Homework: Putting Interaction into the Infrastructure

Richard Mortier, Tom Rodden, Peter Tolmie, Tom Lodge, Robert Spencer, Andy Crabtree

University of Nottingham, UK
{firstname.lastname}@nottingham.ac.uk

Alexandros Koliousis, Joseph Sventek

University of Glasgow, UK
{firstname.lastname}@glasgow.ac.uk

ABSTRACT

This paper presents a user driven redesign of the domestic network infrastructure that draws upon a series of ethnographic studies of home networks. We present an infrastructure based around a purpose built access point that has modified the handling of protocols and services to reflect the interactive needs of the home. The developed infrastructure offers a novel measurement framework that allows a broad range of infrastructure information to be easily captured and made available to interactive applications. This is complemented by a diverse set of novel interactive control mechanisms and interfaces for the underlying infrastructure. We also briefly reflect on the technical and user issues arising from deployments.

ACM Classification: H.5.2 [Information interfaces and presentation]: User Interfaces. - Graphical user interfaces.

General terms: Management, Measurement.

Keywords: Home network, infrastructure, interaction.

INTRODUCTION

Domestic networks have become an unremarkable feature of modern life [4], routinely used to generate and consume digital media and to access a burgeoning array of online services. The home network is no longer a novelty for many people, but rather an ordinary background feature of their lives. However, managing domestic networks currently imposes heavy technical overheads and presents critical problems for users. Residents have little or no access to facilities that provide meaningful control over bandwidth use, network access or local network policies.

To address this mismatch between the needs of residents and the nature of the technology we have adopted a user-centred approach to the creation of the next-generation domestic infrastructure. We draw upon empirical studies of home networking to suggest a set of key user-oriented desires for an interactive infrastructure. We then outline how we have re-examined the protocols and architectures of the domestic setting to incorporate these requirements within the infrastructure, opening it up to interactive systems' developers. This allows us to make key features of the domestic infrastructure available to inhabitants in a way that reflects their needs and allows non-technical users to manage and control the network.

Our focus on the underlying network extends consideration of HCI systems beyond interfaces and interaction techniques. Interaction inevitably shapes and is shaped by the nature of the underlying infrastructure. We respond to this *infrastructure challenge in HCI* [5] by undertaking end-to-end systems research that responds to the needs of users. This allows us to push interaction deeper into the infrastructure both *broadly*, in terms of which interactions the infrastructure supports; and *directly*, by adding interactivity to protocols traditionally invisible to users.

End-to-end systems research is a long-term endeavour combining extensive ethnographic study, detailed systems development, and iterative user-centred prototyping. For example, different ways of presenting and controlling the infrastructure represent significant iterative HCI research, requiring repeated deployment and assessment with users.

Our project, *Homework*, has been underway for over three years. We have previously published novel systems elements of our work [15] and the analytical orientation of our ethnographic work towards the unremarkable nature of the domestic network [4]. The core contribution of this paper is the articulation of key requirements arising from our ethnographic work; and the resulting development of a deployable interactive networking infrastructure, informed by empirical understandings of users' needs and capable of supporting a wide range of interesting uses and research interfaces. While we refer to some of our initial interfaces, these are in extensive longitudinal user trials now; their detailed presentation will be the subject of future papers.

SUPPORTING DOMESTIC NETWORK MANAGEMENT

The domestic network has become a significant focus in HCI with researchers offering insights into setting up and maintaining network infrastructure [6,7], in weaving the home network into domestic routines [16], and in users understanding their home networks [11]. As the Internet increasingly underpins more aspects of modern life it becomes a crucial element in how residents access online services and communicate with others. Unfortunately, network remain opaque to users, are often clumsy in use, and lack transparency and local accountability, e.g., [3,16].

Contemporary computer networks are built around essentially the same protocols, architectures and tools

UIST '12, October 7–10, 2012, Cambridge, Massachusetts, USA.

developed for the Internet as a whole in the 1970s. These were designed for a certain context of *use* (assuming relatively trustworthy hosts), made assumptions about *users* (skilled network and systems administrators), and tried to accomplish a particular set of *goals* (e.g., scalability to millions of nodes and resilience against node/link failure).

The role of the digital has changed significantly since the early days of the network, presenting a quite different context of use and set of goals. The home network is really quite different to backbone and enterprise networks. Domestic networks are relatively small in size. They are predominately self-managed by residents not typically expert in networking technology. They connect a highly heterogeneous collection of devices, including desktop PCs, games consoles, and a variety of mobile devices ranging from smartphones to printers to digital cameras. Furthermore, different household members routinely own and individually exercise control over their devices. Finally, home network access and use tends to be locally negotiated between inhabitants where immediate resolution of problems requires direct control over the network [17].

Infrastructure has traditionally been separated from the needs of and control by the user. This separation makes it hard for people to understand and manage their networks in support of their activities. It has also made it hard for interactive systems developers to build applications to meet inhabitants' needs. However, several recent approaches attempt to increase access to domestic networks.

Revealing the Domestic Infrastructure

A range of distinct applications have been developed that expose the underlying infrastructure to users. These include products such as Network Magic[1] that provide simple visualization and configuration wizards to aid users but provide little information on the "traffic" (data flows) in the network and only limited control of the infrastructure itself. More sophisticated support is provided by research systems such as Home Watcher [3] which exploits custom applications (*client agents*) installed on domestic machines to monitor and control network traffic. The system offers users a control panel to throttle (limit) traffic to different machines but its control is limited to those MS Windows-based personal computers where a client is installed.

As the need for users to more effectively manage the network has grown, a range of *middleware* has also emerged. Middleware conceptually sits between the network and the application, offering alternative services and more user awareness and control. Middleware-based approaches tend to offer greater measurement and control by exploiting the role of the router as the main point of contact with an Internet Service Provider (ISP). This has included capturing network layer traffic [2] and storing *flow records*, referring to aggregates of network packets travelling between endpoints, in a database collocated with the web server using custom *DD-WRT*[2] router firmware. Technology probes such as Kermit [2] provide visualizations of this data to users that have been favourably received. Other systems such as Eden [17] also exploit router facilities to offer a graphical UI with drag and drop actions mapped to underlying network facilities.

Existing work has demonstrated the advantages of presenting the underlying infrastructure to residents in domestic settings by exploring a range of visualization techniques and providing new metaphors to allow residents to configure the underlying infrastructure. However, *these researchers have had to work within the limits of the underlying infrastructure* and the specific controls it offers. As Edwards *et al* [5] argue this has restricted the design space for HCI, preventing an exploration of the new possibilities that might emerge if the underlying infrastructure mechanisms were reshaped. We wish to shift this balance of control to allow greater user involvement in the services and protocols of the infrastructure. Rather than treating the infrastructure as a pre-ordained fixed set of facilities, we wish to open it up to allow access to parts of the domestic network infrastructure that are normally either closed to or hidden from both HCI developers and users.

REDESIGNING THE DOMESTIC INFRASTRUCTURE

Our reshaping of the domestic infrastructure is informed by ethnographic studies conducted since 2009 across 24 different households. Distributed geographically around the UK, these have been enormously varied in their make-up: with younger children; with a mixture of younger and older children; with just older children; with young adults still living at home; older couples with children now living elsewhere; younger couples without children; single occupancy households (younger and older); and mixed occupancy shared households. The participants have covered a wide range of different occupations and income brackets, ranging from the unemployed, to factory workers, to a waitress living with her partner (a chef), to highly skilled professional couples.

The empirical approach to the studies has been ethnographic and has included interviews, technology tours, and self-logging of events. Our studies have been complemented by long term "in the wild" studies where we have replaced people's home routers with our infrastructure and undertaken formative assessment of the developed features. The analytic backbone to all our studies has been ethnomethodological: we have sought to elicit how people methodically reason about and account for the operation of their networks as a part of ordinary everyday practice. Details of these studies are the focus of other papers [4]; in this paper we consolidate the key issues these studies raised into a set of basic infrastructure challenges.

Key Domestic Infrastructure Challenges

To drive the reshaping of the underlying infrastructure we have consolidated our own and other ethnographic

[1] http://www.purenetworks.com

[2] http://www.dd-wrt.com/site/index

understandings of domestic settings into four key challenges each presenting distinct challenges to the underlying infrastructure. Residents routinely express the following desires: to understand network bandwidth use and ***manage consumption***; to understand network activity and ***monitor performance***; to respond to demands by ***prioritization*** of network activities and interaction; and to be able to ***police users on the network***. In the following sections we briefly illustrate each of these needs before considering the technical challenges each presents.

Managing Consumption

Residents wished to be aware of bandwidth consumption on both momentary and cumulative bases. Where bandwidth capping exists, this was often articulated at a household level: people want to know when they are approaching or have crossed a threshold above which supplementary charges or other penalties will apply. This can also relate to the bandwidth consumed by specific devices and (implicitly) people, both here-and-now and over longer time periods. Knowledge of such consumption can provide evidence for negotiation of specific rights and responsibilities, and matters of moral accountability:

I would like to see an accumulative/historical record of bandwidth usage. The current month/week/day so I can see patterns of use of time… This is important to me because we keep exceeding the Internet allowance. It has gone up five-fold because we have an international student living with us. I don't think she believes it's her who's eaten up all of the allowance!

A number of HCI researchers have developed technology probes to explore appropriate means of presenting this form of information [2] with existing infrastructures. These have been restricted to the information provided by existing mechanisms in particular infrastructure components, e.g., simple traffic statistics as sFlow/NetFlow records.

The infrastructure challenge is to provide mechanisms that will capture usage information at an appropriate level of abstraction and make it more readily available to the user. The encapsulation inherent within layered protocol stacks limits access to network traffic. HCI developers are thus left to make do with the level of traffic detection provided rather than shaping traffic measurement to meet their needs. Both operational and research approaches to traffic measurement have been driven predominantly by the needs of large backbone networks, where the focus is on capturing information about dominant traffic types to improve network efficiency. These methods do not readily map to the home where the technical context and constraints are quite different, and the need is to link traffic to user activities. It is thus difficult for developers to accurately and efficiently detect key features of importance to users. *The key requirement this challenge imposes is accessibility of data from each protocol layer, in common and extensible representations*.

Monitoring Performance and Activity

Across our various studies people expressed an interest in knowing what others are up to on the network and how the network is performing. Often it is about having a global view of the network as an object so as to reason why your own particular device is behaving the way it is:

I think occasionally we've said, y'know, someone's gone and said "Is someone torrenting?" or "Is someone running a big download?" or something like that. And then they'll go sort of "I've bought a game and it's six gig and it's a download that's gobbling all the bandwidth" …

A part of this is about having the resources to assess what impact other people's network use might be having upon your own activities. Another part is about troubleshooting, about being able to use different views of the network to disambiguate where problems might lie. Some routers already make part of this functionality available, albeit rarely and in a manner not amenable to construction of UIs:

It [The Router] shows the connectivity … and if it's wireless or Ethernet. It's just reassuring that- Well J may say I can't link for example and I can see the connection is actually on so it may be something actually on her laptop in settings rather than in the network. It's quite a nice feature.

Understanding and controlling activity can equally be considered in terms of how it is viewed, how we may be informed of it, and how we might shape or prohibit use.

The infrastructure challenge is to provide mechanisms to enable this form of monitoring and to alert users of these issues as they occur. Existing approaches to monitoring assume the recipient of information is an expert network administrator, whether in a corporate or a backbone network. As a result they provide current and historical information at an inappropriate level of detail and without necessary scaffolding for the "uninterested" home user. In the home this leads to the need to develop efficient means to undertake such monitoring in local settings in real time, and to provide the means to detect and alert users of specific traffic issues at a level that makes sense to them. *The key requirement this challenge imposes is for an event notification system that enables applications to dynamically register interest in particular changes in network state*.

Prioritization of Activities

A strongly voiced concern is that the network fails to recognize the ordinary workings of priorities and preferences within a household. Certain people may need to use the network for work, some may need to accomplish particular things at specific times of the day, certain kinds of activity may need to be accommodated on an ad hoc and contingent basis, whilst the actual operation of allocating priority between devices remains opaque. For example, those who work at home often feel that being able to prioritize devices on the network would better recognize the contribution their activities make to the household:

I see myself as using the Internet to bring in income, so I can justify that pretty well ***everything that I do takes priority****.*

On occasion this can even stretch as far as wanting to give priority to specific *individuals*, regardless of which device or application they may be using at the time:

I mean if he is asking for God knows how much to be downloading as I'm trying to download my own stuff, I want mine to take priority over what his requirements are… That would always be the case.

However, sometimes this is more nuanced and the interest is in recognizing certain kinds of higher priority activity and giving preference for however long they may last:

I use a lot of presentations. I do a lot of PowerPoint stuff and I use a lot of photographs in them, so sometimes my computer can be really slow when downloading stuff like that. So… I think that, I'm doing that activity, Give me priority now. Because it's not the sort of thing I do every day. It's the sort of thing I do regularly and when I'm doing it, it's probably over two days where I'm doing that thing on it... And there may be video stuff, that kind of thing.

For other households the interest is in having a network that can recognize the routines of the household and shape the traffic across devices accordingly, giving some priority at one time of day and others priority at another:

M: … we have had big rows about T stealing the Internet. E said to him "You've stolen the Internet!" coz he's uploading to YouTube and the whole thing just like grinds to a halt for everybody else. We have had a "You put it on overnight T when nobody else needs it".

T: Yeah so normally I just upload overnight. And that's it. … if the video files are under 50 megabytes I upload it because it only takes 5 or 10 minutes, but normally if it's bigger than that I do it overnight.

The infrastructure challenge is to provide mechanisms to prioritize and control traffic associated with different devices and user activities in real time. Existing approaches to prioritising focus on fine-tuning networks and often deal with large-scale aggregate traffic flows (so-called *traffic engineering*). Reconfiguration of such flows relies on expert judgement by experienced network operators driven by business requirements. Judgement in the home is more closely related to use and, given the subtleties involved, requires human situated judgment. This strongly suggests there is a need to involve the user in such mechanisms, and thus to embed user interaction directly within related control mechanisms. *The key requirement this challenge imposes is for primitives supporting programmable network control, at all protocol layers*.

Policing Users of the Network

A more contentious set of requirements revolves around the control of what people can do on the network. Almost inevitably, interests here frequently relate to parental desires to manage what their children do on the network:

I do use Facebook quite a lot and social networking and I know that a lot of J's friends have asked me to be a friend and I'm very strict on that. At the moment he hasn't even tried to go there but if he does then I would want certain restrictions on that as well.

It can also be about punitive responses to 'bad behaviour':

So if teacher says she's not doing homework and I think she's not doing it because she's spending her life on Facebook, I could block them and say "I'll let you have them back when your homework's done". You see that might be handy, if you could do it at the level of saying- You know, it's easy enough for me to say 'show your homework, right that's done', type something, 'right you can have Facebook now'.

I used to share a house with someone who was- … largely nocturnal and he used to do a lot of a protocol called direct connect or program and there were some evenings where there was a lot of uploading and swamping the bandwidth and the problem was if you maxed the upload on the Internet connection it just absolutely killed everything else. And, because he was a bit nocturnal, at the times when I'd really want to check email or something in the morning before going off to work- I used to have a hub, which I could sort of disconnect him from, and there were days when I used to do that just so I could get some usage out of the network

An important aspect of the above is the degree to which these things may be reasoned about on the basis of an application or its specific uses. Thus a mother may want to restrict her daughter's access to Facebook but not the whole Internet, as that might be deemed a required homework tool. Existing *platforms* do not typically support such fine grained access control though some tools can, e.g., *StayFocusd*, a Chrome browser extension, *Freedom*[3] and *AntiSocial*.[4] However, they apply to specific client devices/programs, not an *individual's* access.

Another set of requirements here relates to the degree of difficulty people experience giving other people access to their network and the wish to make that more tractable:

…In my parents' house. I think my mum's friend brought a laptop round and then it was sort of, can we get her onto our network so she can copy off her photographs from the holiday that they've all been on across. It caused some problem. I set them up with MAC address only rather than a code. So it was a case of actually having to go and sort that out and log on and add her computer's MAC address to the list. I think for many people this is a big faff…

The infrastructure challenge is to provide mechanisms that make it much easier to police users of the network, managing their access and what exactly they may or may not do when connected. This requires us to consider how we might exercise control locally within the network and to make these controls available to users. Current approaches to policing tend to be removed from the point of use and consequently broad-brush in nature, focusing on wholesale blocking of access to particular sites or services by all, or denying particular devices any form of connectivity and thus access to any site or service. In practice the highly contingent nature of policing in the home is much finer grained and more dynamic in nature. *The key requirement this challenge imposes is for policy and access control primitives that more closely match human practice rather than network state*.

While we have suggested four broad classes of need within the domestic setting we stress the significant diversity of users and uses of the network visible within our, and other, studies. This strongly indicates the need for iterative development of appropriate interfaces and applications with these users. However, before we can begin a process of iterative refinement of these interfaces and applications, we must first develop appropriate underlying interactive mechanisms within the infrastructure. Our aim is to provide open infrastructure that promotes exploration of a range of different styles of interaction with the underlying network.

REALISING A NOVEL INFRASTRUCTURE

The results of our ethnographic work underpin the shaping a new network infrastructure, which we now describe in

[3] http://macfreedom.com/
[4] http://anti-social.cc/

detail. We exploit the arrangement of the home network to adopt a gateway model to changing the infrastructure [12] in response to user needs emerging from our studies. This allows us to reinvent key infrastructure mechanisms locally without changing the Internet as a whole. We have developed a dedicated router from the perspective of the home user, re-examining the means through which network information is collected and the network controlled. As part of this redesign of the infrastructure we have developed:

- A scalable and dynamic measurement infrastructure designed to make available information about the behaviour of the network to interactive user applications.
- A set of mechanisms that exploit user engagement and interaction to allow direct control of the network.

Our aim is to provide an open infrastructure that allows an exploration of a range of different styles of interaction with the underlying network. Our router has been deployed in a range of domestic settings and supports several user interfaces currently undergoing iterative refinement. Our open-source code is online at http://github.com/homework/.

Externally our setup is similar to operator-provided home routers, where one box acts as the wireless access point, uses a wired connection for upstream connectivity to the ISP, and may provide a small number of other wired interfaces. Our router (Figure 1) is deployed over Linux 2.6 on an eeePC. An active database provides an integrated network monitoring facility to applications [15]. We treat the router as an OpenFlow device using the Open vSwitch and NOX implementations – OpenFlow is a network control standard [10] described briefly below. Our router uses OpenFlow datapath rules to control access and connectivity, both upstream and local, of devices.

In the rest of this paper we detail how our router provides the interactive infrastructure needed to capture a rich picture of network behaviour and make this available to users. We then present our distinctive control infrastructure, which enables direct involvement of users in the day-to-day management of the network.

CAPTURING ACTIVITY ON THE HOME NETWORK

"if all the traffic goes through that box ... why can't I see it?"

Home routers embody the invisible nature of current digital infrastructures. They provide a network for wired and wireless devices in the home and act as a gateway to the Internet. Consequently, all traffic in the home typically flows through the domestic router. The router is designed to handle this traffic efficiently and to ensure that it is appropriately *routed*, i.e., correctly passed on toward the correct destination. However, it provides few facilities to capture this information or make it available to applications wishing to surface the nature of the network to users.

The first infrastructure challenge the Homework router addresses is how to capture traffic information efficiently and make this available to applications. To do this our router includes an active measurement database that provides a focal point for information collected about the

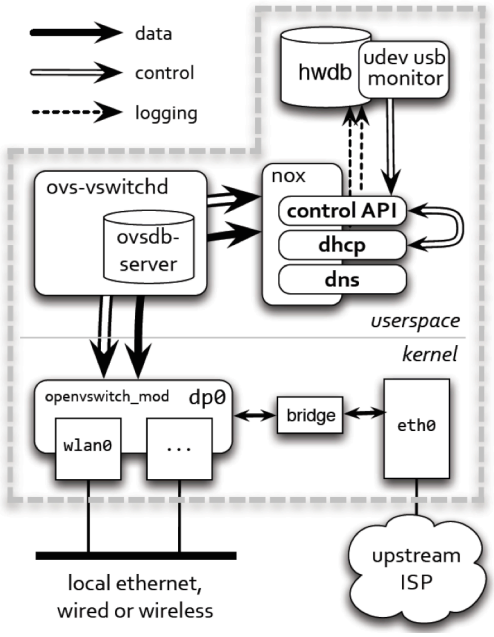

Figure 1. The Homework Router architecture. Open vSwitch and NOX manage the network interfaces. Three NOX modules provide a web services control API, a custom DHCP server, and a DNS proxy.

infrastructure. It offers network visualisation and control applications an extensible facility where dynamic information about the state of the infrastructure is collated.

The measurement database is composed of three distinct components. An *ephemeral timeseries component* holds the most recent (complete) data received from monitoring processes. The continuous, large volume of such data makes it infeasible to persist it all, and demands careful implementation to keep up. A *persistent timeseries component* holds (selected) timeseries data for later use, and a *persistent relational component* stores derived information unrelated to the time of occurrence, e.g., machine details and the daily volume of data.

We use *libpcap* to intercept packets and process to generate appropriate table entries, e.g., flow records. Through careful implementation, no deployment has yet recorded significant loss as a result, in contrast to naïve use of *tcpdump*, reported as initially seeing 10% packet loss [1].

The ephemeral component of the database implements an extended version of the Stanford STREAM Data Manager.[5] Applications access it via a lightweight UDP-based Remote Procedure Call (RPC) system that exchanges request packets (queries) for response packets (data). We have C/C++ and Java bindings that have been tested on Linux, Windows/Cygwin, OS/X, iOS and Android.

Applications periodically query the ephemeral component either for raw events or derived information. This is used

[5] http://infolab.stanford.edu/stream/

directly by user interfaces or stored for subsequent use. There are three default persistent timeseries tables:

- A ***flows table*** captures network traffic by recording the number of packets and bytes associated with a particular (transport level) type of traffic in the preceding second, recording protocol, source and destination information. This allows us to monitor bandwidth usage in the home.
- A ***links table*** captures wireless device information by recording the received signal strength, number of retries, and number of packets associated with a particular device. This allows us to show machines within range of the network, and the wireless topology of the setting.
- A ***leases table*** captures connection to the network by recording when a *DHCP lease* (see below) is granted to a device, or a lease is revoked. This allows us to indicate the status of machines connected to the network.

Figure 2 shows the schema associated with each table.

Table	*Attributes*
Flows	Protocol, src/dst IP addresses, src/dst ports, # packets, # bytes
Links	MAC address, RSSI, # retries, # packets
Leases	Action, MAC address, IP address, host name

Figure 2. The default Homework Database schemas.

The measurement infrastructure is designed to be extensible beyond these core tables allowing additional information about the domestic context to be collected, e.g., arrival and departure of people in the home, or logged interactions with different devices. Applications can exploit and contribute to this time ordered set of heterogeneous data to capture information about users' interactions as they manipulate the infrastructure. The result is a rich log of network activity and user interaction.

Coordination and User Notification

The Homework Database also acts as a central point of coordination for infrastructure services. *Listeners* subscribe to particular tables, and are then invoked when a datum is added to that table. Among these listeners is a user-level notification service that can be configured to notify users of critical network events. It can currently use email, SMS, Twitter and Growl to deliver events to users as desired.

Our notification service plays a critical role in informing users of changes in the infrastructure across a heterogeneous range of devices. For example, if the infrastructure blocks Internet access for a particular device, we can send a message informing the user of this fact.

CONTROLLING THE INFRASTRUCTURE

The router's measurement infrastructure is complemented by a set of user-oriented control mechanisms enabling interactive management of the network. We treat the Homework Router as an OpenFlow device. An OpenFlow *switch* has three parts: a *datapath,* a *secure channel* connecting to a controller, and the *OpenFlow protocol* used by the controller to talk to the switch.

Each OpenFlow *datapath* contains a set of physical ports, plus a table of flow entries with a set of actions associated with each flow entry. Flows are defined in terms of the input datapath and selected values of packet header fields. There are four basic types of action, ranging from simply dropping or forwarding the packet, to forwarding it to the controller for further processing, to forwarding it through the switch's normal processing pipeline. Packets can be selectively modified as they are forwarded.

Open vSwitch[6] is an implementation of OpenFlow running on Linux. It implements a datapath as a kernel module that can be configured to control one or more physical or virtual interfaces. The OpenFlow protocol used to communicate with the datapath is provided as a userspace process, *ovs-vswitchd*, which also maintains a device configuration database. In the current implementation the datapath's flow table supports exact-match rules only; packets that do not have an exact match are forwarded for processing to the *ovs-vswitchd* process that maintains all wildcard rules. Packets that do not match a rule are sent to the controller.

Method	*Function*
/permit: <eaddr>	Permit access by specified client
/deny: <eaddr>	Deny access by specified client
/status: [eaddr]	Retrieve currently permitted clients, or status of specified client
/dhcp-status/	Retrieve current MAC—IP mappings
/whitelist: <eaddr>	Accept associations from client
/blacklist: <eaddr>	Deny association to client
/blacklist-status/	Retrieve currently blacklisted clients
/permit-dns: <eaddr> <domain>	Permit the specified device to access the given domain
/deny-dns: <eaddr> <domain>	Deny access to the given domain by the specified device

Figure 3. Homework Router web API. All methods are prefixed *https://…/ws.v1/*. <*X*> and [*X*] denote required and optional parameters respectively.

In our router, the controller controls just a single datapath that manages all but one of the network interfaces on the eeePC. It implements filtering to control wireless association, and a custom DHCP server. These software processes exercise control by managing rules in the OpenFlow datapath to control both access of devices within the home, and their local and upstream connectivity. The controller presents a simple web RPC interface (Figure 3). The datapath forwards traffic destined upstream for local processing via the built-in bridge, with Linux's *iptables* IP Masquerading rules providing standard NAT functionality.

Having described some of the core technical elements of the router itself, we now discuss how we have extended and used this infrastructure to allow direct involvement of users in the day-to-day management of the network.

[6] http://openvswitch.org/

PUSHING INTERACTION INTO THE INFRASTRUCTURE

Using our infrastructure we have exploited three strategies in response to the challenges involved in managing consumption, prioritization of network activities and interaction, and policing network access. Each illustrates a different means of placing interaction in the infrastructure:

1. **Putting people in the protocol** by embedding user interaction in existing infrastructure protocols. Encapsulation has traditionally meant that these protocols make no reference to users.
2. **Bringing services closer to users** by allowing greater control and configuration. Infrastructures have traditionally designed these services to be remote and neutral with respect to use.
3. **Exploiting the physical arrangement of the home** by manifesting infrastructure in the home. Infrastructures have traditionally sought to be independent of the physical setting and so seldom exploit its affordances.

In the following sections we will briefly illustrate how we exploit each of these strategies in on-going deployments.

Putting People in the Protocol

A key example of this strategy is our manipulation of the *Dynamic Host Configuration Protocol* (DHCP). In order to use IP (i.e., the network layer, and everything above it) a device must have a valid *IP address*. DHCP is an application protocol that allows a device, upon discovering it is connected to a network, to *request* an IP address that is valid for that network. A network's DHCP server allocates addresses to devices and records each device's *MAC address*. This is set in the factory and is often used to identify the device as it never normally changes, even when a device moves between networks. This process is normally invisible to users and there is no mechanism to involve users in responding to the request for a valid IP address. The result is that machines join and leave the network unbeknownst to users who have no opportunity to control access to the network beyond blanket permit/deny policies.

We implemented a DHCP server within our router as a NOX module, enabling interface devices to control which devices will receive an address via the simple web API (Figure 3). As well as recording DHCP leases in the lease table and providing awareness of who is on the network, the server provides control over the leases it grants. When devices are first detected, they are placed in a requesting pool and this is flagged in the leases table. Applications subscribed to the leases table are then made aware of this request and can inform users. Users then respond to the request by interacting in some application specific manner, and the application completes the process by invoking the web API. The router drops all traffic from devices that have not been permitted, allowing machines to be selectively prevented from using the network.

This facility may be exploited in a number of different ways by HCI developers. The interface in Figure 4 is an example of a situated noticeboard interface exercising this functionality that we are currently exploring with users. Requesting machines appear in the central display panel. Any user with access to the display may then choose to drag any device to the right. Doing so invokes the web API on the router to mark the device (specifically its MAC address) as "permitted", granting it an IP address and enabling its traffic to be routed.

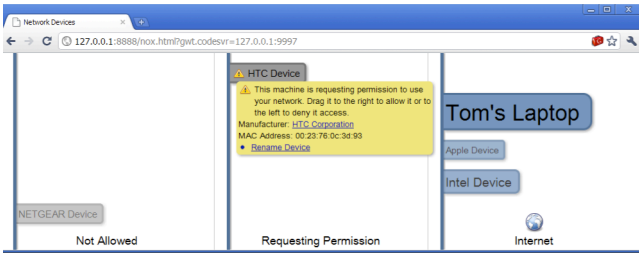

Figure 4. Control panel showing an HTC device requesting connectivity.

This control is enabled by the combination of publishing information about DHCP leases and enabling direct interaction in the protocol by the user to complete address allocation. Obviously, user involvement may take other forms depending on the interaction and management styles at play. For example, we may provide an alert to the mobile device of one of the residents requesting permission for this machine to connect. The means of presenting this facility appropriately and understanding its utility obviously requires significant HCI research. Our contribution is in embedding interaction within the protocol so as to enable different forms of user involvement.

Bringing Services Closer to Users

Our custom realization of another service illustrates our second strategy of localizing standard services to the specific home. The *Domain Name System* (DNS) is a standard Internet service that translates computer names (e.g., as appear in website URLs) into IP addresses. This *must* be done before an application such as a browser can communicate with the named computer because the IP protocol uses only IP addresses, not names. For example, when a user opens *facebook.com* in their web browser the browser first resolves the name 'facebook.com' into an IP address using DNS, and only then can it request page(s) from the Facebook server(s), using that IP address.

In a typical home network DNS requests from every device are sent to the router, which passes them on to a *DNS server* in the ISP's network. This server may query several other servers before returning a response, which may then be *cached* by both the home router (to answer subsequent requests) and the original requesting device.

In contrast, we have incorporated a DNS proxy into the home router itself, which we have extended to allow *specific devices* to be permitted or denied the ability to access *particular names* (such as facebook.com). Shifting the service closer to the point of use allows us to involve users and the context of use, as part of the name resolution in this case. In this way we can provide quite fine-grained

control (e.g., per device, per user) over access to external services hosted at those locations.

The DNS proxy is implemented as another NOX module. DNS requests are intercepted by the proxy and dropped if the requesting device is not allowed access to that domain, preventing the initial lookup. In addition, any traffic the router encounters that is not already permitted by an explicit OpenFlow flow entry has a reverse lookup performed on its destination address, using a local cache of recent DNS requests to provide acceptable performance. If the resulting name is from a domain that the source device is not permitted to access, then a rule will be installed to drop related traffic. This prevents access to sites if the user directly enters the IP for a forbidden domain name, or if the device was previously allowed access and has cached the IP address but is no longer permitted access.

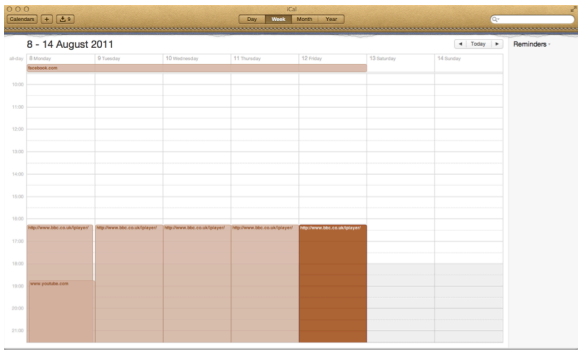

Figure 5. Diary showing restrictions for a given user.

Implementing such fine-grained control over the different sites that a given user's devices can access is very difficult, perhaps impossible, to perform successfully *upstream* in the network, e.g., by the ISP. Different users using different devices within the household have different policies for accessing different sites at different times: it is not possible to define a successful one-size-fits-all policy, and the ISP cannot easily identify user devices in any case. In contrast, local intervention in name resolution enables us to build a router that *can* provide the necessary degree of control.

Again this facility may be presented to users in a variety of ways. For example, we exploit an iCal feed to expose this behaviour to the user via a standard calendar application, showing which sites a user is barred from accessing at which times. This enables, e.g., a parent to control access by their children's devices to sites like Facebook, restricting them to (say) particular times (Figure 5).

Designing an appropriate means to present this level of control to users obviously requires iterative user-centred development. It is also likely to surface potentially contentious issues of control, trust, and power. Indeed, we have already started to find these within our own studies of interface deployments. Our contribution of localizing the service within the home enables this fine grained control to be exercised, opened up to user-centred investigation and specialized to the particular household: it will be sensitive to *that household's* specific, complex, changing demands, and able to reflect negotiations that take place between the various actors, homeowner and guest, parent and child.

Exploiting Local Physical Arrangements

The final strategy we explore is to exploit knowledge of the local situation to drive control. Although placed within our homes, devices have few means to access the nature of the setting and exploit this to control the network. Equally, the infrastructure has limited physical manifestation in the home that users can exploit.

As well as monitoring traffic, the database at the core of our router allows us to coordinate network control with user activities and actions in the physical home. This might include recognition of particular devices and individuals with results placed in the ephemeral timeseries database.

We currently use a simple USB memory stick as an exemplar implementation as these are cheap and readily available. Use of the USB key to provide access control is straightforward: inserting the key in the router enables the devices specified on the key to connect to the network. When the key is removed, access by those devices is revoked. A USB hub connected to the router is placed in a publicly available location allowing USB keys to be easily inserted and removed. Physical access to the USB hub is required to gain access to the network.

Our implementation uses the Linux *udev* subsystem to detect insertion and removal of the USB key. When a key containing appropriate metadata is inserted, the router reads the metadata specifying the MAC addresses of the devices to be permitted, and invokes the NOX controller's web service interface accordingly. Upon removal of the USB key, all devices for which it had been permitted access have their OpenFlow rules removed, denying subsequent access.

As with other forms of control the means of presenting this to users will require a significant amount of HCI research. Our redesign of the router provides the mechanism to link between users' activities and actions in the physical space, and the control elements of the router. Placing both detailed network information and interactive activities in the same active timeseries database allows us to explore a wide set of interrelationships between users' activities in the home and the consequent control of the network.

THE INFRASTRUCTURE IN ACTION

This paper has detailed the changes to the underlying infrastructure made in response to the challenges of home networking. Our first deployment of this router began in October 2010. We have since undertaken a rolling programme of deployments to drive interface refinement. The router has subsequently been deployed in 12 homes, each deployment lasting at least 3 months. It has also run continually in two project members' homes since summer 2010. Our deployments have considered both technical and user-related issues and so we conclude with brief reflections on the deployments from both perspectives.

Technical Reflections

The Homework Router has been successfully deployed in a range of homes in the UK as described above with very few issues. Our measurement system has little impact on the performance of the router. The router provides an ideal point of traffic measurement in the home [1]. As in the case of projects such as Bismark [14] we have been able to capture a significant amount of traffic information.

While the Bismark router focuses on ISP measurement, our local measurement facilities allow us to capture a richer picture of traffic within the home. For example, during one month, one of our households the router observed: 16 unique devices obtaining DHCP leases and connecting to the network; 4578 unique devices on the wireless network; ~54GB of data in ~94M packets; and IP flows from 178,321 unique sources to 309,473 unique destinations.

During initial deployments we noted that P2P traffic within the home was not visible to the router. Given the growing importance of traffic from storage and media servers in the home, this was a significant omission in any router-based measurement approach! This invisibility is due to the router switching traffic between wireless devices as if those devices are connected via a single Ethernet segment, rendering it invisible to the router at the IP layer. To compensate for this and ensure that *all* traffic is visible to the router, the DHCP implementation in our router pays careful attention to the way in which IP addresses and subnets are allocated: it ensures each device is allocated a distinct IP subnet forcing all traffic to be IP-routed by the Homework Router, rather than simply Ethernet-switched.

Note that the use of standard WPA2 security mechanisms means that *all non-broadcast traffic incurs no extra overhead*. Under WPA2, each device creates a distinct cryptographically secure channel with the access point: data between two devices must thus travel via the access point anyway so that the necessary decryption and re-encryption can take place. Allocating each device to a distinct subnet simply forces each packet to be made visible to the IP layer on the access point. Extra overhead occurs only for packets broadcast to the local subnet: under normal operation, a shared group key would be used allowing the transmitting client to encrypt traffic so that all other connected clients could receive it directly. Due to the use of distinct subnets such traffic must instead be sent to the access point, which must decrypt it before replicating and retransmitting to each connected receiver.

Usability Reflections

The router has been used to support the development of a range of interfaces that make the infrastructure more visible and promote increased user control. Each interface embodies different interaction styles and raises distinctive issues. These interfaces have been placed in households for extended periods of time and are subject to an on-going process of iterative user refinement. During that time we have seen a broad shift from richly featured applications providing a single management application for the network to a set of lightweight apps with more specific information.

It is worth noting that while iterative refinement of interfaces is relatively straightforward, changes to underlying infrastructure (e.g., our DHCP implementation) require considerably more engineering effort. In this section we wish to reflect on a number of broad lessons can be extracted from our deployments.

The invisible nature of a mundane infrastructure

We are particularly interested in how the infrastructure and its interfaces become a mundane part of everyday live. Consequently, we didn't scaffold our studies with particular user tasks. A notable feature across all deployments is the unremarkable nature of the home network. Users are uninterested in the day-to-day operation of the infrastructure and this was reflected in the orientation to many of the interfaces, which were initially explored as curios reflecting the technical nature of the network. People became less curious about who was routinely consuming resources or even accessing the network, an effect that is mirrored in a variety of smart meter energy displays and other public displays [9]. Our users soon forgot passive network displays unless there was a distinct prompt or purpose. Consequently, we found a growing need to notify users of significant events and exploited the user notification facility of the infrastructure to push network events at users through a range of media.

Increasing network information increases social discord

A striking feature of our deployments was the extent to which everyday family life is now predicated on network-based digital services. Network activity is now intertwined with the moral ordering of the home [4]. Revealing network traffic is not a neutral action in the home and can have significant negative impact on the dynamics of the home. A notable example arose in one household where a member suggested understanding traffic would help dealing with a a long-term overseas student visitor who was causing the household to exceed a bandwidth cap. Our interfaces did indeed reveal that the majority of traffic was from the guest's device. However, resolving the issue was more problematic with a number of tense conversations drawn out over succeeding weeks. The key role the interface served was to draw attention to the phenomenon, which may actually have *increased* tensions, making resolution harder. It remains unclear what might be the most effective ways of revealing information to all stakeholders.

The challenge of privacy

Domestic settings have quite subtle privacy issues often associated with awareness of actions across a family. Monitoring tended to be at client screens by looking over users' shoulders. People were strategic about where they would access services. People also exploited browser histories both to occasionally monitor use and to ensure their past use was no longer available for inspection.

Changing the infrastructure in the manner that we have alters the visibility of the network. Information about the activities of a range of clients is now available through the network, with the router providing a single point of record

and audit for network activity. The raises a host of new privacy challenges. Who should control this? How broad should access be? How are activities identified and audited? Consider the current use of browser histories: to view your browser history requires access to your device(s). This allows users significant and subtle control of their privacy. However, if the browser logs of all clients are made available through the router this social mediation is altered. Addressing these challenges is complex and is a focus of our ongoing longitudinal study; even in the early stages our data indicates a need to provide techniques for users to maintain some ambiguity in their online actions.

Managing the network is managing the household

Our deployments also highlight the home network as an everyday social object within the household. Interactions within the network are embedded within a host of other social interactions in the household and must be understood in these terms. This is particularly important in terms of network control where changes to the network are subject to a host of domestic judgments. Throttling traffic from a particular device makes a statement about the relative importance of that family member's activity on that device. Blocking traffic from a device to a particular site makes a clear statement of the acceptability of that particular behaviour. Denying access from a guest's device to your home network inevitably has implications for, and causes inferences to be drawn as to, your relationship to the guest.

While all users in all of our deployments enthusiastically requested control of this form they also shared considerable reluctance in the active *use* of such mechanisms in the network. In fact, they welcomed the potential (threat) provided by the control mechanisms but did not see them as a substitute for the nuanced negotiation involved in discussing network use in the family. Using these network-based control mechanisms was seen as the culmination of a longer process of discussion and negotiation: many felt they would only turn to network control mechanisms as a last resort. Thus, although users did not anticipate routine use of these facilities, they felt their existence was crucial in framing discussions of network use.

CONCLUSION

We have presented a reshaping of the home network informed by studies of network use. This required us to recreate the underlying infrastructure to provide greater access to and control, allowing a broader range of interactive possibilities to manage of the infrastructure. This demanded we move beyond a focus on user interfaces, to place interaction deeper into the infrastructure by amending how the underlying network deals with protocols and services. As users increasingly interact through an ecology of devices connected to a complex network, interactive systems developers must consider how they shape underlying systems and services to meet user needs.

While we have focused on the infrastructure of the digital it is worth observing that a host of other infrastructures (water, energy, transport) are also becoming digitally rich, altering our visibility of them. The interactive issues surrounding an infrastructure are subtle: we wish it to be simultaneously unremarkable and invisible in use while providing enough information to orientate our activities [13]. This sociotechnical balance requires reflection of understanding of users throughout the infrastructure

ACKNOWLEDGEMENTS

We would like to thank Keith Edwards for his comments on a draft of this paper. This work was supported by RCUK/EPSRC awards EP/G065802/1 and EP/F064276/1

REFERENCES

1. Calvert, K. *et al*. (2010) "Instrumenting Home Networks", *ACM CCR*, 41(1), pp. 84–89.
2. Chetty, M *et al*. (2011) "Why is my Internet slow?: Making network speeds visible." *Proc. ACM CHI*, pp.1889—1898.
3. Chetty, M. *et al*. (2010) "Who's hogging the bandwidth? The consequences of revealing the invisible home", *Proc. ACM CHI*, pp.659–668.
4. Crabtree, A. *et al*. (2012) "Unremarkable Networking: The Home Network as Part of Everyday Life", *Proc. ACM DIS.*
5. Edwards, W.K. *et al*. (2010) "The Infrastructure Problem in HCI", *Proc. ACM CHI*.
6. Grinter, R. *et al*. (2005) "The work to make the home network work", *Proc. ECSCW*, pp.469–488.
7. Grinter, R. *et al*. (2009) "The Ins and Outs of Home Networking: The Case for Useful and Usable Home Networking" *ACM ToCHI*, 16(2):1–28, June 2009.
8. Grudin. J. (1990) "The computer reaches out: the historical continuity of interface design". *Proc. ACM CHI*, pp.261–268.
9. Huang, E. M. *et al*. (2006) "Displays in the wild: Understanding the dynamics and evolution of a display ecology." Proc. Pervasive, Dublin, Ireland.
10. McKeown, N, *et al*. (2008) "OpenFlow: enabling innovation in campus networks", ACM CCR 38(2).
11. Shehan-Poole, E. *et al*. (2008) "More than meets the eye: transforming the user experience of home network management", *Proc. ACM DIS*, pp.455–464.
12. Shehan, E., Edwards, W. K. (2007). "Home networking and HCI: what hath god wrought?" CHI '07: ACM
13. Star, L., "The ethnography of infrastructure," American Behavioural Scientist, vol. 43, no. 3, pp. 377-391, 1999.
14. Sundaresan, S., de Donato, W., & Feamster, N. (2011). Broadband Internet performance: A view from the gateway. Proc SIGCOMM 2011, Toronto.
15. Sventek, J. *et al.* (2011) "An Information Plane Architecture Supporting Home Network Management", *Proc. IFIP/IEEE IM.*
16. Tolmie, P., *et al*. (2007) "Making the home network at home: digital housekeeping", *Proc. ECSCW*, pp.331–350.
17. Yang, J. *et al*. (2010) "Eden: supporting home network management through interactive visual tools", *Proc. ACM UIST*, pp.109–118.