thesis designed techniques to assist home users identifying whether the home network is a performance bottleneck. We contribute with measurement methods for home networks and new insights on current home networks configuration and performance. Our controlled experiments show that the home network can affect end-to-end performance and that most existing diagnosis tools ignore the home network when identifying the cause of performance problems. Controlled experiments, however, are not sufficient to represent the diversity of possible home network topologies and environments. To shed light on home networks at large, we design and evaluate HomeNet Profiler, a measurement software that runs on end-hosts connected to volunteers' home networks.

We designed HomeNet Profiler as a one-shot measurement tool to attract as many users as possible. This decision proved successful as we collected data in more than 3,000 homes. This data let us characterize the set of devices and popular services in home networks, the implementation of UPnP in home gateways, and the WiFi environment of home networks. In addition, HomeNet Profiler takes the user perspective into account with a user survey. Our data show that home networks are often small but can have up to 20 devices. While the broad types of devices are similar in home networks, the particular model vary significantly. This result implies that diagnosis techniques for home networks have to work on fairly diverse home network configurations. A pathological example where the variety of home devices model hurts diagnosis techniques is the implementation of UPnP in home gateways. We demonstrate that UPnP queries can determine the ground-truth access link capacity, detect cross-traffic from the home network, and differentiate local from wide-area losses. However, our data collected with HomeNet Profiler and Netalyzr in 120,000 homes show that UPnP is not always available in today's home gateways and, when available, results are frequently inaccurate or simply wrong.

The user survey in HomeNet Profiler was also a valuable source of insights. Even though half of the users decided to skip the survey, it informed us on the household and on the devices which are not active in the home network when the user ran HomeNet Profiler. The survey results allowed us to observe a moderate correlation between the number of devices in home networks and the size of the household. The comparison between the survey results and the network scan results also show that only a small fraction of devices are active when users ran HomeNet Profiler. Only repeated measurements of the home network, which we perform in a limited number of homes, can observe all the home devices. Repeated measurements also proved valuable to understand how to interpret HomeNet Profiler's one-shot WiFi scans: a single WiFi scan is enough to observe all neighbor WiFi access points with strong signal.

The home WiFi environment is generally dense in our dataset, with up to 54 distinct WiFi neighbors. Further, 8% of the end-hosts running HomeNet Profiler received a neighbor WiFi with a signal stronger than the home WiFi signal. While dense WiFi leads to higher interference, we elaborate techniques to leverage the high density of WiFi neighborhoods. We develop methods for neighbor-assisted diagnosis to identify the directional delays and loss rates on the access link. On one hand, controlled experiments show that neighbor-assisted diagnosis is able to efficiently detect and distinguish uplink and downlink delays and loss rates with small error. On the other hand, we demonstrate neighbor-assisted diagnosis in a real-world deployment in five homes in France. Our deployment in those homes used WiFi communities to connect to neighbor WiFis. Current WiFi communities policies forced us to adapt NALD and NADD probes (e.g., fake DNS requests to send probes between interfaces) but our results show that neighbor-assisted diagnosis works in practice.

To summarize, our findings indicate two possible techniques to determine whether the home network is a performance bottleneck. First, we can query the home gateway using UPnP to attribute losses to the home network and identify when cross-traffic from the home network is limiting end-to-end bandwidth. Unfortunately our results also show that UPnP is not always available in today's home gateways. Second, we can leverage paths through WiFi neighbors to identify high delays and losses. These techniques can already be used in home networks today (for example, Dasu [141] incorporated UPnP measurements). However, we hope that these techniques will also motivate home gateway vendors and ISPs to enhance support for diagnosis in home networks. For example, home gateway vendors could improve the implementation of UPnP in their products and ISPs in other countries could deploy WiFi communities allowing neighbor-assisted network diagnosis probes.

8.2 Future work

The home network is a complex environment that deserves attention from the research community. The way forward to achieve better diagnosis in home networks appears to be in the cooperation between multiple devices: either between devices inside a same home network (e.g., end-hosts querying the home gateways) or between home networks (e.g., neighbor-assisted network diagnosis). As future work, we plan to follow two immediate directions: study what could be achieved when management and measurement functions are available to the end user on the home gateway; and deploy a neighbor-assisted diagnosis system at large scale. Ultimately, we plan to propose and study architectures that allow all home devices (spanning multiple devices in each home network and multiple home networks) to cooperate for network diagnostic.

Diagnosis techniques running on the home gateway

This thesis studies the performance of home networks from and end-host perspective. We show that to determine whether performance degradation occurs in the home network or in the access link, an end-host must cooperate with other devices (e.g., an end-host can query the home gateway with UPnP or connect through a WiFi neighbor). A natural extension to this work is to directly modify home gateways.

As development on home gateways becomes easier (either with improved toolchains or increased processing power), it will be possible to build performance diagnostic tools for home networks running directly on home gateways. Home gateways can passively monitor end-host traffic as well as independently measure the Internet and the home network with active probes.

Passive measurements on the home gateway solve the problem of pinpointing whether cross-traffic on the access link slows down an end-to-end flow. Under simple topologies or in home networks with a small number of devices (as we observe in HomeNet Profiler data), the home gateway alone is likely to be able to detect a performance bottleneck in the home network or in the access link. However home gateways see a different WiFi environment than other home devices. In particular, a WiFi neighbor may be a hidden-terminal for a home device. To diagnose such difficult WiFi environments, the diagnosis system needs the cooperation between as many WiFi devices as possible. Also, some home networks may have Layer-2 switches or WiFi-Direct links between devices. In such topologies, the traffic between pairs of devices may be invisible to the home gateway.

The home gateway is the only device that will have a full-picture of all connected devices. With active probing, the home gateway can independently probe inside the home network and towards the Internet. The concept of neighbor-assisted network diagnosis remains valid while probing from home gateways. From an implementation perspective, home gateways generally have a WiFi adapter. However, for a real-world use of neighbor-assisted network diagnosis, home gateways need an extra WiFi adapter in order to connect to neighbor networks and maintain WiFi connectivity to home devices at the same time.

Other home devices should be able to query home gateways. There are no screens on home gateways. Thus users interact with home gateways via applications running on end-host computers, tablets, or smartphones. It is unclear whether industries will agree on a common set of protocols and data representations to access home gateways diagnosis capabilities. This problem is a technical and political challenge which may impact researchers' efforts in home networks. Especially when considering the erroneous UPnP implementation we observed in HomeNet Profiler and Netalyzr datasets.

Designing a neighbor-assisted network diagnostic system

This thesis also presents neighbor-assisted network diagnosis techniques for measuring network losses and delays on the access link. A few steps are missing before turning neighbor-assisted network diagnosis into a complete diagnostic system.

A first direction is to perform "traditional" network tomography towards Internet paths from the home network and from neighbor networks. Such a measurement allows to pinpoint whether a network-performance problem is the same across multiple homes, if it specific to one ISP or to a single home network. Each neighbor WiFi is a candidate path to run active measurements. Hence, the larger the number of neighbor WiFis, the finer the results.

However, there is a tradeoff between the number of neighbor networks a neighbor-assisted network diagnosis system we connect to and the duration of the diagnosis. Attaching and authenticating to a neighbor WiFi network takes seconds. The worst situation happens when a neighbor-assisted network diagnosis system connects to a WiFi neighbor with poor WiFi quality. The combined effect of slow transmission rates and packet losses may significantly increase the duration of the WiFi association. Poor WiFi conditions may further add variability to delay and loss rates. The WiFi connectivity may even break while performing measurements. The set of usable WiFi neighbors from a home device is likely to be stable in the short-to-medium term. Hence, a home device could evaluate WiFi neighbors once and remember whether the WiFi neighbor is usable or not for neighbor-assisted network diagnosis. Such a mechanism would cut-down the duration of neighbor-assisted network diagnosis measurements over multiple neighbors.

In summary, a neighbor-assisted network diagnosis system will benefit from a learning phase, which evaluates each WiFi neighbor. Before running a neighbor-assisted network diagnosis measurement (either NALD, NADD, or more traditional network tomography), we envision an optimization phase to discard WiFi neighbors that bring little path diversity and to discard the WiFi neighbors with too poor WiFi performance to support NADD or NALD probing schemes.

Coordinated-diagnosis framework

Provided that gateway-based and neighbor-assisted diagnosis are well understood, it will be possible to integrate theses two approaches into a broader framework, where all home devices coordinate to diagnose one problem. Even more, devices in neighbor networks may cooperate. We plan to develop a coordinated-diagnosis framework to make this cooperation possible.

Coordinated-diagnosis require a common protocol or API. Inside a home network, architectures like HomeOS show that abstraction layers above UPnP, Zigbee and proprietary protocols allow for cooperation of devices in a single home. Therefore, HomeOS is a promising option to provide a programming interface to devices sitting in neighboring home networks. The exact protocol or set of protocols to use in a coordinated-diagnosis framework is only one part of the problem.

There are interesting research challenges to answers. One challenge that we plan to tackle is to translate a diagnostic question (e.g., “why is my video choppy?”) into a set of measurement actions (e.g., “ping Destination A and B from Machine 1 then ping Destination B from Machine 2”). Such a translation requires a system able to take into consideration all the vantage points available in a neighborhood. There likely are multiple translations for a single diagnostic question, thus, the coordinated-diagnosis framework will have to find one good solution to answer accurately and in a timely manner while keeping the overhead low.

Appendix A

Introduction

La dernière décennie a vu une forte augmentation du nombre de connexions résidentielles à l'Internet avec la généralisation de l'accès à haut débit [79]. Parallèlement, les utilisateurs peuvent désormais accéder à Internet via une grande variété d'appareils. De nos jours, il n'est pas rare que chaque membre d'un ménage possède son propre ordinateur personnel, smartphone ou tablette Internet. D'autres appareils tels que les équipements réseau (par exemple, les points d'accès WiFi et les routeurs) sont partagés par tous les membres d'une famille. Tous ces appareils, une fois connectés à la maison, constituent un *réseau domestique*. Les appareils d'un même réseau domestique partagent une connexion Internet unique. La figure A.1 représente un réseau domestique simple. Ce réseau est composé d'un ordinateur portable, un ordinateur de bureau, un téléphone et une télévision. Nous appelons les appareils avec lesquels les utilisateurs interagissent des *appareils domestiques*, par opposition aux routeurs Internet et aux serveurs. Les appareils domestiques se connectent à Internet via une *passerelle Internet*, qui combine un modem, un routeur et un point d'accès WiFi. Ces trois fonctions pourrait résider dans des objets physiques distincts, mais par souci de simplicité, nous supposerons que le même appareil effectue ces trois fonctions. Les fournisseurs d'appareils électronique grand public vendent maintenant une variété d'appareils (par exemple, les téléphones, les compteurs d'électricité et des capteurs de santé) qui reposent sur l'accès Internet du domicile pour se connecter à un service distant. Le lien qui relie la passerelle Internet au réseau du Fournisseur d'Accès Internet (FAI) est le *lien d'accès*. Les technologies courantes de lien d'accès sont le DSL et le Câble. Ces technologies offrent généralement une bande passante supérieure aux offres mobiles, et à un prix inférieur.

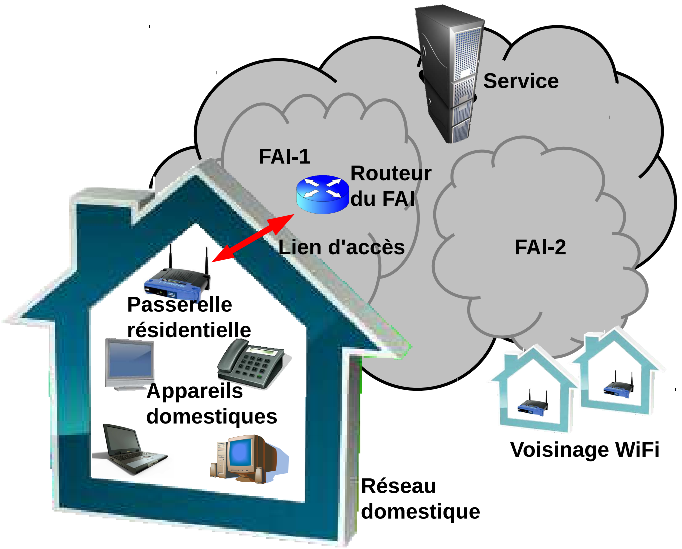


Figure A.1 – Example d'accès Internet d'un réseau domestique.

Lorsque les utilisateurs d'Internet subissent des performances insatisfaisantes (par exemple, des transferts de fichiers lents, une conférence audio hâchée), n'importe lequel des réseaux sur le chemin *bout-en-bout* (i.e., le trajet entre l'appareil domestique et le service distant) peut en être responsable. Cette thèse porte sur la contribution du réseau domestique aux performances bout-en-bout et donc nous séparons la performance de bout-en-bout selon trois principaux blocs : le réseau domestique, le lien d'accès, et le reste de l'Internet (y compris les serveurs distants). Le réseau domestique peut influer sur les performances de bout-en-bout. Les application ou bien le réseau limitent les performances bout-en-bout d'un service. Lorsque c'est le réseau qui limite les performances de bout-en-bout, un ou plusieurs liens que nous appelons *goulots d'étranglement*, peuvent limiter la performance bout-en-bout. Une raison qui fait qu'un lien devient un goulot d'étranglement est la congestion du réseau. Par exemple, sur la figure A.1, un utilisateur peut démarrer un long téléchargement sur l'ordinateur portable tandis qu'un autre utilisateur joue à un jeu en ligne sur l'ordinateur de bureau. Les deux applications nécessitent une grande quantité de bande passante. Si le lien d'accès ne peut pas soutenir les flux de chaque application, au moins l'un des les deux flux sera dégradé. En l'absence de congestion, la capacité réseau détermine le goulot d'étranglement. Par exemple, une mauvaise liaison WiFi à la maison entraîne des pertes et des délais de paquets, ce qui peut également expliquer des performances bout-en-bout dégradées [63]. Bien qu'il y ait un certain nombre d'études sur les performances des liens d'accès et du reste de l'Internet [47,94,173], on commence seulement à étudier le comportement des réseaux domestiques et peu de résultats de recherche sont disponibles sur les réseaux domestiques.

Les utilisateurs d'Internet ont besoin d'outils pour identifier l'emplacement précis des problèmes de performance réseau. Les utilisateurs d'Internet ne sont généralement pas des experts en réseau et, sans les outils adéquat, ils sont incapables de savoir pourquoi un service a de mauvaises performances. Des études montrent que les utilisateurs d'Internet ont souvent recours à des actions simples telles que redémarrer leurs appareils dans le but de résoudre leurs problèmes de connectivité [168]. Si le redémarrage ne résout pas le problème, les utilisateurs ont tendance à téléphone à leur FAI, mais le FAI n'est pas toujours responsable des faibles performances bout-en-bout. Le maintien des centres d'appels et l'envoi de techniciens pour vérifier les lignes DSL ou Câble engendrent des coûts élevés pour les FAI [84]. Par conséquent, à la fois les FAIs et les utilisateurs d'Internet bénéficieraient d'outils permettant aux utilisateurs finaux de diagnostiquer leur réseau domestique, en particulier d'outils pouvant déterminer lequel du réseau domestique ou du réseau du FAI est à l'origine des dégradations de performance. Des services de tests de bande passante tels que Grenouille [71], SpeedTest [157], et Netalyzr [94] sont populaires parmi les utilisateurs férus de technologie. Ces services exposent certaines propriétés des liens Internet tels que la capacité, le délai ou les taux de perte. Un certain nombre d'outils en ligne de commande peuvent aussi mesurer les mêmes propriétés [132]. Cependant, ces services de mesure ne peuvent pas toujours identifier si une dégradation des performances prend sa source dans le réseau domestique ou pas.

Cette thèse développe des techniques qui s'exécutent sur un *end-host* connecté à un réseau domestique pour identifier si le réseau domestique est un goulot d'étranglement des performances. Nous nous concentrons sur les techniques qui s'exécutent sur des end-hosts, car il est plus facile pour les utilisateurs non avertis d'installer des outils sur leur PC que sur d'autres appareils domestiques (par exemple, la passerelle Internet). Nous montrons d'abord avec des expériences semi-contrôlées que les réseaux domestiques peuvent en effet influer sur les performances de bout-en-bout. Ces expériences nous permettent de quantifier l'effet de différents facteurs sur les performances de bout-en-bout (par exemple, lorsque il y a du traffic depuis d'autres end-hosts ou lorsque les appareils domestiques sont connectés en WiFi) Toutefois, ces expériences nous permettent de tester seulement un petit ensemble de configurations de réseaux domestiques. Il est difficile d'affirmer que ces configurations sont représentatives d'une majorité de réseaux domestiques. En réalité, il ya peu des données sur les réseaux domestiques existants. Nous abordons ce problème avec HomeNet Profiler, un logiciel de mesure qui collecte la configuration et observe les performances des réseaux domestiques. Des volontaires font tourner HomeNet Profiler sur un ordinateur de leur réseau domestique. Ce faisant, HomeNet Profiler nous permet de recueillir la liste des appareils domestiques ainsi que la liste des services qu'ils annoncent. HomeNet Profiler mesure également l'environnement WiFi. Dans nos résultats, la plupart des ordinateurs exécutant HomeNet Profiler avait une interface WiFi et l'environnement WiFi était dense. Ces environments WiFi denses représentent une opportunité pour diagnostiquer les réseaux domestiques parce qu'un end-host peut se connecter au même service en utilisant la connexion Internet de l'utilisateur et celle d'un réseau voisin. Par exemple, sur la figure A.1, un ordinateur portable connecté à la fois au réseau domestique et à un réseau voisin peut envoyer des sondes vers les passerelles Internet de chaque réseau et peut également envoyer des sondes sur un chemin en forme de boucle passant par les deux réseaux. Ces sondes permettent aux end-hosts de déduire les pertes et les délais sur les liens de chemins bout-en-bout proches du réseau domestique. Cette information permet aux ordinateur portables d'identifier si les délais et les pertes se produisent dans le réseau domestique ou sur le lien d'accès. Nous concevons des techniques de diagnostic assisté par les voisins qui mettent à profit ces chemins alternatifs.

Le reste de ce chapitre fournit des informations générales sur la configuration des réseaux domestiques, les mesures des réseaux domestiques, et le diagnostic des réseaux domestiques. Nous présentons ensuite nos contributions de recherche et décrivons le reste de cette thèse.

A.1 Informations générales sur les réseaux domestiques

Comme illustré sur la figure A.1, dans les réseaux domestiques typiques les appareils partagent une seule connexion à l'Internet à travers la passerelle Internet. En France, la passerelle Internet combine généralement un modem DSL ou câble, un point d'accès WiFi, et un routeur. Dans d'autres pays, la passerelle Internet est un point d'accès WiFi et un routeur tandis que le modem est un appareil physique distinct. De nombreux FAIs fournissent une passerelle Internet à chacun de leurs clients. Autrement, les utilisateurs Internet achètent eux-même une passerelle Internet de leur choix et l'installent chez eux.

La passerelle Internet fait suivre le trafic Internet au routeur du FAI via le lien d'accès. Il y a plusieurs technologies de lien d'accès tels que le DSL, le Câble, et la fibre optique. Chacune de ces technologies a ses spécificités (par exemple, pour les délais de transmission ou la capacité montante et descendante), mais l'accès est souvent asymétrique (c'est à dire que la capacité descendante est plus élevée que la capacité montante). Les capacités typiques qu'offrent les FAI français sont : pour l'ADSL, 20 Mbps en download et 1 Mbps en upload, 60 Mbps/4 Mbps pour le câble et 100 Mbps/50 Mbps pour la fibre optique.

La connectivité à la maison est soit filaire (par exemple, Ethernet, MoCA, et CPL) ou sans fil (par exemple, WiFi, Bluetooth). Chaque technologie a ses propres caractéristiques : Ethernet et MoCA, qui utilisent des câbles blindés, fournissent des débit élevés (jusqu'à 10 Gbps pour Ethernet, 200 Mbps pour MOCA) et une bande passante stable mais nécessitent un câblage spécial dans la maison. Le CPL utilise le câblage électrique de la maison mais peut subir des interférences (et peut offrir jusqu'à 200 Mbps). Le WiFi est une technologie sans fil largement répandue pour raccorder les appareils domestiques. Le WiFi offre des débits allant jusqu'à 300 Mbps. Un réseau domestique peut utiliser plus d'une technologie. Par exemple, sur la figure A.1, l'ordinateur de bureau, le téléphone, et la télévision peut utiliser une liaison Ethernet, tandis que l'ordinateur portable ne se connectera qu'en WiFi.

Nous appelons le point d'accès WiFi (souvent la passerelle Internet) auxquel les appareils domestiques s'attachent le *WiFi domestique*. Les lois physiques de la propagation WiFi à la maison peut empêcher certains clients WiFi de recevoir un bon signal WiFI [126]. Du reste, le WiFi ne s'arrête pas aux murs de la maison. De ce fait, les clients WiFis sont généralement exposés à plusieurs réseaux WiFi. Une majorité de ces réseaux WiFi sont les WiFis domestiques de réseaux voisins. Par conséquent, nous appelons ces réseaux WiFi les *voisins WiFi*. Par exemple, sur la figure A.1, il y a deux voisins WiFi. Dans des zones densément peuplées, il peut y avoir des dizaines de voisins WiFi.

Tous les clients WiFi et points d'accès WiFi (y compris ceux des voisins WiFis) partagent le medium d'accès (i.e., l'air), soit en étalant leur accès sur des bandes de fréquences différentes ou en y accèdant à des moments différents. Le spectre est divisé en canaux et un point d'accès WiFi fonctionne sur un seul canal. Le point d'accès du WiFi domestique détermine donc le canal pour tous les appareils domestiques qui y sont associés. Par conséquent, tous les appareils domestiques sont en concurrence pour accéder au canal. En outre, les appareils et les points d'accès des voisins WiFis sont également en concurrence avec les clients domestiqus s'ils sont sur le même canal que le WiFi domestique (ou même sur un canal proche de celui en cours d'utilisation par le WiFi domestique). En conséquence, un WiFi domestique peuvent avoir de faibles performances dans des zones densément peuplées avec de nombreux réseaux WiFi en concurrence [76].

Les utilisateurs s'abonnent à Internet pour accéder à un certain nombre de services depuis chez eux. Ils peuvent accéder aux services de leur FAI et plus généralement des services de l'Internet. Deux services populaires sont la TV et la voix sur IP (VoIP). La TV et la VoIP sont appelés *services triple-play* lorsqu'un FAI regroupe ces services dans l'abonnement Internet. Certains utilisateurs installent aussis des appareils bénéficier d'autres services à l'intérieur leur réseau domestique (par exemple, un disque réseau peut offrir un service de sauvegarde et un serveur multimédias). L'installation de services tels que le partage de fichiers entre les appareils domestiques et le contrôle à distance des lecteurs multimédias exige des efforts de configuration. Par exemple, un ordinateur dans le réseau domestique doit connaître l'adresse IP des serveurs multimédias ou d'autres services dans le réseau local. Certains protocoles permettent l'autoconfiguration des services, par exemple Universal Plug and Play (UPnP) [159] et Zeroconf (aka Bonjour) [26]. Ces deux protocoles définissent des règles pour découvrir les services en émettant des requêtes de multidiffusion ainsi que des règles pour configurer les services via des requêtes de monodiffusion. La principale différence entre Zeroconf et UPnP est que UPnP spécifie également un ensemble de procédures d'appel de fonctions distantes. Au dessus d'UPnP, la Digital Living Network Alliance (DLNA) publie des spécifications pour que les applications multimédia découvrent les clips multimédias et les lisent sur des téléviseurs compatibles. Par exemple, le téléviseur de la figure A.1 peut parcourir des clips vidéo stockés sur l'ordinateur de bureau. En outre, UPnP et Zeroconf ont des formats de paquets différents et utilisent une adresse IP de multidiffusion différentes. Dans cette thèse, nous utilisons UPnP et Zeroconf dans le but de découvrir les services que les utilisateurs peuvent utiliser dans leur réseau domestique.

A.2 La mesure et la caractérisation des réseaux domestiques

Il y a un grand nombre de techniques pour mesurer et caractériser les réseaux IP en général. Jusqu'à présent, les chercheurs ont mesurés la topologie de l'Internet, ses performances, ainsi que les performances du WiFi. En dépit de l'intérêt croissant pour les réseaux domestiques, peu de données sont disponibles à propos des propriétés des réseaux domestiques (ex., quels sont les appareils ou les services disponibles). Des travaux précédents se sont concentrés sur la mesure et la caractérisation des liens d'accès résidentiels — en mesurant depuis des serveurs situés dans l'Internet [35, 47, 73, 107, 149], depuis des clients s'exécutant sur des end-hosts [31, 94], ou encore sur des passerelles domestiques modifiés pour effectuer des mesures actives et passives [154]. D'autres études ont également déployé des points de mesure chez des volontaires pour enregistrer ou améliorer les performances du réseau domestique [50, 89], pour mesurer comment le WiFi se propage dans des maisons [126], et même pour étudier le comportement des utilisateurs Internet quand ils utilisent leur réseau domestique [20, 27, 28, 168]. Cependant, récolter des mesures dans un nombre représentatif de maisons n'est pas une tâche aisée pour un certain nombre de raions.

Sonder l'intérieur des réseaux domestiques depuis l'extérieur est difficile. Le manque de données sur les réseaux domestiques est en partie dû aux challenges de mesurer les réseaux domestiques à grande échelle. La grande majorité des réseaux domestiques sont derrières des translateurs d'adresses (NATs) ou des pare-feu. De ce fait, un point de mesure hors du réseau domestique ne peut normalement pas envoyer de sondes pour mesurer les caractéristiques du réseau domestique. C'est pourquoi les chercheurs doivent recruter des volontaires pour faire tourner des mesures à l'intérieur de leur réseau domestique.

Les volontaires sont durs à trouver. L'effort nécessaire pour recruter un grand nombre de volontaires est un défi en soi. D'abord, les utilisateurs ne veulent pas s'investir plus que quelques minutes pour installer ou configurer des logiciels ou du matériel. Ensuite, seuls quelques utilisateurs participeraient à ce des études de recherche sans avoir des garanties fortes sur le respect de leur vie privée [86]. Enfin, une étude de recherche doit généralement trouver les bonnes incitations pour attirer un grand nombre de volontaires.

Les passerelles Internet ont des resources limitées. Lorsqu'un bénévole est prêt à exécuter des mesures dans son réseau domestique, l'emplacement particulier où installer le logiciel ou le matériel de mesure est un élément crucial à prendre en compte lors de la conception de l'expérience. Les mesures peuvent fonctionner sur les passerelles Internet ou sur les end-hosts. D'un côté, les passerelles Internet sont toujours branchées et elles peuvent observer tout le trafic Internet de la maison [154]. D'un autre ôté, les passrelles Internet disposent souvent de ressources limitées [136] et il n'y a pas de moyen simple pour exécuter du code arbitraire à des fins de mesure sur ces passerelles Internet. Il est possible de fournir des passerelles Internet modifiées, mais un tel déploiement matériel est coûteux lorsqu'on souhaite mesurer un grand nombre de réseaux domestiques. Inversement, les utilisateurs peuvent installer un logiciel sur leurs propres ordinateurs à moindre coût.

Les end-hosts ont une vue limitée du réseau domestique. Les end-hosts disposent de ressources suffisantes pour permettre un large éventail de mesures. Cependant, les utilisateurs éteignent parfois les end-hosts ou bien ils les déplaçent hors du réseau domestique, ce qui ne permet pas le suivi continu de l'état du réseau domestique. En outre, les end-hosts ne peuvent observer que leur propre contribution au trafic sur le lien d'accès, ce qui limite l'analyse des données connectées. Par exemple, pour savoir si une mesure de bande passante est représentative de la capacité du lien d'accès, il faut savoir si d'autres appareils domestiques ont également utilisé le lien d'accès lors de la mesure.

Dans cette thèse, nous mesurons les près de 3,000 réseaux domestiques depuis un end-host derrière un NAT ou un pare-feu. Nous gagnons accès à ces réseaux domestiques via un logiciel que des volontaires font eux-même tourner chez eux sur leur ordinateur.

A.3 Diagnostic des réseaux domestiques

Les utilisateurs Internet diagnostiquent les problèmes de performance de leur réseau domestique à l'aide d'outils de mesure qui s'exécutent sur un end-host ou sur la passerelle Internet. La plupart des systèmes d'exploitation fournissent des outils sommaires pour diagnostiquer le réseau. Par exemple, *Traceroute* infère la liste de *hops* IP vers une destination et *ping* détecte si une destination est joignable. *Iperf* mesure la bande passante entre deux hôtes Internet. Un certain nombre d'outils existent aussi avec lesquels les utilisateurs peuvent vérifier le réseau paramètres de leur stack IP et qui affectent les performances du réseau (par exemple, l'adresse IP du serveur DNS ou la MTU). En outre, certaines passerelles domestiques fournissent une interface web permettant d'effectuer un diagnostic similaire. Par exemple, les utilisateurs peuvent vérifier que la passerelle Internet a une adresse IP publique, lister les appareils connectés au réseau domestique, et même effectuer des ping directement depuis la passerelle Internet. Ces outils peuvent aider un expert à déduire quel est le problème, mais connaître le bon ensemble d'outils à utiliser et savoir interpréter leurs résultats est un usage trop avancé pour la plupart des utilisateurs. Un certain nombre de raisons expliquent pourquoi le diagnostic des réseaux domestiques est un problème difficile.

Le réseau domestique influe sur les outils de mesure de performance Comme nous le verrons dans le chapitre 3, les outils existants ne sont pas suffisants pour identifier si le réseau domestique est un goulot d'étranglement des performances. Par exemple, quand un ordinateur télécharge un fichier, du traffic concurrent d'un second appareil domestique peut réduire la vitesse de téléchargement du fichier. Un outils de mesure bout-en-bout observera une augmentation du délai ou une bande passante réduite. D'autres raisons pourraient conduire aux mêmes symptômes (par exemple, la congestion dans le réseau du FAI). Ainsi, même si la mesure de bout-en-bout observe une dégradation des performances, une ambiguïté sur les causes de cette dégradation subsiste. Les mesures de type *Traceroute* (par exemple, Tulip [106]) peut identifier les retards et les taux de perte de segments individuels du réseau le long d'un chemin bout-en-bout. Cependant ces techniques s'appuient sur les messages ICMP et l'option IP d'horodatage qui ne sont pas toujours pris en charge par les routeurs Internet [41,140], ou pris en charge mais avec des limitations d'usage [10, 91, 106]. Bien que Traceroute soit capable d'identifier un retard accru sur le lien d'accès, Traceroute seul ne peut pas identifier si le réseau domestique est responsable de la baisse de performance.

Il n'y a pas de modèles du comportement des passerelles Internets Des modèles du comportement des passerelles Internet en présence de flux de traffic concurrents pourraient aider à inférer la quantité de traffic en concurrence à l'aide de mesures bout-en-bout mais de tels modèles mathématiques n'existent pas encore.

Les réseaux domestiques ne sont pas supervisés. Les appareils domestique typiques ne possèdent pas de logiciel de supervision et il n'y a pas d'API commune pour demander des statistiques de traffic à tous les appareils domestiques. De fait, un appareil domestique n'a pas de moyen simple pour savoir si un deuxième appareil entre en concurrence pour accèder à Internet en même temps. La passerelle domestique peut quant à elle, observer si plusieurs flux réseaux sont en concurrence et ainsi peut lever l'ambiguïté de savoir si le réseau domestique est bien le goulôt d'étranglement ou pas. Malheureusement, dans les réseaux domestiques typiques, les utilisateurs ne peuvent pas communiquer avec la passerelle Internet pour avoir de telles données de traffic.

Les liens d'accès sont asymétriques L'asymétrie des réseaux d'accès résidentiels rend le diagnostic des problèmes de performances encore plus difficile. Les techniques *round-trip* telles que ping renvoie une seule valeur qui couple le lien descendant avec le lien montant en une seule mesure de délai. La seule façon de mesurer chaque direction de manière indépendante est d'utiliser un serveur synchronisé avec la source (ex., via un signal GPS) mais un tel niveau de synchronization n'est généralement pas disponible dans les appareils domestiques.

Dans cette thèse, nous montrons comment combiner des requêtes UPnP envoyées à la passerelle Internet avec des mesures de bout-en-bout pour localiser si les pertes de paquets ont lieu dans le réseau domestique ou sur le lien d'accès. Nous développons également des techniques utilisant les voisins WiFi pour distinguer les délais et les pertes sur le lien d'accès dans la direction montante de ceux dans la direction descendante.

A.4 Contributions

Cette thèse fait les contributions suivantes sur la mesure des réseaux domestiques, leur caractérisation, et leur diagnostic.

1. Nous montrons à l'aide d'expériences contrôlées que le réseau domestique peu avoir un effet significatif sur les performance de bout-en-bout. Par exemple, regarder la TV peut doubler le temps de transfer d'un fichier. Nous montrons que même un bon lien WiFi ajoute de la variance aux RTT. Malgré son impact sur les performances de bout-en-bout, la plupart des outils de diagnostic réseau ignorent l'effet du réseau domestique quand il faut identifier la cause des baisses de performance. De plus, nos résultats montrent que de simples techniques qui sondent directement la passerelle Internet ne peuvent pas fiablement identifier que le réseau domestique est le goulôt d'étranglement.

2. Nous concevons et évaluons HomeNet Profiler, un outil logiciel de mesure pour caractériser les réseaux domestiques. HomeNet Profiler s'exécute sur un ordinateur connecté à un réseau domestique pour collecter un large évantail de mesures à propos du réseau domestique dont la liste des appareils, l'ensemble des services (via UPnP et Zeroconf), et les caractéristiques de l'environnemnt WiFi. HomeNet Profiler embarque également un sondage pour collecter des informations qu'on ne peut pas mesurer directement. Pour attirer un grand nombre d'utilisateurs, HomeNet Profiler exécute des mesures une seule fois, à la demande de l'utilisateur. Nous évaluons ce choix de conception à l'aide de mesure répétées prises dans six réseaux domestiques. Nos résultats montrent qu'un seul scan WiFi suffit à observer tous les réseaux WiFi avec un signal puissant. Tandis que seuls des mesures répétées permettent d'observer tous les appareils du

réseau domestique. Ainsi, le sondage de HomeNet Profiler est un complément important pour connaître la liste entière d'appareils.

3. Nous présentons la première étude à grande échelle des implémentations UPnP dans les passerelles Internet. La technologie UPnP est un moyen prometteur pour collecter efficacement et exploiter les données de mesure et de configuration dans les réseaux domestiques. Malheureusement, UPnP s'avère moins disponible et moins fiable que l'on pourrait espérer. Nous utilisons les données de 120,000 réseaux domestiques, recueillies par HomeNet Profiler et Netalyzr [94]. Nos résultats montrent que dans la majorité des foyers, nous n'observons pas de passerelle UPnP du tout. Quand une passerelle UPnP est présente, les résultats sont souvent inexacts ou tout simplement faux. Cependant, lorsque les données UPnP sont exactes, nous démontrons que les requêtes UPnP permettent de déterminer la capacité du lien d'accès, de détecter la présence de flux concurrents, et de distinguer les pertes locales des pertes dans l'Internet. En outre, UPnP permet d'identifier les caractéristiques des passerelles Internet par modèle.

4. Avec notre jeu de données HomeNet Profiler composé de 2940 domiciles, nous montrons que les réseaux domestiques sont souvent de petite taille avec entre 2 et 20 appareils. Les types d'appareils ne varient pas beaucoup d'une maison à l'autre, mais les modèles particuliers varient d'une maison à l'autre. En conséquences, les techniques de diagnostic pour réseaux domestiques doivent fonctionner avec des configurations très diverses de réseaux domestiques.

5. A l'aide de scans WiFi dans 1,313 domiciles, nous montrons que l'environnement WiFi est généralement dense. Les end-hosts obvservent jusqu'à 54 réseaux WiFis différents et jusqu'à 15 sur le même canal que le WiFi domestique. En outre, environ 8% des end-hosts faisant tourner HomeNet Profiler, reçoit un voisin WiFi qui possède un signal plus puissant que celui du WiFi domestique. Nous montrons également que la forte densité des environnements WiFi dans les réseaux domestiques ouvrent des opportunités pour diagnostiquer les performances des réseaux domestiques.

   Nous développons des méthodes de diagnostic assisté par les voisins pour identifier les pertes et les délais. Nous prenons avantage des voisins WiFi pour diagnostiquer les baisses de performance. Un end-host connecté à la passerelle Internet du réseau domestique et en même temps à la passerelle Internet d'un voisin WiFi peut envoyer différents types de sondes pour mesurer les délais et les pertes unidirectionnels sur le lien d'accès. Notre évaluation montre que le diagnostic assisté par les voisins permet de détecter et distinguer les délais et pertes avec une erreur faible sur le lien montant et sur le lien descendant. Du reste, nos expériences en environnement réel dans six maisons en France monte que le diagnostic assisté par les voisins permet à l'utilisateur et aux FAIs de repérer l'emplacement des délais et des pertes à partir de la périphérie du réseau.

A.5 Aperçu de la thèse

Le restant de cette thèse est organisé comme suit. Après avoir présenté l'état de l'art et les travaux connexes aux notres sur les mesures de bout-en-bout, les mesures de lien d'accès, et les mesures de réseau domestique dans le Chapitre 2, nous étudions l'impact du réseau domestique sur les performances de bout-en-bout dans le Chapitre 3. Le Chapitre 4 conçoit et évalue HomeNet Profiler, notre outil de mesure de réseaux domestiques à grande échelle. Le Chapitre 5 décrit le jeu de données HomeNet Profiler ainsi que nos heuristiques pour séléctionner une seule mesure représentative par réseau domestique. Le Chapitre 6 présente notre charactérisation de trois aspects des réseaux domestiques : l'implémentation d'UPnP dans les passerelles Internet, la liste des appareils et services présents dans les réseaux domestiques, et l'environnement WiFi des réseaux domestiques. Notre caractérisation montre que les voisins WiFis offrent une opportunité pour identifier si le réseau domestique est un goulôt d'étranglement. Le Chapitre 7 introduit des techniques de diagnostic assisté par les voisins pour identifier quels segments du réseau ont de fortes pertes ou de forts délais. Enfin le Chapitre 8 conclut cette thèse et discute des travaux futurs.

Bibliography

[1] Bhavish Aggarwal, Ranjita Bhagwan, Tathagata Das, Siddarth Eswaran, Venkata N. Padmanabhan, and Geoffrey M. Voelker. NetPrints: Diagnosing Home Network Misconfigurations Using Shared Knowledge. In *Proc. NSDI*, 2009.

[2] Akamai. The State of the Internet – Official Akamai Internet Traffic Report. `http://www.akamai.com/stateoftheinternet/`.

[3] Aditya Akella, Glenn Judd, Srinivasan Seshan, and Peter Steenkiste. Self-Management in Chaotic Wireless Deployments. In *Proc. ACM MOBICOM*, 2005.

[4] Mark Allman. Comments on bufferbloat. *ACM SIGCOMM Computer Communication Review*, 43(1), 2013.

[5] Xueli An, Venkatesha Prasad, and IGMM Niemegeers. Exploring the Suitability of 60 GHz Radio for Building in-Home Networks. In *ACM SIGCOMM HomeNets Workshop*, 2010.

[6] Google Analytics. Enterprise-class web analytics. `http://www.google.com/analytics/`.

[7] P. Antoniadis, S. Fdida, C.H. Griffin, Y. Jin, and G. Kesdis. Distributed medium access control with dynamic altruism. In *International Conference on Ad Hoc Networks*, 2012.

[8] A. Arjona and S. Takala. The Google Muni WiFi Network: Can it Compete with Cellular Voice? In *AICT*, 2007.

[9] Brice Augustin, Xavier Cuvellier, Benjamin Orgogozo, Fabien Viger, Timur Friedman, Matthieu Latapy, Clémence Magnien, and Renata Teixeira. Avoiding traceroute anomalies with Paris Traceroute. In *Proc. IMC*, 2006.

[10] Brice Augustin, Renata Teixeira, and Timur Friedman. Measuring Load-Balanced Paths in the Internet. In *Proc. IMC*, 2007.

[11] Francois Baccelli, Sridhar Machiraju, Darryl Veitch, and Jean Bolot. On Optimal Probing for Delay and Loss Measurement. In *Proc. IMC*, 2007.

[12] Steven Bauer, David Clark, and William Lehr. Powerboost. In *ACM SIGCOMM HomeNets Workshop*, 2011.

[13] Maria Eugenia Berezin, Franck Rousseau, and Andrzek Duda. Citywide Mobile Internet Access Using Dense Urban WiFi Coverage. In *UrbaNE*, 2012.

[14] BGR. Comcast announces bandwidth throttling in FCC filing. `http://bgr.com/2008/09/20/comcast-announces-bandwidth-throttling/`, Sep 2008.

[15] Zachary S. Bischof, John S. Otto, Mario a. Sánchez, John P. Rula, David R. Choffnes, and Fabián E. Bustamante. Crowdsourcing isp characterization to the network edge. In *ACM SIGCOMM W-MUSt Workshop*, 2011.

[16] A. Broido, Y. Hyun, and k. claffy. Spectroscopy of traceroute delays. In *Proc. PAM*, 2005.

[17] A.J. Bernheim Brush, Jaeyeon Jung, Ratul Mahajan, and James Scott. HomeLab: Shared Infrastructure for Home Technology Field Studies. In *ACM HomeSys Workshop*, 2012.

[18] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. Home Automation in the Wild: Challenges and Opportunities. In *Proc. ACM CHI*, 2011.

[19] Tian Bu, Nick Duffield, Francesco Lo Presti, and Don Towsley. Network tomography on general topologies. In *Proc. ACM SIGMETRICS*, 2002.

[20] Kenneth L. Calvert, W. Keith Edwards, Nick Feamster, Rebecca E. Grinter, Ye Deng, and Xuzi Zhou. Instrumenting Home Networks. In *ACM SIGCOMM HomeNets Workshop*, 2010.

[21] Igor Canadi, Paul Barford, and Joel Sommers. Revisiting Broadband Performance. In *Proc. IMC*, 2012.

[22] Rich Carlson. Network diagnostic tool (ndt): An internet2 cookbook. `http://www.internet2.edu/performance/ndt/index.html`.

[23] Rui Castro, Mark Coates, Gang Liang, Robert Nowak, and Bin Yu. Network tomography: recent developments. *Statistical Science*, 19, 2004.

[24] Edmond W. W. Chan, Ang Chen, Xiapu Luo, Ricky K.P. Mok, Weichao Li, and Rocky K.C. Chang. TRIO: Measuring Asymmetric Capacity with Three Minimum Round-trip Times. In *Proc. CoNEXT*, 2011.

[25] Edmond W. W. Chan, Xiapu Luo, and Rocky K.C. Chang. A minimum-delay-difference method for mitigating cross-traffic impact on capacity measurement. In *Proc. CoNEXT*, 2009.

[26] Stuart Chesire and M. Krochmal. Multicast DNS. `http://www.rfc-editor.org/rfc/rfc6762.txt`. RFC 6762.

[27] Marshini Chetty, Richard Banks, Richard Harper, Tim Regan, Abigail Sellen, Christos Gkantsidis, Thomas Karagiannis, and Peter Key. Who's Hogging The Bandwidth?: The Consequences Of Revealing The Invisible In The Home. In *Proc. ACM CHI*, 2010.

[28] Marshini Chetty, David Halsem, Andrew Baird, Ugochi Ofoha, Bethany Summer, and Rebecca E. Grinter. Why Is My Internet Slow?: Making Network Speeds Visible. In *Proc. ACM CHI*, 2011.

[29] Kenjiro Cho, Kensuke Fukuda, Hiroshi Esaki, and Akira Kato. Observing Slow Crustal Movement in Residential User Traffic. In *Proc. CoNEXT*, 2008.

[30] David R. Choffnes and Fabian E. Bustamante. Pitfalls for Testbed Evaluations of Internet Systems. 40(2), 2010.

[31] David R. Choffnes, Fabián E. Bustamante, and Zihui Ge. Crowdsourcing Service-Level Network Event Monitoring. In *Proc. ACM SIGCOMM*, 2010.

[32] Gkantsidis Christos, Karagiannis Thomas, Key Peter, Radunovic Bozidar, Raftopoulos Elias, and D. Manjunath. Traffic management and resource allocation in small wired/wireless networks. In *Proc. CoNEXT*, 2009.

[33] k. claffy, H. Braun, and G. Polyzos. Measurement considerations for assessing unidirectional latencies. *Journal of Internetworking*, 4(3), 1993.

[34] ComScore. EU5 Smartphone Penetration Reaches 55 Percent in October 2012. `http://www.comscore.com/Insights/Press_Releases/2012/12/EU5_Smartphone_Penetration_Reaches_55_Percent_in_October_2012`.

[35] D. Croce, T. En-Najjary, G. Urvoy-Keller, and E. Biersack. Capacity Estimation of ADSL links. In *Proc. CoNEXT*, 2008.

[36] Daniele Croce, Taoufik En-Najjary, Guillaume Urvoy-Keller, and Ernst Biersack. Fast Available Bandwidth sampling for ADSL links: Rethinking the estimation for larger-scale measurements. In *Proc. PAM*, 2009.

[37] Heng Cui and Ernst Biersack. Trouble Shooting Interactive Web Sessions in a Home Environment. In *ACM SIGCOMM HomeNets Workshop*, 2011.

[38] Heng Cui and Ernst Biersack. Distributed Troubleshooting of Web sessions using clustering. In *Proc. TMA*, 2012.

[39] Italo Cunha, Renata Teixeira, Nick Feamster, and Christophe Diot. Measurement Methods for Fast and Accurate Blackhole Identification with Binary Tomography. In *Proc. IMC*, 2009.

[40] Italo Cunha, Renata Teixeira, Darryl Veitch, and Christophe Diot. Predicting and Tracking Internet Path Changes. In *Proc. ACM SIGCOMM*, 2011.

[41] Walter de Donato, Pietro Marchetta, and Antonio Pescapè. A hands-on look at active probing using the IP prespecified timestamp option. In *Proc. PAM*, 2012.

[42] Serge Defrance, Rémy Gendrot, Jean Le Roux, Gilles Straub, and Thierry Tapie. Home Networking as a Distributed File System View. In *ACM SIGCOMM HomeNets Workshop*, 2011.

[43] The OpenWRT developers. OpenWRT: Wireless Freedom. `https://openwrt.org/`.

[44] Amogh Dhamdere, Renata Teixeira, Constantine Dovrolis, and Christophe Diot. NetDiagnoser: Troubleshooting network unreachabilities using end-to-end probes and routing data. In *Proc. CoNEXT*, 2007.

[45] Mohan Dhawan, Justin Samuel, Renata Teixeira, Christian Kreibich, Mark Allman, Nicholas Weaver, and Vern Paxson. Fathom: A Browser-based Network Measurement Platform . In *Proc. IMC*, 2012.

[46] Marcel Dischinger, Andreas Haeberlen, Ivan Beschastnikh, Krishna P. Gummadi, and Stefan Saroiu. SatelliteLab: Adding Heterogeneity to Planetary-Scale Network Testbeds. In *Proc. ACM SIGCOMM*, 2008.

[47] Marcel Dischinger, Andreas Haeberlen, Krishna P. Gummadi, and Stefan Saroiu. Characterizing Residential Broadband Networks. In *Proc. IMC*, 2007.

[48] Marcel Dischinger, Massimiliano Marcon, Saikat Guha, Krishna P. Gummadi, Ratul Mahajan, and Stefan Saroiu. Glasnost: Enabling End Users to Detect Traffic Differentiation. In *Proc. NSDI*, 2010.

[49] Colin Dixon, Ratul Mahajan, Sharad Agarwal, A.J. Brush, Bongshin Lee, Stefan Saroiu, and Victor Bahl. The Home Needs an Operating System (and an App Store). In *ACM SIGCOMM HotNets Workshop*, 2010.

[50] Colin Dixon, Ratul Mahajan, Sharad Agarwal, A.J. Brush, Bongshin Lee, Stefan Saroiu, and Victor Bahl. An Operating System for the Home. In *Proc. NSDI*, 2012.

[51] A. De Domenico, E.C. Strinati, and M.G. Di Benedetto. A Survey on MAC Strategies for Cognitive Radio Networks. 14(1), 2012.

[52] Changyu Dong and Naranker Dulay. Argumentation-based Fault Diagnosis for Home Networks. In *ACM SIGCOMM HomeNets Workshop*, 2011.

[53] Benoit Donnet, Matthew Luckie, Pascal Mérindol, and Jean-Jacques Pansiot. Measured Impact of Crooked Traceroute. *ACM SIGCOMM Computer Communication Review*, 41(1), 2011.

[54] Benoit Donnet, Matthew Luckie, Pascal Mérindol, and Jean-Jacques Pansiot. Revealing MPLS Tunnels Obscured from Traceroute. *ACM SIGCOMM Computer Communication Review*, 42(2), 2012.

[55] C. Dovrolis, P. Ramanathan, and D. Moore. Packet Dispersion Techniques and Capacity Estimation. *IEEE/ACM Transactions on Networking*, 12(6), 2004.

[56] DSL Forum. Technical Report 069. `http://www.broadband-forum.org/technical/download/TR-069.pdf`.

[57] W. Keith Edwards, Rebecca Grinter, Ratul Mahajan, , and David J. Wetherall. Advancing the state of home networking. In *Communications of the ACM*, 2011.

[58] B Eriksson, Paul Barford, R. Nowak, and M. Crovella. Learning Network Structure From Passive Measurements. In *Proc. IMC*, 2007.

[59] Jeffrey Erman, Alexandre Gerber, and Subhabrata Sen. HTTP in the home: It is not just about PCs. In *ACM SIGCOMM HomeNets Workshop*, 2010.

[60] FCC's Office of Engineering and Technology and Consumer and Governmental Affairs Bureau. Measuring broadband america, 2011. `http://www.fcc.gov/measuring-broadband-america`.

[61] Nick Feamster. Outsourcing Home Network Security. In *ACM SIGCOMM HomeNets Workshop*, 2010.

[62] Federal Communications Commission. Fcc chairman julius genachowski announces major effort to increase wifi speeds and alleviate wifi congestion at airports, convention centers, and in homes with multiple devices and users, 2011. `http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0109/DOC-318326A1.pdf`.

[63] Bianchi G. Performance analysis of the ieee 802.11 distributed coordination. *IEEE J. Selected Areas in Communications*, 18, 2000.

[64] Alexandre Gerber, Jeffrey Pang, Oliver Spatscheck, and Shobha Venkataraman. Representative Speed tests for Free: Estimating Achievable Download Speed from Passive Measurements. In *Proc. IMC*, 2010.

[65] Jim Gettys and Kathleen Nichols. Bufferbloadt: Dark buffers in the internet. In *Communications of the ACM*, volume 55, 2012.

[66] Denisa Ghita, Katerina Argyraki, and Patrick Thiran. Network tomography on correlated link. In *Proc. IMC*, 2010.

[67] Denisa Ghita, Katerina Argyraki, and Patrick Thiran. Toward accurate and practical network tomography. In *Operating System Review*, volume 47, 2013.

[68] Denisa Ghita, Can Karakus, Katerina Argyraki, and Patrick Thiran. Shifting Network Tomography Toward A Practical Goal. In *Proc. CoNEXT*, 2011.

[69] Oana Goga and Renata Teixeira. Speed Measurement of Residential Internet Access. In *Proc. PAM*, 2012.

[70] Eduard Goma, Marco Canini, Alberto Lopez Toledo, Nikolaos Laoutaris, Dejan Kostic, Pablo Rodriguez, Rade Stanojevic, and Pablo Yague Valentin. Insomnia in the Access. In *Proc. ACM SIGCOMM*, 2011.

[71] Grenouille. La météo du Net. `http://www.grenouille.com/`.

[72] Vivien Gueant. Iperf: The TCP/UDP Bandwidth Measurement Tool. `http://iperf.fr/`.

[73] Dongsu Han, Aditya Agarwala, David G. Andersen, Michael Kaminsky, Konstantina Papagiannaki, and Srinivasan Seshan. Mark-and-Sweep: Getting the Inside Scoop on Neighborhood Networks. In *Proc. IMC*, 2008.

[74] Dongsu Han, David Andersen, Michael Kaminsky, Dina Papagiannaki, and Srinivasan Seshan. Hulu in the Neighborhood. In *International Conference on COMmunication Systems and NETworkS*, 2011.

[75] Seppo Hatonen, Aki Nyrhinen, Lars Eggert, Stephen Strowes, Pasi Sarolahti, and Markku Kojo. An Experimental Study of Home Gateway Characteristics. In *Proc. IMC*, 2010.

[76] Martin Heusse, Franck Rousseau, Gilles Berger-Sabbatel, and Andrzej Duda. Performance anomaly of 802.11b. In *Proc. IEEE INFOCOM*, 2003.

[77] Bradley Huffaker, Marina Fomenkov, Daniel Plummer, David Moore, and kc Claffy. Distance Metrics in the Internet. In *IEEE International Telecommunications Symposium*, 2002.

[78] Bradley Huffaker, Daniel Plummer, David Moore, and kc Claffy. Topology discovery by active probing. In *Symposium on Applications and the Internet (SAINT)*, 2002.

[79] Internet World Stats. `http://www.internetworldstats.com/dsl.htm`.

[80] J. Case and M. Fedor and M. Schoffstall and J. Davin. A Simple Network Management Protocol (SNMP). `http://tools.ietf.org/rfc/rfc1157`. RFC 1157.

[81] Sharad JAiswal, Gianluca Iannaccone, Christophe Diot, Jim Kurose, and Don Towsley. Inferring tcp connection characteristics through passive measurements. In *Proc. IEEE INFOCOM*, 2004.

[82] Szymon Jakubczak, David G. Andersen, Michael Kaminsky, Konstantina Papagiannaki, and Srinivasan Seshan. Link-alike: Using Wireless to Share Network Resources in a Neighborhood. *ACM SIGMOBILE Mobile Computing and Communications Review*, 12(4), 2008.

[83] Haiqing Jiang, Yaogong Wang, Kyunghan Lee, and Injong Rhee. Tackling Bufferbloat in 3G/4G Networks. In *Proc. IMC*, 2012.

[84] Yu Jin, Nick Duffield, Alexandre Gerber, Patrick Haffner, Subhabrata Sen, and Zhi-Li Zhang. NEVERMIND, the problem is already fixed: proactively detecting and troubleshooting customer DSL problems. In *Proc. CoNEXT*, 2010.

[85] Diana Joumblatt, Oana Goga, Renata Teixeira, Jaideep Chandrashekar, and Nina Taft. Characterizing end-host application performance across multiple networking environments. In *Proc. IEEE INFOCOM*, 2012.

[86] Diana Joumblatt, Renata Teixeira, Jaideep Chandrashekar, and Nina Taft. Perspectives on Tracing End-Hosts: A Survey Summary. *ACM SIGCOMM Computer Communication Review*, 40(2), 2010.

[87] Partha Kanuparthy and Constantine Dovrolis. ShaperProbe: End-to-end Detection of ISP Traffic Shaping using Active Methods. In *Proc. IMC*, 2011.

[88] Partha Kanuparthy, Constantine Dovrolis, and Konstantina Papagiannaki. Can User-Level Probing Detect and Diagnose Common Home-WLAN Pathologies? *ACM SIGCOMM Computer Communication Review*, 42(1), 2012.

[89] Thomas Karagiannis, Elias Athanasopoulos, Christos Gkantsidis, and Peter Key. HomeMaestro: Order from Chaos in Home Networks. Technical Report MSR-TR-2008-84, MSR, 2008.

[90] Ethan Katz-Bassett, Harsha V. Madhyastha, Vijay Kumar Adhikari, Colin Scott, Justine Sherry, Peter van Wesep, Thomas Anderson, and Arvind Krishnamurthy. Reverse Traceroute. In *Proc. NSDI*, 2010.

[91] Ken Keys, Young Hyun, Matthew Luckie, and k.c. Claffy. Internet-Scale IPv4 Alias Resolution with MIDAR . 2012.

[92] Hyojoon Kim, Srikanth Sundaresan, Marshini Chetty, Nick Feamster, and W. Keith Edwards. Communicating with Caps: Managing Usage Caps in Home Networks. In *Proc. ACM SIGCOMM*, 2011. Poster.

[93] Sam Knows. Accurate broadband performance information for consumers, governments, and ISPs. `http://www.samknows.com/`.

[94] Christian Kreibich, Nicholas Weaver, Boris Nechaev, and Vern Paxson. Netalyzr: Illuminating the Edge Network. In *Proc. IMC*, 2010.

[95] S. Shanmuga Krishnan and Ramesh K. Sitaraman. Video Stream Quality Impacts Viewer Behavior: Inferring Causality using Quasi-Experimental Designs. In *Proc. IMC*, 2012.

[96] Sriram Lakshmanan, Karthikeyan Sundaresan, Sampath Rangarajan, and Raghupathy Sivakumar. The Myth of Spatial Reuse with Directional Antennas in Indoor Wireless Networks. In *Proc. PAM*, 2010.

[97] Kaushik Lakshminarayanan, Srinivasan Seshan, and Peter Steenkiste. Understanding 802.11 Performance in Heterogeneous Environments. In *ACM SIGCOMM HomeNets Workshop*, 2011.

[98] Anthony LaMarca, Yatin Chawathe, Sunny Consolvo, Jeffrey Hightower, Ian Smith, James Scott, Tim Sohn, James Howard, Jeff Hughes, Fred Potter, Jason Tabert, Pauline Powledge, Gaetano Borriello, and Bill Schilit. Place lab: Device positioning using radio beacons in the wild. Technical Report IRS-TR-04-016, 2004.

[99] K. Lee, J. Lee, Y. Yi, I. Rhee, and S. Chong. Mobile data offloading: how much can wifi deliver? In *Proc. CoNEXT*, 2010.

[100] Yanlin Li, Dina Papagiannaki, and Anmol Sheth. Uplink Traffic Control in Home 802.11 Wireless Networks. In *ACM SIGCOMM HomeNets Workshop*, 2011.

[101] Shu Liu and Aaron D. Striegel. Casting Doubts on the Viability of WiFi Offloading. In *Proc. CellNet*, 2012.

[102] LLDP. 802.1AB - Station and Media Access Control Connectivity Discovery. `http://www.ieee802.org/1/pages/802.1ab.html`.

[103] M. Luckie, Y. Hyun, and B. Huffaker. Traceroute Probe Method and Forward IP Path Inference. In *Proc. IMC*, 2008.

[104] Harsha V. Madhyastha, Tomas Isdal, Michael Piatek, Colin Dixon, Thomas Anderson, Arvind Krishnamurthy, and Arun Venkataramani. iPlane: An Information Plane for Distributed Services. In *Proc. OSDI*, 2006.

[105] Harsha V. Madhyastha, Ethan Katz-Bassett, Thomas Anderson, Arvind Krishnamurthy, and Arun Venkataramani. iPlane Nano: Path Prediction for Peer-to-Peer Applications. In *Proc. NSDI*, 2009.

[106] Ratul Mahajan, Neil Spring, David Wetherall, and Thomas Anderson. User-level Internet Path Diagnosis. In *Proc. SOSP*, 2003.

[107] G Maier, A Feldmann, V Paxson, and M Allman. On Dominant Characteristics of Residential Broadband Internet Traffic. In *Proc. IMC*, 2009.

[108] G Maier, Fabian Schneider, and A Feldmann. NAT Usage in Residential Broadband Networks. In *Proc. IMC*, 2011.

[109] G. Malkin. Rfc1393: Traceroute using an ip option. `http://tools.ietf.org/rfc/rfc1393`.

[110] Lefteris Mamatas, Ioannis Psaras, and George Pavlou. Incentives and Algorithms for Broadband Access sharing. In *ACM SIGCOMM HomeNets Workshop*, 2010.

[111] Yun Mao, Shu Tao, Hani Jamjoom, and Jonathan M. Smith. NetworkMD: Topology Inference and Failure Diagnosis in the Last Mile. In *Proc. IMC*, 2007.

[112] Jake Martin and Nick Feamster. User-Driven Dynamic Traffic Prioritization for Home Networks. In *ACM SIGCOMM W-MUSt Workshop*, 2012.

[113] Mathis Matt, Heffner John, and Reddy Raghu. Network path and application diagnosis. `http://www.psc.edu/networking/projects/pathdiag/`.

[114] Maxmind. GeoIP – IP Address Location Technology. `http://www.maxmind.com/app/ip-location`.

[115] MetaGeek. Wi-Spy: Visualize your wireless landscape. `http://www.metageek.net/`.

[116] Microsoft. Link Layer Topology Discovery Protocol Specification. `http://msdn.microsoft.com/en-US/windows/hardware/gg463024`.

[117] Arunesh Mishra, Vivek Shrivastava, Suman Barnejee, and William Arbaugh. Partially overlapped channels not considered harmful. In *Proc. ACM SIGMETRICS*, 2006.

[118] R. Mortier, T. Rodden, T. Lodge, D. McAulay, C. Rotsos, A.W. Moore, A. Koliousis, and J. Sventek. Control and Understanding: Owning Your Home Network. In *International Conference on COMmunication Systems and NETworkS*, 2012.

[119] Mike Muuss. The Story of the Ping Program. `http://ftp.arl.mil/~mike/ping.html`.

[120] Neil Spring and Ratul Mahajan and David Wetherall. Measuring ISP Topologies with Rocketfuel. In *Proc. ACM SIGCOMM*, 2002.

[121] NewRelic. Web Application Performance Management and Monitoring. `http://newrelic.com/`.

[122] NMAP. Nmap: Free security scanner for network exploration and security audits. `http://nmap.org/`.

[123] OASIS. Devices Profile for Web Services (DPWS). `http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01`.

[124] Overlook. Fing - network tools (android market). `https://play.google.com/store/apps/details?id=com.overlook.android.fing`.

[125] Christoph Paasch, Gregory Detal, Fabien Duchene, Costin Raiciu, and Olivier Bonaventure. Exploring Mobile/WiFi Handover with Multipath TCP. In *Proc. CellNet*, 2012.

[126] Konstantina Papagiannaki, Mark Yarvis, and W. Steven Conner. Experimental Characterization of Home Wireless Networks and Design Implications. In *Proc. IEEE INFOCOM*, 2006.

[127] V. Paxson, G. Almes, J. Mahdavi, and M. Mathis. Framework for ip performance metrics. `http://www.rfc-editor.org/rfc/rfc2330.txt`, 1998. RFC 2330.

[128] Kandarak Piamrat and Patrick Fontaine. Coordinated Architecture for Wireless Home Networks. In *ACM SIGCOMM HomeNets Workshop*, 2011.

[129] Louis Plissonneau and Ernst Biersack. A Longitudinal View of HTTP Video Streaming Performance. In *Proc. MMSys*, 2012.

[130] Polarcloud. Tomato Firmware. `http://www.polarcloud.com/tomato`.

[131] J. Postel. Internet control message protocol. RFC 792.

[132] R. Prasad, C. Dovrolis, M. Murray, and k.c. Claffy. Bandwidth estimation: metrics, measurement techniques, and tools. *IEEE Network Magazine*, 17(6), 2003.

[133] R. Kapoor and L. Chen and L. Lao and M. Gerla and M. Sanadidi. CapProbe: A simple and accurate capacity estimation technique. In *Proc. ACM SIGCOMM*, 2004.

[134] Ramya Raghavendra, Michael Kaminsky, Konstantina Papagiannaki, Srinivasan Seshan, and Elizabeth Belding. IdleChat: enabling high bandwidth realtime applications in residential broadband networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 15(3), 2011.

[135] Tahiry Razafindralambo, Isabell Guérin-lasous, Luigi Iannone, and Serge Fdida. Dynamic and distributed packet aggregation to solve the performance anomaly in 802.11 wireless networks. In *Computer Networks*, volume 52, 2008.

[136] Ahlem Reggani and Fabian Schneider. Packet capture on home gateways: Is it feasible? Technical Report hal-00763742, 2011.

[137] Ahlem Reggani, Fabian Schneider, and Renata Teixeira. An end-host view on local traffic at home and work. In *Proc. PAM*, 2012.

[138] TechCrunch (Forrester Research). Forrester Projects Tablets Will Outsell Netbooks By 2012, Desktops By 2013. `http://techcrunch.com/2010/06/17/forrester-tablets-outsell-netbooks/`.

[139] A. Ritacco, C. Wills, and M. Claypool. How's my Network? A Java Approach to Home Network Measurement. In *ICCCN*, 2009.

[140] Fonseca Rodrigo, Porter George Manning, Katz Randy H., Shenker Scott, and Stoica Ion. IP Options are not an option. Technical Report EECS-2005-24, UC Berkeley EECS, 2005.

[141] Mario A. Sanchez, John S. Otto, Zachary S. Bischof, and Fabian E. Bustamante. Trying broadband characterization at home. In *Proc. PAM*, 2013.

[142] Mario A. Sanchez, John S. Otto, Zachary S. Bischof, David R. Choffnes, Fabian E. Bustamante, Balachander Krishnamurthy, and Walter Willinger. Dasu: Pushing Experiments to the Internet's Edge. In *Proc. NSDI*, 2013.

[143] S. Saroiu, P. Gummadi, and S. Gribble. Sprobe: A fast technique for measuring bottleneck bandwidth in uncooperative environments. In *Proc. IEEE INFOCOM*, 2002.

[144] S. Savage. Sting: A tool for measuring one-way packet loss. In *Proc. IEEE INFOCOM*, 2000.

[145] Sayandeep Sen, Jongwoo Yoon, Joshua Hare, Justin Ormont, and Suman Banerjee. Can They Hear Me Now?: A Case for a Client-assisted Approach to Monitoring Wide-area Wireless Networks. In *Proc. IMC*, 2011.

[146] Yuval Shavitt and Eran Shir. DIMES: Let the Internet Measure Itself. 35(5), 2005.

[147] Sangho Shin and Henning Schulzrinne. Balancing Uplink and Downlink Delay of VoIP Traffic in WLANs using Adaptive Priority Control (APC). In *QShine*, 2006.

[148] A. Shriram, M. Murray, Y. Hyun, N. Brownlee, A. Broido, M. Fomenkov, and k. claffy. Comparison of Public End-to-End Bandwidth Estimation Tools on High-Speed Links. In *Proc. PAM*, 2005.

[149] M. Siekkinen, D. Collange, G. Urvoy-Keller, and E. Biersack. Performance Limitations of ADSL Users: A Case Study. In *Proc. PAM*, 2007.

[150] J. Sommers, P. Barford, N. Duffield, and A. Ron. A geometric appraoch to improving active packet loss measurements. *IEEE/ACM Trans. Networking*, 16(2), 2008.

[151] Joel Sommers, Paul Bradford, Nick Duffield, and Amos ron. Improving accuracy in end-to-end packet loss measurement. In *Proc. ACM SIGCOMM*, 2005.

[152] H. Soroush, P. Gilbert, N. Banerjee, M. D. Corner, B. N. Levine, and L. Cox. Spider: improving mobile networking with concurrent WiFi connections. In *Proc. ACM SIGCOMM*, 2011.

[153] S. Sundaresan, W. de Donato, N. Feamster, R. Teixeira, S. Crawford, and A. Pescape. Measuring home broadband performance. In *Communications of the ACM*, volume 55, 2012.

[154] Srikanth Sundaresan, Walter de Donato, Nick Feamster, Renata Teixeira, Sam Crawford, and Antonio Pescapè. Broadband Internet Performance: A View From the Gateway. In *Proc. ACM SIGCOMM*, 2011.

[155] T. Chown and J. Arkko and A. Brandt and O. Troan and J. Weil. Home Networking Architecture for IPv6. `http://tools.ietf.org/html/draft-ietf-homenet-arch-03`. draft-ietf-homenet-arch-03.

[156] M. Tariq, M. Motiwala, N. Feamster, and M. Ammar. Detecting Network Neutrality Violations with Causal Inference. In *Proc. CoNEXT*, 2009.

[157] The Global Broadband Speed Test. Speedtest.net. `http://www.speedtest.net/`.

[158] The Official Netflix Blog. November ISP Rankings for the USA, Dec 2012. `http://blog.netflix.com/2012/12/november-isp-rankings-for-usa.html`.

[159] UPnP forums. UPnP specifications. `http://www.upnp.org/`.

[160] UPnP Forums. WANCommonInterfaceConfig:1, 2001.

[161] Y. Vardi. Network Tomography:Estimating Source-Destination Traffic Intensities from Link Data. *Journal of the American Statistical Association*, 91(433), 1996.

[162] Y. Wang, C. Huang, J. Li, and K. Ross. Queen: Estimating packet loss rate between arbitrary Internet host. In *Proc. PAM*, 2009.

[163] Udi Weinsberg, Augustin Soule, and Laurent Massoulié. Inferring traffic shaping and policy parameters using end host measurements. In *Proc. IEEE INFOCOM*, 2011.

[164] Jon Whiteaker, Fabian Schneider, Renata Teixeira, Christophe Diot, Augustin Soule, Fabio Picconi, and Martin May. Expanding home services with advanced gateways. *ACM SIGCOMM Computer Communication Review*, 42(5), 2012.

[165] WiGLE. Wireless Geographic Logging Engine. `http://wigle.net/`.

[166] MIMO Wireless Networks with Directional Antennas in Indoor Environments. Tae Hyun Kim and Theodoros Salonidis and Henrik Lundgren. In *Proc. IEEE INFOCOM*, 2012.

[167] Kuai Xu, Feng Wang, Lin Gu, Jianhua Gao, and Yaohui Jin. Characterizing home network traffic: An inside view. In *WASA*, 2012.

[168] Jeonghwa Yang and W. Keith Edwards. A Study on Network Management Tools of Householders. In *ACM SIGCOMM HomeNets Workshop*, 2010.

[169] Kok-Kiong Yap, Te-Yuan Huang, Masayoshi Kobayashi, Yiannis Yiakoumis, Nick McKeown, Sachin Katti, and Guru Parulkar. Making Use of All the Networks Around Us: A Case Study in Android. In *Proc. CellNet*, 2012.

[170] Yiannis Yiakoumis, Te-Yuan Huang, Kok-Kiong Yap, Sachin Katti, Nick McKeown, and Ramesh Johari. Putting Home Users in Charge of their Network. In *ACM HomeSys Workshop*, 2012.

[171] Yiannis Yiakoumis, Kok-Kiong Yap, Sachin Kati, Guru Parulkar, and Nick McKeown. Slicing Home Networks. In *ACM SIGCOMM HomeNets Workshop*, 2011.

[172] YouTube. YouTube Video Speed History. `http://www.youtube.com/my_speed`.

[173] Rui Zhang-Shen and Nick McKeown. Guaranteeing Quality of Service to Peering Traffic. In *Proc. IEEE INFOCOM*, 2008.

[174] Qing Zhao. A Survey of Dynamic Spectrum Access. *IEEE Signal Processing Magazine*, 24(3), 2007.

List of Figures

List of Tables