Survey on Network Interface Selection in Multihomed Mobile Networks

Pratibha Mitharwal, Christophe Lohr, Annie Gravey

Survey on Network Interface Selection in Multihomed Mobile Networks

Pratibha Mitharwal, Christophe Lohr and Annie Gravey

firstname.lastname@telecom-bretagne.eu
Télécom Bretagne, Brest, France

Abstract. This survey is focused on providing a cruising ship with Internet access facilities. On a ship, the entire network infrastructure (networks, subnets, devices, terminals, etc.) is subject to mobility. Multiple connections (e.g., satellite, LTE, 3G, WiFi, etc.) can provide Internet access, thus making the ship multihomed, but the different connections may be sporadic, and provide different services in terms of bandwidth, throughput, cost. The user may thus need to dynamically select one connection among those that are available, according to its preferences. This paper presents a survey of network interface selection in existing mobility and mutlihoming protocols to provide multihomed network mobility to a cruising ship, or to any vehicle (e.g., train, car, airplane, etc.).

1 Introduction

In early days computers were very heavy to move around and had only one interface. Therefore, it was easy to identify any computer with a single Internet address. With the evolution of technology, computers can be easily moved around (i.e., they are mobile) and are connected through several network interfaces simultaneously (i.e., they are multihomed). Mobility and multihoming are closely related to each other with respect to IP addressing. Concerning mobility, IP address changes due to changing network attachment point (location) of the host (interface), whereas in multihoming, IP addresses change while changing communication paths (the selected network interface). Changes in IP address cause connection disruption as upper layers sockets are bound to IP addresses.
Multihomed mobile hosts such as smartphones, tablets etc. commonly use a single link at a given time. The network selection for every data connection on such technologies is based on "the best availability" or "on user choice". These two choices do not provide the user with cost effective benefits of multihoming scenario, e.g., one link may be free of charge but with a poor connection while another may provide dedicated services, a managed quality of service, etc., and be costly with a specific cost scheme (by volume of data, time of the day, distance, etc.).
Similarly, in multihomed mobile networks (e.g., train, ship, airplanes etc.), there are many users and every user will have different requirements. These user requirements (influenced by user & application preferences) and network characteristics (e.g., price, bandwidth, quality etc.), can be used to select the best available interface. If the interface selection is done appropriately it can improve the

performance of network applications [2]. Interface selection mechanism combines two steps: taking the decision on interface selection, and enforcing the decision. In mobile networks, the decision enforcement is located at the edge router (i.e., mobile router) of the network. Therefore, a interface selection mechanism which can communicate with the users and the mobile router, is required.

During mobility, the availability of network interfaces and also the characteristics of access networks are constantly changing as the system moves. Whenever this happens, one may want to transfer the ongoing communication from one network interface to another interface. Multihoming uses same scenario to provide best available connection. This paper discusses about network interface selection mechanism in the existing protocols for mobility in multihomed context.

The remainder of the paper is organized as follows. In Section 2, we explain about the project and requirements. Section 3, explains functionality of multihomed mobility protocols with provided interface selection mechanism (if any) and Section 4 concludes this paper.

2 Context of Study & Requirements

This study is part of TMS (Terminal Marine Stablisé) project[1], which aims to design a ship terminal facilitating broadband access for cruising ships. The major requirements of this project are explained in following subsections. An overview of all these requirements is given in Table 1.

Table 1. Requirements of TMS project

$\mathcal{R}1$: Network Mobility	reachability, session continuity, security, handover, roaming
$\mathcal{R}2$: Network Multihoming	session continuity, handover, security
$\mathcal{R}3\mathcal{S}$: Static Interface Selection	decision enforcement, binding of packet flows
$\mathcal{R}3\mathcal{D}$: Dynamic Interface Selection	user preferences, service provider's constraints, network administrator preferences

2.1 Mobility

Mobility refers to a situation where an end-host changes its topological point of attachment to the Internet. Whenever a host moves, its network layer address changes. Thus, in order to continue to communicate, the host must be able to signal the changes in its addresses to its active peers. This signaling must be secure since non-secured signaling can lead to an unauthorized traffic diversion and denial-of-service attacks. If end user hosts are mobile it is considered as "*host mobility*", and if border routers and interconnected edge network hosts are mobile it is considered as "*network mobility*".

[1] The project is supported by the French Government (Direction Générale des Entreprises)

Requirement $\mathcal{R}$1: Network Mobility First requirement for TMS project is, network mobility management. The network mobility management [7, 20] needs to provide support for handover management to forward the packets towards new location for an ongoing communication imposing minimal disconnection time for reducing unacceptable data loss, reachability to mobile network's new location, support for existing applications and services without any change, transparency to user applications about mobility, minimal infrastructure changes, roaming agreement and authentication process while switching network interfaces between different operators to avoid security concerns, e.g., address stealing, address flooding which cause Denial-of-Service, man-in-middle etc. In TMS project, mobile networks are ship based where network changes does not happen too often, so handover speed is of minor interest.

2.2 Multihoming

Multihoming refers to a situation where an end-point has several parallel path for communication with rest of the Internet [12]. This situation can be characterized as the host being reach-able through several topological paths (with multiple network layer addresses) which are completely independent of each other. When a host is connected with several different edge networks it is known as *"host multihoming"*, and when an edge network is interconnected to the core redundantly with multiple connections via multiple borders or via multiple interfaces of a border router it is known as *"site multihoming"*.
Multihoming helps to achieve redundancy and fault tolerance, increase bandwidth, balance the load inside the access network and provide traffic engineering by stripping the flows over all existing paths, using user defined rules[22].

Requirement $\mathcal{R}$2: Multihoming Second requirement for TMS is multihoming management. The multihoming solutions [46] needs to provide support for interface selection mechanism required when a communication is established (e.g., when a TCP connection is opened for an outgoing & incoming traffic), a secure recovery mechanism for handover management and session continuity to divert ongoing communication from one interface to another in case of failure with minimal delay, a mechanism to handle growth of routing tables in case of aggregated routes, a mechanism to handle change of traffic characteristics, and a mechanism for controlling the load balance (symmetric flow of packets across all existing paths) based on address assignment.

2.3 Interface Selection

Interface selection refers to the selection of source IP address among all existing interfaces for a connection association or indirectly selection of first hop router influenced dynamically by user application preferences. In mobile networks, user's participation can play an important role in interface selection as shown in [4]. However, this experiment is done considering static scenarios. In

interface selection mechanism first step would be to specify interfaces that can be used on account of a user/application's, operator's or peer node's requirements. Then, a policy set is created prioritizing the interfaces based on policies. A policy set contains filtering rules which can be stored as table distribution mechanism [21] or database [48]. After the policy set is created, these filtering rules can be used as input at OS level filtering frame work such as APIs, which will then enforce the decision in packet routing.

Requirement $\mathcal{R}3$: Interface Selection Third requirement for TMS project is Interface selection which can be divided into static interface selection ($\mathcal{R}3\mathcal{S}$) and dynamic interface selection ($\mathcal{R}3\mathcal{D}$). Static interface selection can be managed by putting some filtering rules in OS whereas the management of dynamic interface selection is a challenge in multihomed mobile networks due to frequent changes of topological location of interface, changes in application requirement or change in availability of access, so it requires a way to manage these operations. Dynamic network interface selection decisions lie on the various information such as user preferences, application requirements, hardware capacity, available network's characteristics, service provider's constraints, network administrator preferences etc. [48]. So there is a need for decision modules which will have all the available information from link layer (network signal quality and related metrics), several attributes like source address destination address from IP layer, information about cost, bandwidth and availability of Internet access from network service provider (and constraints if any), information originated from user & applications etc.

3 Multihomed Mobile Networks

There exists several proposals on how to take decisions with respect to interface selection and most of them follow the policy filtering rules. Some approaches use Multiple Attribute Decision Making (MADM) algorithms for decision making about best available network, such as Analytical Hierarchical Process (AHP) [31], Grey Relation Analysis (GRA) [36] and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [42]. A MADM algorithm first creates a decision matrix by measuring values of each criterion and then the effect of parameters scales and units is eliminated by normalization. Next the final decision scores are calculated to take the decision. An architecture is proposed in [40] for automatic network interface selection and allow user to stay connected with best available access network. The selection decision algorithm uses classical weighting objective method for decision making, considering multiple network and application preferences in account. The interface selection module for multihomed mobile hosts based on policy management and flow distribution were proposed in [2, 23, 34, 40], but none is standardized. The following subsection details about the dynamic enforcement of interface in various network and transport layer multihomed mobility protocols.

3.1 Mobile IP with Extensions

Mobile IP is a network layer protocol, which enables mobile host to leave its home network and continue to receive packets at its home address irrespective of its current location. Each mobile host is identified by its home address. A new entity called *home agent* (HA) is introduced , which is a router at a static location in the host's home network for supporting mobility services. HA intercepts the packets destined to mobile host's home address when it is away. The idea was standardized for IPv4 (Mobile IPv4, MIPv4) in RFC 3344 [28] and IPv6 (Mobile IPv6, MIPv6) in RFC 3775 [15]. The protocol offers transparent movement of a mobile host to transport layer protocols and applications.
When the host moves to another network, it acquires a new address called a care-of address (CoA) through either stateless or stateful auto-configuration. The mobile host then informs the home agent of its current address. A binding is created between mobile host's home address and care-of address. Any host communicating with mobile host is known as a corresponding node (CN). The CN uses the mobile host's permanent home address (belongs to the network associated with HA) as the destination address. Normal IP routing mechanisms forward these packets to the home agent. HA then redirects these packets to care-of-address through the IP tunnel by encapsulating the datagram with a new IP header using the care-of address of mobile host.

Hierarchical Mobile IPv6 (HMIPv6) was defined in RFC 5380 [35], is an extension to MIPv6. It aims to improve performance of MIPv6 by reducing signaling traffic and by optimizing delays that are introduced by binding updates. There is another extension for fast handover in MIPv6 [17] to reduce handover-latency.

Proxy Mobile IPv6 (PMIPv6), specified in RFC 5213 [10], extends MIPv6 signaling and reuses many concepts such as the home agent functionality. It is a network based mobility management solution which frees mobile host from participating in any mobility related signaling. The proxy mobile agent in the serving network performs mobility related signaling on behalf of mobile host. However, this protocol does not support multihoming.

Network Mobility (NEMO) Protocol was specified in RFC 3963 [3, 6]. NEMO basic support also extends the idea of MIPv6 to support connectivity of network which moves. It contains a mobile router which is in charge of the mobility operation on behalf of all the hosts located in the moving network. In order to fulfill requirement $\mathcal{R}1$, NEMO ensures session continuity and reliability into a mobile network while moving transparently to the mobile network nodes(MNNs) with help of mobile router (MR). The mobile router works as a normal IPv6 router in its home network, i.e., routes all the traffic using traditional routing methods. When mobile router is connected to another IPv6 network it acquires a care-of-address (CoA), which represents its current location in the Internet. Then mobile router like mobile host in MIPv6, registers care-of-

address to its home agent (a router located in mobile router's home network). Whenever mobile router is away from home network, home agent maintains the binding between home address, care-of-address and the prefix advertised in the mobile network (known as mobile network prefix (MNP)). A bi-directional IPv6-in-IPv6 tunnel is used to maintain connectivity between mobile router and home agent.

Multiple care-of addresses registration (MCoA) is an extension for MIPv6 and NEMO that was standardized in RFC 5648 [45]. In MIPv6 and NEMO care-of-address is a single point of failure for the whole network, so MCoA mechanism allows multiple care-of-addresses registration with mobile host's or network's home agent. In MCoA, a new binding identification (BID) generated by mobile host/router for each care-of-address, is used as unique key to distinguish multiple bindings that are registered by the same mobile host. The home agent caches the received binding identifications in a binding table and is therefore able to distinguish the multiple care-of-addresses of the mobile host/network. MCoA enables Mobile IPv6 and NEMO to support multihoming, which fulfills requirement $\mathcal{R}2$.

Flow binding is also an extension for MIPv6 and NEMO that was standardized in RFC 6089 [43] which allows hosts to bind one or more flows to a care-of address. These extensions allow multihomed hosts to instruct home agents and other Mobile IPv6 entities to direct inbound flows to specific addresses. In flow binding extension user can define any policies at OS level (fulfills $\mathcal{R}3\mathcal{S}$), but not in real time. It is assumed that the policies are configured on the mobile host's packet filtering tool [30] and the rules specified by the user are according to interface and binding, so the rules are protocol specific [23].

3.2 Location Independent Network (LIN6)

LIN6 [41], follows the idea of identifier and locator separation [18]. It introduces an identifier for each host known as LIN6 ID which is independent of its location and interfaces. It also defines two types of network addresses: the LIN6 generalized ID and LIN6 address. The LIN6 generalized ID is formed by concatenating a constant value called the LIN6 prefix before the LIN6 ID which is used at the transport layer to identity the connection. Whereas, the LIN6 address is formed by concatenating the network prefix (changes according to the mobile host's current network) and LIN6 ID which is used to route packets over network layer. The generalized IDs are then stored into DNS, together with the address of a mapping Agent. Since the generalized IDs are globally unique and permanent, the communicating hosts use them as endpoint identifiers. Apart from this, a mapping agent is used in LIN6 for queries related to mobile host's current address. LIN6 also supports multihoming through a single GI to be associated with several real addresses (fulfills $\mathcal{R}2$). There is no explicit way for interface selection mechanism in LIN6 for multihomed mobile hosts.

3.3 Locator Identifier Separation Protocol (LISP)

LISP achieves site-multihoming through core-edge separation and provides end-to-end packet delivery [8, 14, 32]. It follows three simple principles: address role separation, encapsulation, & mapping. To achieve first principle, LISP splits the semantics of IP addresses into endpoint identifiers (EID) and routing locators (RLOC). RLOCs are assigned to border routers by ISPs and EIDs are assigned inside edge networks. In LISP, the packets are created with EIDs in source and destination addresses, then these are encapsulated in a UDP segment with LISP header and finally forwarded through tunnels between edge networks. Border routers of the packet source are known as ingress tunnel routers (ITR), which perform encapsulation and the border routers of the destination site are known as egress tunnel routers (ETR), which perform the decapsulation. A mapping system (like DNS) is created for the mappings between EIDs & RLOCs. LISP's tunnel routers can query the mappings for specific EIDs and the system returns all the related mappings. LISP provides improved traffic engineering capabilities and multihoming (fulfills $\mathcal{R}2$). LISP mobile host [47] receives an EID from its home network and an address inside foreign network which can be used as RLOCs. Whenever mobile host moves and its RLOC changes, it registers the new mapping into the map server of its home network. LISP extension for network mobility (fulfills $\mathcal{R}1$) has been proposed in [5]. This locator identifier split can improve Internet scalability but it has deployment constraints. LISP does not provide any interface selection mechanism considering user preferences.

3.4 Host Identity Protocol

Host identity protocol (HIP) [24–26] has been developed to solve security, mobility and host multihoming issues in an integrated concept. It separates host identification & location, and introduces a new namespace, namely the host identity (HI). The purpose of HI is to support trust between systems, enhance mobility, and greatly reduce the DoS attacks to provide better security than other multihomed mobility solutions. HIP introduces a new host identity layer (layer 3.5) between the IP layer (layer 3) and the upper layers to avoid a dual role of IP address as endpoint and forwarding identifier. In HIP, upper layer sockets are bound to HI instead of IP addresses. In addition, the binding of these host identities to IP addresses is done dynamically. A great advantage in this mobility solution is that the hosts can easily have both the IPv4 and the IPv6 addresses. Furthermore, there is no need to change the current routing methods. Multihoming (fulfills $\mathcal{R}2$) and avoiding man in the middle(MitM) attacks are the other features offered by HIP. The HIP authenticates the connection and establishes security associations for a secure connection with IPsec ESP. For this purpose it uses a four-way handshake with Diffie-Hellman key exchange.
During mobility, HIP protocol is needed to take care of the dynamic binding between the host's IP address and HI as HIs are used to identify the mobile host instead of IP addresses, the location of the host is not bound to the identifier. When one of the communicating peers changes location, it simply sends a HIP

readdress (REA) packet through the secured ESP channel. However, if both of the peers change location at the same time (the double jump problem), a rendezvous server (RSV) is needed [19]. RSV is a packet forwarding agent which simply temporarily forwards the initial HIP packet to the responder.
For HIP an interface selection mechanism was defined in shim API [16], which enables participation from applications in interface selection per packet flow basis for both peers (fulfills $\mathcal{R}3\mathcal{D}$).

3.5 Site Multihoming by IPv6 Intermediation (SHIM6)

The SHIM6 protocol is another multihoming (fulfills $\mathcal{R}2$) host-centric solution [13, 27, 29]. It also introduces a new shim sublayer within the IP layer. It supposes that each host in the network owns multiple global IPv6 address. Each IPv6 address can be used as *locator* for IP routing and identifier or ULID (upper layer ID), for upper layer identification. It also maintains a mapping between locators and ULIDs in all active connections between two hosts. In SHIM6 operation, firstly a normal TCP connection is established between two hosts, then hosts exchange SHIM6 context. At this point, ULIDs and locators have same IPv6 addresses. For failure detection and recovery, SHIM6 uses REAP (REAchability Protocol). In case of any failure, ULIDs will remain same to the upper layers but the underlying locators will change and SHIM6 manages this mapping between locators and ULIDS. Thus the change of locators are transparent to the upper layers. SHIM6 provides denial-of-service (DoS) attack protection to the responder. Although this security measure does not fully preclude the possibility of DoS attacks, at least it imposes an additional effort for the attacker and provides some tracing capabilities.
Interface selection mechanism (fulfills $\mathcal{R}3\mathcal{D}$) is defined in shim API [16], which provides applications the liberty to choose preferred locators for both source & destination host and allows to perform per packet flow distribution.

3.6 Stream Control Transmission Protocol

Stream Transmission Control Protocol (SCTP) is a connection-oriented protocol for the transport layer [9, 37, 38], similar to TCP, but provides message-oriented data transfer, similar to UDP. It provides reliable transmission control, flow and congestion control same as TCP but offers new features such as unordered delivery, multi-streaming and multihoming (fulfills $\mathcal{R}2$). A key difference to TCP is the concept of several streams (sequence of messages) within a connection which are known as associations. During association startup, a list of IP address-port pairs is provided between the communicating hosts. These addresses are used as the endpoints of different streams. One of the addresses is selected as initial primary path, which is used as destination address for all packets and may be changed later if needed. A host has one primary path and zero or more alternative paths. Alternate addresses are used to retransmit packets when any failure occurs on the primary path. The Dynamic address reconfiguration (ADDIP) [44] extension for SCTP enables this protocol to add, delete, and change the IP

addresses during an active connection. The SCTP with the ADDIP extension is called mobile SCTP (mSCTP), and provides a seamless handover for mobile hosts that are roaming between IP networks. The protocol is mainly targeted for client-server services, in which the client initiates the session with a fixed server. For supporting peer-to-peer services, the mSCTP must be used along with an additional location management scheme. SCTP is also incompatible with all old applications.

Being a transport layer protocol, SCTP has the advantage to use security services, offered by the network layer but some vulnerabilities still exist to Men-in-the-Middle attacks. Socket API extension for SCTP [39] describes about implementing interface selection mechanism (fulfills $\mathcal{R}3\mathcal{D}$) but at application level which may not be very efficient.

3.7 MultiPath TCP

Multipath TCP [1, 11] also extends the idea of TCP to add the capability to establish and use multipath between communicating hosts. If the legacy applications want to use all the new features of MPTCP, they would require some changes. The use of an MPTCP socket API being one of them. MPTCP is backward compatible with conventional TCP [33]. The connection establishment in MPTCP begins the same way as in conventional TCP. Signaling messages are used to inform the end user host about MPTCP compatibility. If both endpoints are MPTCP capable and multiple path exists, additional TCP sessions are created on each of the existing path, combining them with existing connection. These additional TCP sessions are also called as sub-flows. In end users network stack applications treat aggregated sub-flows as single MPTCP connection. To exchange available addresses, additional signaling messages are used. Each sub-flow is identified by a five-tuple compound of source and destination address and port as well as used protocol. Sub-flows can be added or removed also after connection establishment.

MPTCP supports concurrent multipath transfer (fulfills $\mathcal{R}2$) using a packet scheduler which divides the byte stream. The byte stream flows through application into segments and allocates these segments to the sub-flows. At the receiver reordering of these segments can be done using sequence numbers. Congestion control across the sub-flows have been proposed in RFC [33]. Multihoming capability of host can support mobility, i.e., if one path fails (or address changes due to host mobility), other paths will still be available but this is a special case in multihoming scenario. For full mobility support the sub-flow disruption due to address changes must be handled which is not provided by MPTCP.

The MPTCP API [33] contains a minimum set of functions which does not allow a user to express preferences about the management of paths or the scheduling of data.

4 Conclusion

This paper has surveyed protocols providing (partial) solutions to interface selection and session continuity in the context of a multihomed mobile network. Multihomed mobile networks & host will be connected through different access technologies and access networks, which offer different services in terms of bandwidth, cost, QoS etc. In order to provide the best available network services, the network interface selection should be influenced dynamically by user preferences, policies, service provider's and network administrator's constraints to adapt the real time environment.
Table 2 summarizes all the multihomed mobility approaches detailed in the previous section. The main results are summarized as:

- Locator/identifier separation approaches such as LISP, HIP, LIN6, SHIM6 are promising to solve mobility and multihoming, but come at the cost of modifying end user hosts or of deploying new network entities such as mapping systems or specialized borders as in LISP.
- Transport layer approaches as SCTP and MPTCP support concurrent multipath transfer, but do not address mobility and multihoming.
- NEMO, together with the MCoA extension, does support network mobility and multihoming but dynamic interface selection is missing.

Table 2. Summary of multihomed mobility approaches

	Approach		MIPv6 +Ext	NEMO	LIN6	LISP	HIP	SHIM6	SCTP	MPTCP
Features	No modification at host network stack		Yes	Yes	No	Yes	No	No	No	No
	Transparency to Application Layer		Yes	Yes	Yes	Yes	Yes	No	No	No
	Additional or modified network entities		HA	HA & MR	mapping agent	border routers, mapping system	PKI, RSV	NA [2]	NA [2]	NA [2]
	Tunneling		Yes	Yes	No	Yes	No	NA [2]	NA [2]	NA [2]
Requirements	Network Mobility $\mathcal{R}1$		No	Yes	No	Yes	No	No	No	No
	Multihoming $\mathcal{R}2$		Yes with McoA	Yes with McoA	Yes	Yes	Yes	Yes	Yes	Yes
	Interface Selection	$\mathcal{R}3S$	Yes with Flow binding	Yes with Flow binding	No	No	No	No	No	No
		$\mathcal{R}3D$	No	No	No	No	Yes with (API)	Yes with (API)	Yes with (API)	No

The filtering mechanism (common feature of all protocols) can help in interface selection by applying specific rules for the flow of packets. The configuration of such rules can be done in two ways, either by using socket API extensions or by relying on inbuilt packet filtering (e.g., NetFilter). A connection socket is identified by associating source & destination IP addresses and ports. The flow binding extensions for Mobile IPv6 and NEMO provide better interface selection mechanism using inbuilt packet filtering at network layer among all surveyed protocols. In HIP and SHIM6, Socket APIs are defined for interface selection. The SCTP API for interface selection supports path maintenance but does not describe the exchange of filtering rules between peers. NEMO together with

[2] NA: Not Applicable

its flow binding extension for nearly fulfills all the requirements of our project except dynamic interface selection. Therefore, our next step is to experiment with interface selection using the flow binding extension of NEMO which is dynamically influenced by user-application preferences, network characteristics, service provider's constraints etc.
In mobile networks, the interface selection requires a communication between user and mobile router. We plan to implement an API, which can communicate between user/application preferences and network level characteristics. Policy management will also be the part of this API, which will store all the required information from user, application, network, service operator, etc. Having all the attributes we would then design an algorithm to select the best available interface for any packet flow. The last step would be to enforce the decision in real time.
We intend to perform feasibility studies of the implemented solutions in terms of scalability, QoS, throughput under various mobility scenarios.

References

1. Barré, S., Paasch, C., Bonaventure, O.: Multipath tcp: from theory to practice. In: NETWORKING, 2011
2. Ben Nacef, A., Montavont, N.: A generic end-host mechanism for path selection and flow distribution. In: IEEE, PIMRC 2008
3. Bernardos-Cano, C.J., Soto-Campos, I., Calderón-Pastor, M., von Hugo, D., Riou, E.: Nemo: Network mobility in ipv6. IPv6 More than A Protocol (2005)
4. Boutet, A., Le Texier, B., Montavont, J., Montavont, N., Schreiner, G.: Advantages of flow bindings: an embedded mobile network use case (2008)
5. Coras, F., Jakab, L., Lewis, D., Domingo-Pascual, J., Cabellos-Aparicio, A.: Lisp network element deployment considerations (2014)
6. Devarapalli, V., Wakikawa, R., Petrescu, A., Thubert, P.: Network mobility (nemo) basic support protocol. RFC 3963 (2005)
7. Eddy, W.M.: At what layer does mobility belong? Communications Magazine, IEEE (2004)
8. Farinacci, D., Lewis, D., Meyer, D., Fuller, V.: The locator/id separation protocol (lisp) (2013)
9. Fu, S., Atiquzzaman, M.: Sctp: state of the art in research, products, and technical challenges. Communications Magazine, IEEE (2004)
10. Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B.: Proxy mobile ipv6. RFC 5213 (2008)
11. Handley, M., Raiciu, C., Ford, A., Iyengar, J., Barre, S.: Architectural guidelines for multipath tcp development. RFC 6182 (2011)
12. Hurson, A.: Connected computing environment, vol. 90. Academic Press (2012)
13. Huston, G.: Architectural commentary on site multi-homing a level 3 shim (2005)
14. Iannone, L., Saucez, D., Bonaventure, O.: Implementing the locator/id separation protocol: Design and experience. Computer Networks (2011)
15. Johnson, D., Perkins, C., Arkko, J.: Mobility support in ipv6. RFC 3775 (2004)
16. Komu, M., Bagnulo, M., Slavov, K., Sugimoto, S.: Socket application program interface (api) for multihoming shim. draft-ietf-shim6-multihome-shim-api-03 (2007)
17. Koodli, R.: Mobile ipv6 fast handovers. RFC 5568 (2009)
18. Kunishi, M., Ishiyama, M., Uehara, K., Esaki, H., Teraoka, F.: Lin6: A new approach to mobility support in ipv6. In: WPMC (2000)
19. Laganier, J., Eggert, L.: Host identity protocol (hip) rendezvous extension (2008)

20. Le, D., Fu, X., Hogrefe, D.: A review of mobility support paradigms for the internet. IEEE Communications Surveys and Tutorials (2006)
21. Matsushima, S., Telecom, S., Okimoto, T., West, N., Wing, D.: Ipv6 multihoming without network address translation. RFC 7157 (2014)
22. Mihailovic, A., Leijonhufvud, G., Suihko, T.: Providing multi-homing support in ip access networks. In: IEEE, PIMRC 2002
23. Mitsuya, K., Kuntz, R., Sugimoto, S., Wakikawa, R., Murai, J.: A policy management framework for flow distribution on multihomed end nodes. In: ACM/IEEE international workshop on Mobility (2007)
24. Moskowitz, R., Nikander, P.: Host identity protocol architecture. RFC 4423 (2006)
25. Moskowitz, R., Nikander, P., Jokela, P., Henderson, T.: Host identity protocol. RFC 5201 (2008)
26. Nikander, P., Gurtov, A., Henderson, T.R.: Host identity protocol (hip): Connectivity, mobility, multi-homing, security, and privacy over ipv4 and ipv6 networks. Communications Surveys & Tutorials, IEEE (2010)
27. Nordmark, E., Bagnulo, M.: Shim6: Level 3 multihoming shim protocol for ipv6. RFC 5533 (2009)
28. Perkins, C.: Ip mobility support for ipv4. RFC 3344 (2002)
29. Rahman, M.S., Atiquzzaman, M.: Semo6-a multihoming-based seamless mobility management framework, milcom. IEEE (2008)
30. Ropitault, T., Montavont, N.: Implementation of flow binding mechanism. In: IEEE PerCom 2008
31. Saaty, T.L.: How to make a decision: the analytic hierarchy process. European journal of operational research (1990)
32. Saucez, D., Iannone, L., Bonaventure, O., Farinacci, D.: Designing a deployable internet: the locator/identifier separation protocol. Internet Computing, IEEE (2012)
33. Scharf, M., Ford, A.: Multipath tcp (mptcp) application interface considerations. RFC 6897 (2013)
34. Shen, C., Du, W., Atkinson, R., Kwong, K.H.: Policy based mobility & flow management for ipv6 heterogeneous wireless networks. Wireless Personal Communications (2012)
35. Soliman, H., Bellier, L., Elmalki, K., Castelluccia, C.: Hierarchical mobile ipv6 (hmipv6) mobility management. RFC 5380 (2008)
36. Song, Q., Jamalipour, A.: A network selection mechanism for next generation networks. In: IEEE ICC 2005
37. Stewart, R.: Stream control transmission protocol (2007)
38. Stewart, R., Metz, C.: Sctp: new transport protocol for tcp/ip. Internet Computing, IEEE (2001)
39. Stewart, R., Xie, Q., Yarroll, L., Wood, J., Poon, K., Tuexen, M.: Sockets api extensions for stream control transmission protocol (sctp) (2006)
40. Suciu, L., Bonnin, J., Guillouard, K., Stévant, B.: Towards a highly adaptable user-centric terminal architecture. In: Intl. Symp. on WPMC 2004
41. Teraoka, F., Ishiyama, M., Kunishi, M.: Lin6: A solution to multihoming and mobility in ipv6. draft-teraoka-multi6-lin6-00 (2003)
42. Triantaphyllou, E.: Multi-criteria decision making methods. In: Multi-criteria Decision Making Methods: A Comparative Study (2000)
43. Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., Kuladinithi, K.: Flow bindings in mobile ipv6 and nemo basic support. RFC 6089 (2011)
44. Tuexen, M., Maruyama, S., Kozuka, M.: Network working group r. stewart internet-draft cisco systems (2007)
45. Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., Nagami, K.: Multiple care-of addresses registration. RFC 5648 (2009)
46. Wakikawa, R., Paik, E., Ng, C., Kuladinithi, K., Noel, T.: Goals and benefits of multihoming draft-ernst-generic-goals-and-benefits-01
47. White, C., Lewis, D., Meyer, D., Farinacci, D.: Lisp mobile node (2014)
48. Ylitalo, J., Jokikyyny, T., Kauppinen, T., Tuominen, A.J., Laine, J.: Dynamic network interface selection in multihomed mobile hosts. In: IEEE, HICSS 2003