A Cooperative Approach to User Mobility

Robin Kravets
Department of Computer Science
University of Illinois, Urbana-Champaign
rhk@uiuc.edu

Casey Carter
Department of Computer Science
University of Illinois, Urbana-Champaign
ccarter@uiuc.edu

Luiz Magalhães
Department of Computer Science
University of Illinois, Urbana-Champaign
magalhae@uiuc.edu

ABSTRACT

We present a networking model that treats a user's set of personal devices as a MOPED, an autonomous set of MObile grouPEd Devices, which appears as a single entity to the rest of the Internet. As the user moves through different environments, the devices cooperate as a coordinated local area network that provides the user the desired mobile services. All communication for a user is directed to a single point of presence on the Internet, essentially an IP address for the MOPED. These personal devices can cooperate to achieve better resource utilization, such as by sharing available communication bandwidth. We present the basic networking functionality necessary to enable the operation of MOPEDs, and their integration into the Internet. We introduce a middleware layer to extend IP routing to work with MOPEDs, and a lightweight IP encapsulation protocol, Multipath Routing enCAPsulation (MRCAP), used to implement that middleware.

1. INTRODUCTION

Trends in mobile communications have resulted in two significant developments. First, advances in processor technology, both in increased processing power and decreased energy consumption, have led to the creation of a new breed of small intelligent devices from palmtops, to PDAs, smart phones, and other wearable devices. Many, if not all, of these devices have some form of wireless communication. As users collect multiple small computing devices, the amount of communication resources available to the user increases and so the demand for coordination of resources through these devices increases. Second, increasing demand for wireless connectivity has produced rapid deployment of many new wireless technologies, with overlapping coverage in some areas. Considering the set of devices supporting a user, at any point in time, some subset of these devices may have connectivity. The convergence of these two developments presents a new challenge to provide coordination of a user's devices to provide better connectivity, and potentially more communication resources, to the user.

As a user acquires multiple personal technology and communication devices, the efficiency of these devices is limited by their isolation from each other. When the resources of a device are completely consumed (e.g., a dead mobile phone battery), the user is completely cut off from key services. Similarly, if a user leaves the coverage area of a device, the services currently available via that device are no longer accessible. As a user moves through different environments, the cooperation of devices brings the potential for increased bandwidth and better connectivity by exposing to all devices the aggregation of services available to individual devices. Current technology and communication support provide connectivity between devices, but do not enable cooperation between devices. The goal of our research is to bridge this gap from communication to cooperation.

This collection of devices to support a mobile individual demands the extension of the mobility paradigm from an individual device to a network of devices. In this paper, we present a networking model that treats a user's set of personal devices as a MOPED, an autonomous set of MObile grouPEd Devices, which appears as a single entity to the rest of the Internet. All communication traffic for a MOPED user is delivered to the MOPED, where the final disposition of traffic is determined. Since a MOPED is designed to support a single user, communication with any of the devices in the MOPED is equivalent to communication with the user. This model enables the mapping of a group of devices into a point of presence on the Internet for a user. To the outside world, this MOPED appears as a single device with a single interface or identifier. In reality, the group of devices cooperates to provide better services to the user.

The MOPED architecture enables localized cooperation of devices through the concept of a MOPED *component*, a subset of the user's devices connected via a Personal Area Network (PAN), enabling the desired sharing of resources among those devices. As the user moves through different environments, the devices cooperate as a coordinated local area network. As part of a MOPED component, a device's resources are added to the pool of resources available to the component in that environment. If the user needs to make a connection from a device which currently has no external connectivity, the connection will be routed through a device that *does*have external connectivity. Since the goal of the MOPED is to support a single user, management of the MOPED's resources can be solved based on the needs and preferences of the user. In contrast to traditional networks, a MOPED component can be considered as an ad-hoc network that represents a distributed virtual device. This connectivity enables external connectivity to all devices when any one device has external connectivity.

The goal of the MOPED project is to provide service to a user through the cooperation of the MOPED devices that is better than the service provided by the devices working individually. Our solution provides four key benefits. First, a user can be connected via any of the services currently available to the individual devices. Second, if multiple devices have connectivity in a certain environment, the MOPED can take advantage of the additional bandwidth by routing different flows through different connections. Third, devices with no external connectivity can share the resources of other devices with external connectivity in their component. Finally, such connectivity enables smooth handoffs as individual devices gain and lose connectivity, allowing external connectivity to all devices as long as at least one device in the component has external connectivity.

In addition to improved service, the design of the MOPED architecture provides three additional benefits that ease the integration and deployment of MOPEDs. First, our design supports the commonly accepted idea that non-mobile users should not have to be aware of the extra infrastructure needed to support mobile users. Our architecture supports communication with non-mobile-aware users as well as optimizations for mobile-aware users. This abstraction also provides the benefit of hiding the topology of the MOPED from external hosts, providing flexibility and anonymity. Second, any new device acquired by a user can be integrated into the MOPED as long as it can become part of the PAN connecting the MOPED. This covers the easy inclusion of new technology as well as legacy devices. The level of cooperation of the individual devices in the MOPED depends on whether or not the device is MOPED-enabled. Finally, the sharing of communication resources across devices allows each device to be specialized to its specific purpose – A smart watch need not also be a phone.

In Section 2, we present the motivation for MOPEDs, and discuss constraints on their design and the challenges involved in integrating MOPEDs into the routing structure of the Internet. In Section 4, we present our design decisions in the context of related research in the area of mobile computing. Section 5 describes our solution, the MOPED Routing Architecture (MRA), including the lightweight IP encapsulation protocol, MRCAP. Finally, Section 6 evaluates the work and briefly discusses our prototype implementation.

2. MOTIVATION

The design of the MOPED architecture is based on two basic assumptions. First, we believe that a user should be able to create a representative presence on the Internet. All communication to a user is directed through this presence. A user may even create multiple presences (e.g. business, personal). By providing a unique network name for this presence, the user is in essence built into the network infrastructure. All communication destined for that presence is addressed to a unique identifier. Second, correspondent hosts need not, and in fact should not, be aware of how the user realizes a presence. The mapping of this identifier to an actual end host is dependent on the devices and infrastructure used to support the user. The MOPED architecture provides flexibility in the coordination of the user's device or devices, while maintaining transparency to correspondent hosts.

The realization of a user's presence can involve one or more devices. If a user has a single device with a single interface (e.g., a cell phone, laptop), the device, and so the user, can be supported via existing techniques such as cellular telephony or mobile IP [14]. If the device has multiple interfaces, each interface can be used as available [19] or simultaneously [22]. We believe that the next logical step is to support a user via multiple devices.

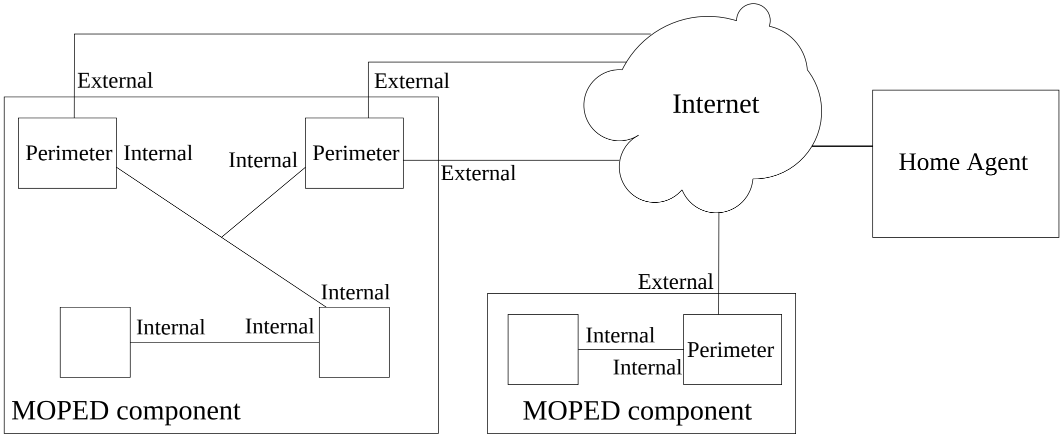
Consider a group of devices connected in a personal area network (PAN) via a wireless technology such as BlueTooth, Infrared or wireless Ethernet. If any one of the devices is within its service area, cooperation between the devices can provide connectivity to all of the devices. In this context, a user's devices can be represented as a mobile network, which may have multiple means of connectivity to the Internet at any point in time. In reality, we do not expect all of a user's devices to always be connected in one PAN. If a user leaves their laptop on a desk and walks away with their phone, the short-range connectivity between the two devices will disappear.

In order to provide support for such scenarios, we place no constraints on the topology of a MOPED. A MOPED may be composed of many devices, only some of which can communicate directly with each other and some of which have direct Internet connectivity. A device that can communicate with the Internet is termed a "perimeter node", while a device that can communicate with the Internet only indirectly through other devices is an "internal node". A set of devices that can reach each other using paths that pass only through internal interfaces a MOPED component, or connected component (from the graph representation of a MOPED). It is possible, and even expected, for a MOPED to be partitioned into multiple components, and still continue to function normally, provided that each component has at least one external interface through which it can communicate with the other components. An example MOPED is depicted in Figure 1. We expect partitioning to occur frequently in a MOPED, such as when the user carries some of the communicating devices out of their limited range. We also expect devices to enter and leave the MOPED with reasonable frequency.

The components of a MOPED can be considered as nodes in a star-like overlay network, where the Internet point of presence for the MOPED (accessed via the user's unique identifier) is at the center of the star. This point of presence can be supported via a home agent similar to MobileIP. Due to the potential of multiple external connections for each MOPED component, there may be multiple paths between each component and the home agent. As we mention above, only one external connection is necessary to support connectivity to a component. This multiplicity of connections goes beyond simple connectivity and provides the possibility for increasing the resources available to the component, as well as to an individual device.

Consider a MOPED component comprised of a PDA with a cellular modem, a cell phone, and a laptop with no connectivity, all connected in a PAN (see Figure 1). If the user is talking on the phone, other connections to the laptop can be routed through the PDA. To support this, the home agent can route flows for different endpoints to the appropriate external interface. If the user is participating in a videoconference on their laptop, the audio could be routed through the phone, while the video could be routed through the cellular modem, providing more bandwidth to the application than had only one of the interfaces been used. Since the endpoint of the communication is the laptop, traditional routing support will not allow the separate flows to the same endpoint to be routed along different paths. Finally, consider a single application whose communication requirements for a single flow are more than the bandwidth provided by either of the external connection. In this case, specialized transport protocols [7, 6] can utilize all available bandwidth by inverse multiplexing a single flows data across multiple

Figure 1: A MOPED with two components and six devices



paths. In order to support these last two scenarios, the MOPED architecture provides flow-based and packet-based routing in order to realize the potential bandwidth improvements.

3. MOPED DESIGN RATIONALE

One consequence of the proliferation of personal communication devices is the complexity of individually addressable communication endpoints. Increasing the possible number of ways to communicate with a person makes it significantly more challenging to determine which method is the "best" in a given situation. The introduction of MOPEDs changes the paradigm for mobile communications, defining communication with any of the devices in the MOPED to be equivalent to communication with the user. Many current solutions are focused on a single host with one network interface [14, 1, 11], while other research seeks the ability to address and locate a person and the device they are currently using [9]. We believe that the appropriate next step is mobility management for a MOPED, the network of devices that is associated with one person.

In order to better support the user's needs, a MOPED may interact with networks and services in the surrounding environment to determine local connectivity and communication service availability. The design of a network routing architecture for MOPEDs must enable the exploitation of knowledge about the devices of the MOPED, the MOPED network topology, and available communication and routing.

3.1 Cooperating Devices and the Internet

Traditional networking and system models have several shortcomings when viewed in this cooperative context. Nodes on the Internet are identified by IP addresses, which statically specify where a packet should be sent to reach the identified node. When users carry devices with them, the location-specific nature of IP addresses becomes a significant burden. Even worse is the plight of the user who wants to have a single IP address represent the several interfaces on their mobile devices.

We present a coherent network model for MOPEDs, enabling them to participate fully in the Internet. We adhere to the common philosophy that any modifications to support mobility should be localized to the mobile hosts themselves, and possibly some support systems associated with the particular MOPED. We do not require the replacement of Internet routers or any alterations to non-MOPED hosts. In fact, our solution preserves end-to-end semantics and is transparent to endhosts. Network applications running on a MOPED device require no modification, and Internet hosts communicating with a MOPED are oblivious to its structure and mobility.

The particular contribution of this work is a framework for integrating a MOPED into the Internet; we define an architecture through which data packets can be routed between the various devices in a MOPED and correspondent hosts at large on the Internet, which may not be MOPED-aware or even mobility-aware. This MOPED Routing Architecture handles the basic connectivity problem for a MOPED: directing traffic to and from the set of mobile devices.

3.2 MOPED Requirements

The goal of our research is to support a large range of devices in the architecture of a MOPED—from personal computers to mobile telephones to smart cards. In order to support such diversity, MOPED capability must place minimal requirements on the processing power, storage space, and bandwidth available to any given device. We expect that most personal technology devices will eventually include efficient short-range wireless communication interfaces (e.g., low-power 802.11, BlueTooth) for communication between the devices. In addition, we expect that many devices will have additional wireless connectivity to the Internet, such as wireless Ethernet or a cellular modem. In order to provide portability, devices in a MOPED can use any channel of communication which can carry IP traffic[1]. We expect to support lighter-weight communication than IP in the future.

Low-power, low-cost communication usually incurs a penalty in terms of low bandwidth and low noise tolerance (i.e., frequent packet loss). These channel characteristics imply that a MOPED may be able to improve overall communication quality by using diverse network interfaces, or by aggregating bandwidth from multiple interfaces. In fact, one of the goals of the MOPED project (although not of this paper) is to devise a family of transport protocols that can aggregate multiple network interfaces to provide service to a single traffic flow. Much of this work has been completed in a non-MOPED context [7], but has yet to be integrated into the MOPED

[1] This author has a special predisposition toward "Avian Carriers" [20].

architecture. Current results of these protocols for single hosts with multiple network interfaces promise that bandwidth aggregation is an achievable goal for MOPEDs.

The design of Internet support for MOPEDs is modeled after MobileIP [14]. A MOPED has a single official IP address by which it may be reached, and must have a supporting Home Agent to direct traffic to the MOPED from its home network. We examine the role of MobileIP in a MOPED in greater depth in Section 4.2.

3.3 MOPED Routing Challenges

We recognize two distinct types of traffic in a MOPED that require different routing behaviors:

- Intra-MOPED: traffic between two devices in the same MOPED connected component, and
- Extra-MOPED: traffic between a MOPED device and a host outside of the MOPED.

We will also occasionally refer to Intra-MOPED routing—traffic between different components of the same MOPED—although this is a special case of Extra-MOPED routing, and not truly distinct.

The dynamic nature of the MOPED's composition and topology is also a challenge to traditional routing, but not a strict focus at this stage in the development of the MOPED Routing Architecture. We assume the existence of an internal routing mechanism that is capable of routing Intra-MOPED packets from one MOPED device to another within the same MOPED component. The choice of this protocol is not critical to the architecture, and is reserved as a subject for future work. For a naïve implementation, a standard routing protocol such as the Routing Information Protocol [8] should suffice, since the expected size of MOPED components is very small. The Moped Routing Architecture's Inter-MOPED traffic handling hierarchically stitches all the components together into a single virtual network; at the Inter-MOPED level, the entire MOPED is a single routing domain.

There are three aspects of routing in a MOPED that prohibit the use of traditional IP routing: addressability, the necessity of addressing each internal device individually although the MOPED itself has only one public IP address; mobility, managing the mobility of the MOPED devices relative to the Home Agent and each other; and path selection, the ability to selectively utilize multiple paths from a MOPED device to the home agent to enhance throughput and reliability.

3.3.1 Mobility

There are two types of mobility we consider in a MOPED: mobility of devices with respect to the Home Agent, i.e., mobility through the Internet proper, and mobility of MOPED devices with respect to each other. For mobility respective to the Home Agent, we take advantage of the existing machinery of MobileIP.

We assign to each interface of a MOPED device a static Home Address for use with MobileIP. Devices with external connectivity then use MobileIP to establish a channel to the Home Agent, effectively forming a link between the device's MOPED component and the Home Agent in the overlay network.

Interestingly, the use of MobileIP is not exposed to upper layers in the architecture; it simply provides a "tunnel" into which a MOPED perimeter node or Home Agent can send packets, expecting them to arrive at the other (mobile) endpoint. In the future, this insulation from MobileIP, as it were, allows it to be easily replaced with another mobility management protocol, such as MobileIPv6 without affecting higher layers in the architecture.

Although it may seem extravagant to have a distinct globally-valid IP address for each external interface, we believe it is necessary to allow maximum flexibility of MOPED connectivity with the existing MobileIP infrastructure. One might imagine it possible for every external MOPED interface to use the public MOPED IP address as its MobileIP Home Address. This approach would require extensive modification to the MobileIP Home Agent to somehow differentiate these multiple registrations, but would still interoperate with existing MobileIP foreign agents. The catch, however, is that these unmodified foreign agents will only be able to support a single registration for an entire MOPED. Since we can envision a MOPED with multiple interfaces using the same link-layer technology possibly registering with the same foreign agent, we prefer to retain the flexibility of assigning unique home addresses to each external interface. We also note that this approach is no less expensive than a non-MOPED approach which would also assign each device a unique home address.

The second variety of MOPED mobility, mobility of devices relative to each other, is a less pat question. A single MOPED component is, in some sense, an ad-hoc network; we plan to use an ad-hoc link-state routing protocol to maintain (at each MOPED node) a topology graph of its component, including which external interfaces are active. The home agent need only know which MOPED devices are in which component, without having full internal knowledge of the components' topology. This reachability information is relayed from the components to the home agent as part of the normal routing information dissemination. In the MOPED overlay network, the home agent effectively switches traffic between the components – when a node must send a packet to a correspondent host, or another node *not in its component*, it simply sends the packet to the home agent. This part of the architecture has not yet been completely investigated, but is essentially a specialized form of micro-mobility protocol.

We believe that the ability to maintain mobility for communications with non-MOPED-aware Internet hosts is crucial to the success of our technology, so we cannot enforce any requirements on the correspondent hosts to communicate with the MOPED. Consequently, our approach to MOPED mobility more closely mirrors the proxy method of MobileIP [14] than the end-to-end approaches of other work [18, et al]. Our future plans will integrate an end-to-end mobility method as an optimization for correspondent hosts that support it, but still retain the proxy for completeness. The proxy provides a fixed location via which a mobile host can be contacted. The addition of location capability to a pure end-to-end mechanism for mobility allows communication to continue even when both end-hosts move simultaneously, and does so without deferring the problem to the Domain Name System.

3.3.2 Addressability

We would like to use IP for communication between devices in the MOPED, so that users can manage the MOPED with familiar applications. This makes it necessary for the MOPED to maintain a mapping between the single public IP address and the (possibly many) MOPED-internal IP addresses. The Home Agent must be able to use this mapping to deliver incoming packets to the proper end-device within the MOPED.

To realize the goal of MOPED-device addressability, the MOPED Routing Architecture assigns to each device a static, private IP address in the MOPED overlay network. These addresses are "private" in the sense that they need not have significance (or even be unique) outside of the MOPED proper, since hosts external to the MOPED will never use, or in fact be aware of, these addresses.

3.3.3 Path Selection

The final task necessary for the MOPED Routing Architecture is a limited form of path selection. We believe that the bottleneck for communication resources in MOPEDs will be the hop from the perimeter nodes to the infrastructure, and not in the MOPED component-internal links. This is to say that long-haul wireless technologies will have lower bandwidths than the short-range wireless technologies used to link MOPED components together. It is also generally the case that lower bandwidth technologies usually have larger coverage areas than high bandwidth technologies, so much of the time MOPED communication will be constrained by the bisection bandwidth through the perimeter of the components.

Since cooperative resource utilization—in terms of bandwidth, power, or cost—is one of the goals of the MOPED design, we would like for traffic flows in the MOPED to load balance in a reasonable way across the (possibly several) interfaces on the perimeter of a MOPED component. Additionally, future transport protocols designed to use multiple interfaces may be able to provide better use of many interfaces by aggregating bandwidth for a single data stream. These requirements together imply that a mechanism must be in place enabling a MOPED node to intelligently schedule packets through particular perimeter interfaces on their route to the home agent. Source routing seems the obvious solution to this problem; a MOPED node can specify the IP address of the chosen external interface in a Loose Source Route (LSR) IP option [16]. This will ensure that the packet is routed through the correct perimeter node, but does not enforce routing through the desired external interface if that perimeter node has several active external interfaces. In that case, the LSR option would need to specify the next-hop router through that interface to guarantee proper routing. Clearly, a mechanism that does not require every MOPED node to track the routing tables of all perimeter nodes is needed.

The reader should note that the MOPED's utilization of multiple communication channels is at a higher level than traditional cellular handoffs, and that the MOPED uses multiple channels simultaneously to carry different traffic, unlike the simple failover mechanism of "vertical handoffs" as in [19] or the MobileIP error-robustness technique of "simultaneous mobility bindings" [14].

Certainly none of these problems is insurmountable, and we shall address each of them individually in Section 5, where we describe the MOPED Routing Architecture at length.

3.4 Multiple Technologies, Multiple Interfaces

Coverage areas for different wireless communication technologies (and wired, for that matter) vary greatly, with some areas of overlap between multiple technologies. In order to maximize user connectivity, MOPED devices which are in their coverage areas must forward traffic for their peer devices which otherwise lack the ability to communicate. Further, a user with high bandwidth requirements would like to utilize all of the bandwidth available to multiple MOPED devices, when several devices are all within their coverage areas. The MOPED therefore requires a routing mechanism capable of directing traffic flow through several simultaneously connected interfaces, and maintaining routes for this traffic in the face of user mobility or network failures.

We believe that our MOPED should support bandwidth aggregation with flow-level granularity, i.e., all packets in a particular flow (identified by IP protocol, and source & destination IP addresses and transport-layer port numbers) should follow the same path. A finer level of granularity, directing packets from the same flow to follow different paths, could easily cause packet reordering which transport layers such as TCP may interpret as loss [17]. Inverse multiplexing a flow across multiple paths also makes it challenging for adaptive transport layer protocols to effectively collect channel quality statistics, such as TCP's estimates of round trip times, or path MTU discovery [10]. Ongoing work in our group is developing a family of transport protocols specifically designed for inverse multiplexing [7] which may enhance the MOPED's ability to efficiently utilize multiple simultaneous communication channels.

4. RELATED WORK

The design of the MOPED Routing Architecture draws from several areas of research in mobile computing. In this section we discuss our design in the context of such research in network technology, routing and user location management.

4.1 Infrastructure

A MOPED provides an infrastructure for several personal technology devices to connect to each other and communicate with the Internet. Integrating a set of personal devices is certainly not an idea original to MOPEDS. Technologies for personal area networks (PANs) such as BlueTooth and low-power IEEE 802.11 have come into vogue in the networking research community, but they are simply mechanisms for physical connectivity amongst a set of devices—they do not address the question of *what* we should do with our PANs or *how* these tasks can be best accomplished. We see MOPEDs as a network-layer (or slightly above) entity that is complementary to the datalink-layer concept of a PAN. Although a PAN is useful, it is not necessary to our design; indeed, we allow separate components of connected devices to participate in the same MOPED using external channels.

4.2 Routing

Many projects address issues involved with mobility of and routing to groups of devices. A MOPED is a composite of many devices with many network interfaces; a mobile network with multiple points of attachment to the Internet. A single MOPED device might itself have multiple external interfaces, so our architecture is a mobility solution for one or more devices with zero or more Internet-mobile network interfaces each.

MobileIP handily solves the problem of mobility for a single device, but does not directly solve the problem of MOPED mobility without some extension. The goal of MobileIP is to make it appear that a mobile host is not mobile, but is, in fact, at "home." The mobile node (MN) has a permanent home address at which other Internet hosts try to reach it. Some host on the MN's home network acts as a supporting home agent. When the MN wanders into a foreign network, it obtains an IP address on that network, a care-of-address. The MN registers this care-of-address with its home agent, which intercepts traffic sent to the MN's home address and redirects it to the care-of-address.

Unfortunately, the multiple-interface, single IP address nature of MOPED mobility does not align well with MobileIP. MOPEDs must have a way to multiplex traffic destined for many devices onto a single IP address. The impedance-mismatch of MobileIP to MOPEDs is exacerbated by the fact that MOPEDs may contain devices that have no direct Internet connection, and thus cannot participate in MobileIP. Clearly, a different solution is necessary to support mobility of MOPEDs. There has been some work in the MobileIP community to address the mobility of a network of hosts with a *single* point of attachment, so called "Mobile Routers" [2, 14]. The work on mobile routers does not address the MOPED goals of user addressability or resource aggregation.

The MOPED Routing Architecture provides a mechanism to access exactly one of a set of several Internet hosts using a single IP address. In this way the MRA resembles anycasting [12]. The MRA, however, provides a much more structured environment for distributing traffic to specific devices in that set, additionally providing for mobility and resource aggregation. Explicit control over access paths into the MOPED makes it possible for the MRA to provide better resource utilization than that possible via blind anycast.

Our use of multiple interfaces and multiple paths for data transmission is greatly influenced by [22]. The prototype implementation of the Multipath Layer (described in Section 5.2) uses their mechanism for binding sockets to particular interfaces. We generalize their work to a multiple-device, network environment.

4.3 User Location

One of the main goals of MOPEDs is to bind communication mechanisms together and create a single point of access to a user. Our work approaches the user location problem by defining a single Internet address (the MOPED address) to which all data for a user should be directed, replacing the user location problem with a more traditional network location problem. This conversion of person-location to network-location lets our solution interoperate with unmodified, legacy network applications.

The user-location-management aspect of MOPEDs is similar to the goal of Stanford's Mobile People Project [9]. Mobile People is an architecture for allowing application-level mobility: it provides a name service to map from user names to application-specific addresses at which that user can be reached, a process Mobile People calls "person-level routing". Mobile People does not address the grouping of several devices into a single logical entity, and certainly does not support aggregation of device resources in a cooperative fashion. It provides an intermediary between communicating parties where they may record their current "address" and learn others' "addresses." Both Mobile People and the MRA provide location privacy; they make it possible to communicate with a given person through a proxy, hiding that person's actual location.

Our work is somewhat complementary to ICEBERG [21]: a comprehensive framework for communication and service adaptation, transforming communication datatypes to suit different devices. A MOPED would be an interesting basis for a communication network atop which to implement ICEBERG. ICEBERG does not address the issues of cooperative resource aggregation and network-layer connectivity upon which the MOPED Routing Architecture is focused. Although the MRA is an enabling technology for the goals to which ICEBERG aspires—namely, the idea of using a person as a communication endpoint—the two are in fact complementary, as they provide services at differing layers of the network hierarchy.

Hewlett Packard Lab's CoolTown project integrates people, places, and things into the web by augmenting each with a "web presence" [3]. CoolTown is an application layer solution for user-location, and therefore requires application modification.

5. MOPED ROUTING ARCHITECTURE

The goal of the MOPED Routing Architecture is to provide a mapping from the single point of contact of the user, the MOPED IP address, to the destination node in the MOPED. First, the MRA must provide addressing capabilities for each of the individual nodes, as well as each of the individual nodes' interfaces. Addressability is provided through the use of Network Address Translation (NAT), which is an approach commonly used in conjunction with connection tracking to compress address space. Second, the MRA must be able to determine and set up an appropriate route to the destination node. Route Selection is supported in the Multipath Layer, which tracks connectivity and topology in order to make appropriate routing decisions. The Multipath Layer's sole responsibility is to maintain a partial graph of the MOPED, and use its tracking information along with possible application input to choose external interfaces by which packets will enter or leave the MOPED. Finally, the MRA must be able to deal with the mobility of the destination. Although it seems contradictory to our earlier claim, mobility of individual nodes is supported through the use of MobileIP. In this section, we present our solutions for each of these functionalities and discuss our solution in the context of a concrete example.

5.1 Addressability

The use of Network Address Translation (NAT) in a MOPED solves the problem of addressing specific nodes and interfaces in a MOPED. NAT has traditionally been used as a solution to the problem of address space pressure in IPv4. It is common for a "secure" IP network to be assigned non-routable, private addresses and hidden behind a firewall. Such networks use NAT in conjunction with connection tracking to achieve what is commonly called "IP Masquerading:" enabling the hidden hosts to communicate with the Internet, while avoiding the problem of address space pressure by multiplexing the entire network of hosts on to the single public IP address of the firewall. We incorporate this approach in the MOPED Routing Architecture, using NAT and connection tracking to multiplex the MOPED on to a single public IP address. Address space pressure is not significant to the design of the MRA, but the ability to access an entire network of devices through a single address is a critical goal. NAT allows us to localize the mapping from the public MOPED address to internal MOPED addresses in the home agent, helping to reduce the complexity and state in the actual MOPED nodes.

To implement NAT in a MOPED, we assign a unique node identifier (i.e., a private "internal" IP address) to each MOPED device. MOPED nodes use these addresses to communicate with each other internally; they are not visible outside the confines of the MOPED and its home agent. The NAT layer's sole responsibility is to maintain a mapping from correspondent host IP and port number to internal IP.

For outgoing MOPED traffic, NAT recognizes packets that originate a flow and records a binding for that flow. The source address in the packet is then mangled so that the packet appears to come from the public MOPED address when it arrives at the destination. Any reply packets, or further packets sent from the MOPED in this flow, match the established binding so that NAT can determine to where they should be sent.

So that the MRA can handle incoming service connections to the MOPED from correspondent hosts, future work will develop protocols to control selective port forwarding at the NAT layer, allowing application programs to receive traffic destined for specific TCP/UDP ports on the public MOPED IP address. In our prototype implementation, any services exported from the MOPED require static port forwarding.

5.2 Route Selection

The Multipath layer determines how data traffic is routed from the home agent to the internal devices addressed by this private space (and vice versa). The Multipath layer maintains partial topology information for the MOPED, so that it can determine which MOPED devices compose each component, and what external interfaces provide access to each component. This topology is used to determine paths for packets sent into the MOPED.

The choice of multipath routing algorithm is crucial to the proper operation of the Multipath layer. This is an open problem, and one we will address in future work. The MOPED Routing Architecture enables the study of multipath policy algorithms by providing an infrastructure that allows paths to be specified, and facilitates communication between peer multipath policy agents on different devices. Our current implementation of the Multipath layer binds all packets of a particular flow—identified by a tuple (local IP, local port, correspondent IP, correspondent port, IP protocol)—to follow the same path. This binding is, of course, dynamic: when the Multipath layer discovers an alternative path with more suitable characteristics, the binding is easily altered.

The Multipath Layer is the key active entity in Extra-MOPED traffic. It piggy-backs path information on the data packets, to be used by Multipath layers on other devices in determining how to handle other packets from the same flow. This need to attach arbitrary data to packets encouraged the development of the light weight, extendible IP encapsulation protocol, Multipath Routing enCAPsulation (MRCAP), described in Section 5.6.

5.3 Mobility

Although not sufficient for supporting mobility of MOPEDs, we adapted MobileIP into the MOPED Architecture to support mobility of individual nodes. Mobility of IP network interfaces in the Internet is a well-studied problem. Instead of casting aside this body of work, we intend to leverage MobileIP as much as possible in handling MOPED mobility. Recall that mobility of a MOPED is unlike traditional MobileIP clients, in that a MOPED has many mobile interfaces to manage, and may be able to deal with mobility by routing traffic through another MOPED device.

In MobileIP, data from the Internet for the mobile node is delivered to its home agent, and then “tunneled” to the mobile node’s care-of-address. MobileIP can also use reverse tunneling, in which all outbound traffic *from* the mobile node is tunneled to its home agent, and them sent on to the true destination. This is necessary to avoid firewalls that use reverse packet filtering—discarding packets that come from the “wrong” side of the firewall. The MOPED Routing Architecture always uses reverse tunneling, for that reason, as well as to ensure that the multipath layer in the home agent will have complete, timely information on MOPED topology.

5.4 Address Hierarchy

We briefly summarize the addressing hierarchy used by the MOPED Routing Architecture; there are four distinct kinds of addresses used:

1. The MOPED IP address. This is the official, public IP address used to identify the MOPED, and therefore its owner.
2. Internal IP addresses. These addresses are used to identify particular MOPED devices; they are private in the sense that they have meaning only within the MOPED and its home agent.
3. Interface IP addresses. These are the MobileIP home addresses of the external interfaces on the MOPED devices. They are distinct from the Internal addresses, as there may be some devices that have only internal addresses.
4. Care-of-Addresses. These are the IP addresses to which the MOPED external interfaces are currently bound by MobileIP.

Different layers of the architecture use each of these sets of addresses to perform different functions, as will be described in Section 5.5. These addresses are depicted in Figure 1.

5.5 Architecture

Now we assemble the pieces of the Moped Routing Architecture, and give an operational description of its function. Intuitively, when a packet arrives from a correspondent host addressed to the MOPED, the Home Agent must determine:

1. To which MOPED device the packet should be delivered—an internal IP address. (NAT)
2. Through which external interface the packet must be routed to reach the target device’s component of the MOPED. (Multipath)
3. Exactly where in the Internet that external interface is. (MobileIP)

Upon arrival at that external interface, the receiving MOPED perimeter device then:

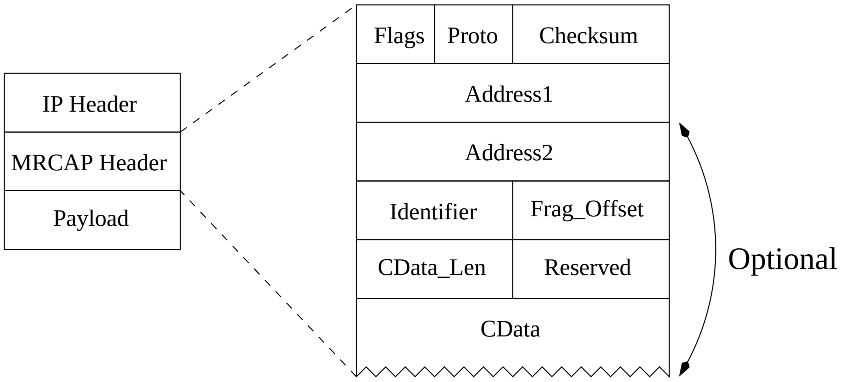
1. Marks the packet as having passed through the external interface. (Multipath)
2. Uses the internal routing protocol to deliver the packet to the correct destination MOPED device.

When the packet is finally delivered, the destination MOPED device may record the path taken by the packet (Multipath), to help decide how to send any packets back to the correspondent host.

Conversely, when a MOPED device needs to transmit a packet to some other host, it must:

1. Determine if the target is a device in this MOPED; if so, try to use the internal routing protocol to find a path to it.

Figure 2: MRCAP Packet Format



2. If such a path exists, the target is in this device's MOPED component and the route is used to deliver the packet.
3. Otherwise, the target is in another MOPED component, or is simply outside of the MOPED—the packet is redirected to the Home Agent for handling by:
   (a) Choosing an external interface from the device's component through which the packet will be sent to the HA, and marking the packet appropriately. (Multipath)
   (b) Delivering the packet via the internal routing protocol to the device where that external interface is located.

Once the internal routing protocol delivers the packet to the desired perimeter MOPED device, it will simply transmit the packet through the chosen external interface to the Home Agent (Multipath). At the Home Agent, the process used for delivery to the MOPED is reversed:

1. The Home Agent may record the external interface through which the packet was directed out of the MOPED component, for use in later routing decisions. (Multipath)
2. The Home Agent mangles the source address in the packet, so that it appears to come from the official, public MOPED address. (NAT)
3. Traditional IP routing delivers the packet to the target host.

A purpose-devised lightweight IP encapsulation protocol, Multipath Routing enCAPsulation (MRCAP), facilitates communication between peer Multipath layers, and packet redirection.

5.6 Multipath Routing enCAPsulation

The design of the MRA, in conjunction with our goal of implementing the entire architecture in user space, makes it apparent that some sort of IP encapsulation is necessary. Since the Multipath layer is responsible for routing pre-formed IP packets and may require the communication of some small amount of state to a peer Multipath layer, we need a lightweight mechanism to:

- Encapsulate any IP packet.
- Twiddle the source and/or destination address.
- Track the original source/destination addresses.
- Facilitate communication between peer multipath policy algorithms.

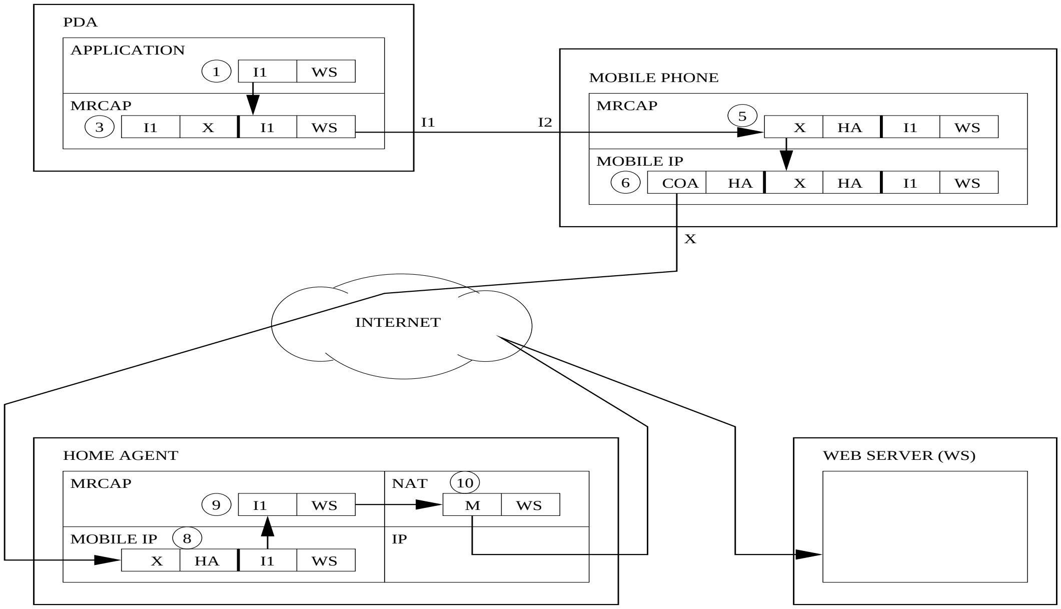
As last-hop bandwidth is a primary concern, we are concerned with per-packet overhead in excess of the costs of MobileIP, a problem which is especially acute when MobileIP reverse-tunneling is employed. We evaluated existing encapsulation protocols, but were concerned with either their consumption of data space (IPIP [13], or GRE [5]), or lack of flexibility and general applicability. Minimal Encapsulation [15] is an optimization to IP in IP encapsulation: instead of adding an entire envelope IP header to the encapsulated packet, it stores a single extra IP address (the original destination address of the tunneled packet) and 4 bytes of accounting overhead. The very low overhead (8 bytes per packet) of Minimal Encapsulation is attractive, but sacrifices extensibility, and incurs an inability to encapsulate fragmented IP packets. Unwilling to sacrifice bandwidth, we determined to develop a general, extendible encapsulation protocol tailored to the needs of MOPED Routing.

The protocol we propose is Multipath Routing enCAPsulation, or MRCAP. MRCAP has very low per-packet overhead, usually 8-12 bytes, comparable to Minimal Encapsulation. The MRCAP packet format (see Figure 2) includes a tiny fixed-length header inserted between the original IP header and the packet payload, as in Minimal Encapsulation. The presence of various extension headers is indicated by option flag bits. The fixed-length header occupies 8 bytes of payload space, while still retaining the flexibility to add optional extensions as necessary. (One of those extensions is a 4-byte Fragment header, so that MRCAP can encapsulate fragments.) All communication between Multipath layers on the Home Agent or in the MOPED occurs in-band, in the control channel of MRCAP.

5.7 Implementation

The MOPED Routing Architecture has been partially implemented atop the Linux 2.4 kernel, running on our MOPED test bed of several laptops communicating over IEEE 802.11b wireless Ethernet. We use the netfilter NAT functionality built-in to Linux as the MRA's NAT layer, and Dynamics MobileIP to provide mobility. The modularity of the architecture allows us to easily combine these unmodified components with our Multipath Layer implementation, the Multipath Routing Daemon (MRD). The MRD is a user-space application that uses the Linux kernel's Universal

Figure 3: A packet's path through the MOPED Routing Architecture



Tun/Tap driver to intercept packets and inject packets directly into the kernel network stack. As currently written, the MRD handles the more technically challenging extra-MOPED traffic only, with intra-MOPED traffic handled by static route configuration.

The MRD operates by carefully manipulating routing tables to direct externally destined packets into the tunnel device, so that they may be captured, MRCAP encapsulated, and have their path to the home agent selected appropriately. As with any packet tunneling implementation, great care is taken to ensure that packets are not multiply encapsulated, and that ICMP error messages are forwarded to the correct originators, as for IPIP encapsulation [13].

At perimeter nodes, the Linux `SO_BINDTODEVICE` socket option [22] is used to force MRCAP packets through raw sockets bound to the proper external interface, as directed in the MRCAP header.

5.8 A Concrete Example or A Day In the Life of a Packet

Consider a MOPED comprised of a PDA (with internal address $I1$) and mobile phone (with internal address $I2$, and external interface X, currently registered to care-of-address COA). We follow an example World Wide Web transaction between the PDA and a correspondent web server outside the MOPED, with reference Figure 3.

1. The web browser on the PDA fires off a packet to the web server (WS); we depict this packet:

2. The intra-MOPED protocol fails to find a route to WS, and hands the packet to the Multipath Layer.

3. The multipath policy algorithm evaluates the packet, and chooses to send the packet through external interface X on the mobile phone. Multipath encapsulates the packet via MRCAP:

4. The internal routing protocol delivers the packet to the mobile phone.

5. The Multipath layer here receives the MRCAP encapsulated packet. It sees that this packet is to be sent to the home agent, through interface X. It mangles the MRCAP header, effectively storing the original source and destination addresses in the MRCAP header, while directing the packet to the home agent.

6. MobileIP on the phone intercepts the packet, and encapsulates it again, annotating the fact that the packet is actually traveling from the care-of-address.

7. The packet is shipped out on interface COA (or X) toward the home agent.

8. At the home agent, the packet is delivered to MobileIP, and the outermost header is stripped.

9. The new outermost header directs the packet to the Multipath layer in the home agent. It records any info communicated to it by its peers in the PDA or the mobile phone, and decapsulates the MRCAP header:

10. NAT on the home agent recognizes $I1$ as being MOPED-internal, and maps it to the public MOPED address M,after recording the binding $(WS, I1)$, but before delivering the packet on to the web server.

The packet has been successfully routed out of the MOPED, and to the destination. We follow the return to the PDA of the response.

1. The web server initiates a response packet:

IP	
Src	Dst
WS	M

2. The home agent intercepts the packet, where it is recognized by the NAT layer as matching the earlier binding $(WS, I1)$; the destination address of the packet is mangled appropriately, and the packet sent on to the Multipath layer:

IP	
Src	Dst
WS	I1

3. Multipath must determine the path into the MOPED for this packet. Our prototype, with its simple binding mechanism, will use the interface through which the first packet passed as it came to the home agent:

IP		MRCAP	
Src	Dst	Src	Dst
WS	X	—	I1

4. MobileIP tunnels the packet to the care-of-address COA:

MobileIP		IP		MRCAP	
Src	Dst	Src	Dst	Src	Dst
HA	COA	WS	X	—	I1

5. IP delivers the packet to the mobile phone, using interface COA. It is delivered to the local MobileIP layer, and the outer header is stripped:

IP		MRCAP	
Src	Dst	Src	Dst
WS	X	—	I1

6. Multipath receives the packet, and records its path thru X before sending it on to the PDA $I1$:

IP		MRCAP	
Src	Dst	Src	Dst
WS	I1	X	—

7. At the PDA, Multipath records the X, as desired by the multipath policy algorithm, and then decapsulates the packet to deliver to the web browser:

IP	
Src	Dst
WS	I1

The MRA directs traffic in its complicated dance, but in the end, the web server and browser are none the wiser; they have participated in the MOPED Routing Architecture without their knowledge.

5.9 Legacy Devices: Freeloaders

The decision to tunnel all traffic that passes through the MOPED perimeter through a proprietary protocol, MRCAP, seems to directly conflict with our stated desire of allowing legacy devices to participate in a MOPED. We have, however, developed a simple extension to the normal MOPED Routing Protocol to allow unmodified legacy devices, or *freeloaders*, to participate in the MOPED with the assistance of another MOPED device, referred to here as the *relay*. The freeloader device is configured to use a MOPED-internal IP address, with the relay as its default router. The relay can intercept the freeloader's network traffic and encapsulate it properly for MOPED Routing. In effect, the relay is acting as the freeloader's MOPED proxy, enabling the freeloader to enjoy the MOPED's advantages without carrying its share of the costs of MOPED operation.

Since the MOPED Routing Daemon intercepts all IP packets with extra-MOPED destinations in the course of its normal operation, the MRD will also capture packets directed to it by the freeloader for handling. Simple inspection of the IP packet will reveal that was originated by a host other than the relay, but is destined outside the MOPED, and not MRCAP encapsulated – the originating host must therefore be a freeloader. The MOPED Routing Daemon must encapsulate the packet, handling it just as it would a locally generated IP packet, and set a flag in the MRCAP header (the *Freeloader* flag) indicating that the source of this packet is a freeloader, and in particular does not understand MRCAP. The MRD then directs the encapsulated packet through normal channels, choosing a path and directing it toward the Home Agent as usual. In its binding cache entry for this packet's association, the Home Agent will annotate that the MOPED device is a freeloader, as indicated in the MRCAP header.

The return path for packets transmitted from correspondent hosts to freeloaders is slightly more complicated. Upon receipt of such a packet, the Home Agent observes the annotation on its binding cache entry for the association and sets the freeloader bit in the MRCAP header of the encapsulated packet, which is then forwarded normally to the freeloader's MOPED component. Upon arrival at the MOPED perimeter device, where the packet would normally be routed to its final destination after being marked with its ingress path, the MRD on the perimeter node observes that the *Freeloader* flag is set in the MRCAP header. Since freeloaders do not, by definition, process MRCAP-encapsulated packets, the perimeter MRD unencapsulates the packet and delivers it to the freeloader using normal intra-MOPED routing procedures.

It is important that any device be capable of acting as relay for a freeloader, since the freeloader and its relay may not remain in the same MOPED component. If the freeloader loses connectivity with its chosen relay, we assume that some traditional mechanism can direct the freeloader to use another MOPED device as its default router, such as ICMP Router Discovery [4]. There is no state kept in the relay specific to freeloader devices, or associations that it is handling for them, so that relay operation places few demands on a MOPED device and there is no state to migrate when the freeloader changes relay.

ICMP error delivery is a critical facet of IP operation that needs special handling for freeloaders. Outside the domain of MOPED Routing, ICMP errors can be generated normally and will be delivered to the freeloader by the MRA like any other packet. An ICMP error generated by an intermediate MOPED Routing Daemon in response to a MRCAP packet with the *Freeloader* flag set requires special handling. Since the IP layer of the freeloader would be confused by ICMP errors generated for MRCAP packets, which a freeloader obviously could not have sent, the MOPED Routing Daemon generating such an ICMP error must unencapsulate the packet before ICMP delivery. Although this requires an extra check to be made before forwarding ICMP error packets, it adds little code to the MOPED Routing Daemon, which must already be capable of decapsulating and delivering ICMP errors to local applications.

5.10 Circumventing MOPED Mobility

A more challenging optimization for MOPED Routing is to circumvent the mobility architecture altogether. Zhao, Casteluccia and Baker describe a system that performs flexible routing for a mobile host using MobileIP, allowing that host to selectively send some packets using regular IP [22]. For services/connections that do not require mobility, e.g., name resolution via a local name server, avoiding MobileIP is a useful optimization. In a MOPED, we would also like the ability for certain traffic to circumvent the mobility and communicate as directly as possible with a correspondent host. “As directly as possible” may not truly mean directly, as it does in the case of MobileIP, since the communicating MOPED device may need another MOPED device to route its traffic to the desired correspondent host. Nevertheless, this optimization avoids the triangle routing incurred by directing all traffic through the Home Agent, and can reduce network latency, as well as reducing overall demand on the network if the correspondent host is near to the MOPED.

Essentially, the MOPED device that wants to circumvents normal MOPED operation needs the perimeter node between it and the correspondent host to carryout the Home Agent’s usual function in the MOPED communication path. That is, the perimeter node needs to use NAT and present the traffic from the internal node as its own. To circumvent mobility as well, the perimeter node must also use an additional mechanism like that of Zhao, Casteluccia, and Baker to allow this traffic to by-pass MobileIP.

Extending our MOPED Routing Architecture to perform this optimization is also simple, although determining what scenarios are correct or well-suited to its application is a topic of future research. In our implementation, the MOPED Routing Daemon circumvents normal MOPED operation for traffic destined to a static list of transport port numbers. When the MOPED Routing Daemon must route a packet whose destination is one of those transport port numbers, it MRCAP encapsulates the packet as usual, and additionally sets the *Masquerade* flag in the MRCAP header. The MRD chooses a perimeter node through which to direct the packets of this association (if one is not already recorded in the binding cache) and sends the packet to that perimeter node normally. Upon receipt, the perimeter MRD notes the *Masquerade* flag in the packet’s MRCAP header, and, if this is the first packet in this association, sets up a NAT rule to translate the internal address of packets on this association to the address of the external interface through which the destination host can be reached. This packet, and other sent from the internal node on this association, is decapsulated and handed to the kernel for delivery so that the the NAT rule can take over.

Similar to the freeloader mechanism of Section 5.9, the return path of the association operates differently from the outgoing path. When packets from the correspondent host arrive at the perimeter node—which is the destination, as far as the correspondent host knows—the NAT layer will translate the packet’s destination address to that of the internal node, reversing the NAT rule. Normal intra-MOPED routing can then forward the packet to the proper internal node.

6. CONCLUSIONS AND FUTURE WORK

The MOPED Routing Architecture is a coherent network model for MObile grouPEd Devices. It addresses the three major challenges of MOPED routing—addressability, mobility, and route selection—allowing MOPEDs full Internet integration. The MRA enables a set of mobile communicating devices to cooperatively maintain Internet connectivity through multiple simultaneous points of access. All of this functionality is realized in a manner that is transparent to the remainder of the Internet, requiring no modification of infrastructure or changes to legacy network applications. An important factor contributing to the effectiveness of the MRA is the light-weight, extendible encapsulation protocol MRCAP.

The most important goal of our future work is the complete implementation of the MRA—we believe that no architectural design is truly complete until any errors and inconsistencies in the design have been exposed by implementation. Completing the implementation would entail the following:

- Examine alternatives for the MOPED-internal routing method (e.g., various static or ad-hoc routing protocols).
- Design a protocol for remote NAT configuration, enabling a MOPED device to declare itself the correct endpoint for a type of data.
- Implement and study alternative policy algorithms for multipath route selection.
- Design a protocol for MOPED self-discovery, so that devices participating in the same MOPED may discover their peers.

After completing the basic structure of the MOPED Routing Architecture, we will scrutinize other aspects of MOPED networking that will enhance the overall MOPED design. We intend to replace the transport layer IP protocols with our family of multipath, bandwidth-aggregating protocols. We must develop the control structure and user interface to manage interface connectivity over the MOPED—an agent to set up and tear down external interfaces as appropriate for optimal resource utilization. We believe that collapsing the layered structure of the MRA, although complicating the implementation, may enable space optimization in the network packets by combining the MRCAP and MobileIP headers.

Security is one important issue of any set of personal technology devices that we do *not* explicitly address here. We believe that existing solutions for network level security in the context of MobileIP apply perfectly well to our extended, MOPED-mobility environment.

We have shown how to extend the paradigm for communication from a mobile device to a mobile person, via the representative Internet presence embodied in a MOPED. The MOPED Routing Architecture enables efficient utilization of MOPED resources through cooperative communication. We make this all possible without necessitating any changes to Internet infrastructure or network software.

7. REFERENCES

[1] M. Baker, Z. Zhao, S. Cheshire, and J. Stone. Supporting Mobility in Mosquitonet. In *USENIX Winter Conference*, 1996.

[2] L. Bellier and C. Casteluccia. Mobile Networks Support in Mobile IPv6. Internet Draft draft-ernst-mobileip-v6-network-01.txt, IETF, November 2000.

[3] P. Debaty and D. Caswell. Uniform Web Presence Architecture for People, Places, and Things. Technical Report HPL-2000-67, HP Labs, June 2000.

[4] S. Deering. ICMP Router Discovery Messages. Request For Comments (Proposed Standard) RFC 1256, IETF, September 1991.

[5] D. Farinacci, T. Li, S. Hanks, S. Meyer, and P. Traina. Minimal Encapsulation within IP. Request for Comments (Proposed Standard) RFC 2784, IETF, March 2000.

[6] L. Magalhães and R. Kravets. End-to-end Inverse Multiplexing for Mobile Hosts. In *19th Brazilian Symposium on Computer Networks (SBRC'01)*, 2001.

[7] L. Magalhães and R. Kravets. MMTP: Multimedia Multiplexing Transport Protocol. In *The First Workshop on Data Communications in Latin America and the Caribbean (SIGCOMM-LA 2001)*, 2001.

[8] G. Malkin. RIP Version 2. Request For Comments (Standard) RFC 2453, IETF, November 1998.

[9] P. Maniatis, M. Roussopoulos, E. Swierk, K. Lai, G. Appenzeller, X. Zhao, and M. Baker. The Mobile People Architecture. *ACM Mobile Computing and Communications Review*, 3(3), July 1999.

[10] J. Mogul and S. Deering. Path MTU Discovery. Request For Comments (Draft Standard) RFC 1191, IETF, November 1990.

[11] A. Myles, D. Johnson, and C. Perkins. A mobile host protocol supporting route optimization and authentication. *IEEE Journal on Selected Areas in Communications*, 13(5):839–849, 1995.

[12] C. Partidge, T. Mendez, and W. Milliken. Host Anycasting Service. Request For Comments (Informational) RFC 1546, IETF, November 1993.

[13] C. Perkins. IP Encapsulation within IP. Request for Comments (Proposed Standard) RFC 2003, IETF, October 1996.

[14] C. Perkins. IP Mobility Support. Request for Comments (Proposed Standard) RFC 2002, IETF, October 1996.

[15] C. Perkins. Minimal Encapsulation within IP. Request for Comments (Proposed Standard) RFC 2004, IETF, October 1996.

[16] J. Postel. Internet Protocol. Request For Comments (Standard) RFC 791, IETF, September 1981.

[17] J. Postel. Transmission control protocol. Request for Comments (Standard) RFC 793, Internet Engineering Task Force, September 1981 1981.

[18] A. Snoeren and H. Balakrishnan. An End-to-End Approach to Host Mobility. In *ACM Mobicom '99*, 2000.

[19] M. Stemm and R. H. Katz. Vertical Handoffs in Wireless Overlay Networks. *ACM Mobile Networking (MONET), Special Issue on Mobile Networking in the Internet*, 1998.

[20] D. Waitzman. A Standard for the Transmission of IP Datagrams on Avian Carriers. Request for Comments (Proposed Standard) RFC 1149, IETF, April 1990.

[21] H. J. Wang, B. Raman, C.-n. Chuah, R. Biswas, R. Gummadi, B. Hohlt, X. Hong, E. Kiciman, Z. Mao, J. S. Shih, L. Sunramanian, B. Y. Zhao, A. D. Joseph, and R. H. Katz. ICEBERG: An Internet-core Network Architecture for Integrated Communications. *IEEE Personal Communications*, August 2000.

[22] X. Zhao, C. Castelluccia, and M. Baker. Flexible Network Support for Mobility. In *Fourth ACM International Conference on Mobile Computing and Networking (MOBICOM'98)*, 1998.