

INTERNET-DRAFT
[draft-miller-homedisc-req-00.txt](#)
May 26, 1999
Expires November 26, 1999

Brent Miller
Thomas Narten
Marcia Peters
John Tavs
IBM Corp.

Home Networking Device and Service Discovery Requirements

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

Networks in the home and similar environments typically do not have, and should not be expected to have a full range of network services such as DHCP servers, DNS and the like. Further, networks in the home and similar environments may have only occasional connectivity to a larger network such as the Internet where these types of services may exist. Typical users of home networks may not have the skills or desire to install, configure, administer and maintain a sophisticated home network.

To enable the effective use of networks in the home and similar environments, methods for discovering devices and services in the network are needed. These methods need to work for occasionally connected and often resource-poor networks such as are typically found in the home. These methods also need to be self-configuring, requiring only minimal involvement of users of a home or similar network to configure and maintain that network.

This document presents requirements for the discovery of devices and services in a home network or similar environment. These

requirements are intended to form a basis that enables further work toward solutions in this area.

Scope

This document discusses the ability to introduce new devices into a given environment. While not limited to a home environment, consideration from a home environment perspective is quite useful in developing the requirements for the problem space of interest. If home requirements are developed, we assert that the same set of requirements will also apply in other environments (such as hotel, SOHO, vehicle, and so on); these requirements may not be sufficient in all other interesting environments but they are likely to be necessary.

Scenario

To illustrate the problem statement that leads to requirements, a home networking scenario is presented. Generically, this scenario considers the introduction of a new device into a home network.

The specific scenario presented here is that of a new computer being introduced to an existing home network (other scenarios could also be developed). The newly introduced computer, to be fully utilized, needs to become a participant in the "home area network". It needs to make itself known to the other network participants, including services that it can offer to them (perhaps it is capable of router functions, or has specific software services that other devices can use). The computer also needs to become aware of the other network participants, including services that they offer that may be of interest (perhaps another computer in the home network offers printing services or image capture services; the newly introduced computer also needs to find the network access point to the larger network).

In a home environment, these functions need to be self-configuring (accomplished with minimal user setup and configuration). This process should "just work", not requiring extensive user knowledge of the network nor onerous configuration or administration processes.

This scenario assumes a home environment, although as noted above, the problem statement and requirements that arise from this scenario are likely to apply to other similar environments. For this scenario, we assume that:

1. The home network is connected to a larger network (like the Internet), but only intermittently. The home network needs to be fully usable whether or not it is connected to the larger network.

2. The devices in the home network use IETF protocols, having at least a TCP/IP stack.

Problem Statement

To accomplish the above scenario and others like it, problems to be solved include:

1. The device needs to achieve connectivity into "the network", where "the network" is not necessarily (and is not likely to be) like the Internet or an intranet with all of its requisite services, such as DHCP servers, name servers, directory servers, time servers, file servers, print servers and so on. The home network needs to be fully usable even when not connected to the larger network, where the services listed above may reside.
2. The device needs a secure and interoperable way to "advertise" the services it provides to "the network".
3. The device needs a secure and interoperable way to provide (allow other network participants to make use of) those services that it makes available to other devices on "the network".
4. The device needs a secure and interoperable way to ascertain what other services are available in "the network".
5. The device needs a secure and interoperable way to access (make use of) appropriate services in "the network".

Note that in order to enable service discovery, device discovery using protocol layers 1-4 is required. Before service discovery can be accomplished, it is probably necessary to learn a layer-2 address such as a MAC address or virtual circuit identifier, and/or a layer-3 address like an IP address. In considering the device discovery process, it is important to understand the scope of the message -- how far it can travel and what blocks it. (Consider a layer-2 service such as Ethernet broadcast, a layer 3 service such as IP multicast, and layer 4 services like a UDP datagram to a NDS or a NetBIOS Name Server or a WINS server. Based upon the network topology, configuration and policies, broadcast or multicast messages might be locally confined, or they might traverse multiple routers, perhaps being limited by filters or hop counts). Scoping is important in discovering that a target device exists without unnecessarily broadcasting outside the required scope and potentially "flooding" larger and larger networks. Furthermore, there may be multiple target devices of interest (and even invalid duplicate devices) that appear within different scopes. Scoping is also important in the area of security. In developing the device and service discovery

requirements and potential solutions for home or similar environments, where "the network" may not resemble the Internet model, scoping is an important consideration.

Requirements

To solve this problem statement in this problem domain, the following functional requirements need to be satisfied:

1. Physical connection, link and transport: These components are needed for basic connectivity in any networked environment. While it is useful to note this requirement, it is not a primary focus of this document; instead, this document focuses primarily on those layers above the transport layer but below the application layer that can enable device and service discovery, assuming that physical connection, link and transport layers appropriate to "the network" are in place. In fact, many of "the networks" of interest may be ad-hoc and/or peer-to-peer.
2. Device identification and address assignment: This deals with recognizing a device's presence on "the network", potentially including determining (at least generically) what type of device it is and what capabilities it has; and assigning an IP address to the device (without necessarily having connectivity to a larger network). The symmetric operation of de-assigning IP addresses when devices no longer require them also needs to be considered.
3. Device naming/"the network" name space: This deals with mapping a name, defined by some schema, to a device or service; and with managing the local name space for the devices in "the network" (which perhaps might include multiple names for a given device), all without necessarily having access to a larger network. The symmetrical operation of deregistering names when devices or services are removed or renamed needs to be considered. Security aspects of managing the name space, such as authentication, also need to be considered.
4. Device lookup and discovery: This deals with the protocols and mechanisms (which may include some of the lower layers of item 1 above) used to determine that a new device is present and to establish communications with a specified device.

5. Service lookup and discovery: This deals with the protocols and mechanisms (which may include some of the lower layers of item 1 above) used to determine that a new service is present. Discovery includes that part of a service discovery protocol that specifies how a client locates the network infrastructure such as a registry (if there is one), including how it can register itself and its services. Lookup defines how a client queries the registry (if there is one) to locate a service it needs, and how it locates the service in the absence of a registry. Security aspects of service lookup and discovery, such as authentication and controlling access to the service registry, also need to be considered.

Note that once a service has been located, other steps may be necessary to make use of the service. For instance, a client may need to negotiate access to the service, including "quality of service" and security considerations. Further, once a client has located a service and has successfully negotiated access to the service, the client may need to determine (and in some cases, obtain a mechanism that implements) the protocol(s) that the client uses to actually make use of the service (examples include IPP, LPR, HTTP, FTP, Java(TM) RMI, and so on). These facets of service discovery are outside the scope of this document.

Another requirement consideration for home networking is dealing with device constraints. In the home and similar environments, consumer electronics, mobile devices and other information appliances which may be network participants are often constrained in at least the areas of total memory (which may be quite small), processing capability (especially for things like encryption), persistent storage (which might be zero), communications bandwidth (which can be quite low, especially in wireless environments), and unique device identification (which may not exist at all, unlike typical IP network devices). While not a unique requirement for device and service discovery, solutions in this space need to consider device constraints for each aspect of device and service discovery.

Technology-to-Requirements Mapping

This section maps the above requirements to a selected set of technologies that might be used to satisfy those requirements. This section is intended to provide background information for consideration in developing solutions to address the requirements and problem statement noted herein. While there are numerous standards and technologies in the area of device and service discovery, this document considers a relatively small set of "interesting" technologies, namely:

1. IETF protocols such as DHCP [1], DNS [2] and LDAP [3]
2. Some well-known IP-centric existing or proposed service discovery technologies, such as the Microsoft-sponsored Universal Plug and Play (UPnP) initiative [4], Service Location Protocol (SLP) [5], Salutation(TM) [6] and Sun's Jini(TM) technology [7].

This is not an exhaustive list of technologies that might be considered; however, we assert that this is a useful set of technologies to consider when evaluating various approaches to satisfying the requirements set forth here. This section is intended to promote discussion that is aimed at developing an interoperable solution for the problem space of interest; it is not intended to promote any particular technologies. Mapping the requirements set forth here to an illustrative set of technologies can aid in better understanding the problems and the requirements.

1. Physical connection, link and transport: While these items are needed in a solution, they are not a primary focus of this document and thus are not further detailed. An illustrative technology for satisfying this requirement is Ethernet-TCP/IP.
2. Device identification and address assignment:
 - DHCP [1] provides a method of identifying a device in an IP network via a unique MAC address and assigning a global IP address to the device.
 - In [8], Troll proposes Automatic Private IP Addressing to assign link-local IP addresses in the absence of a DHCP server.
3. Device naming/"the network" name space:
 - DNS [2] provides name-to-IP address mapping and a hierarchical scheme for managing multiple name spaces.
 - In [9], Woodcock and Manning propose Multicast Name Resolution to achieve DNS-like function in the absence of a DNS.
 - Salutation [6] defines a naming scheme for Salutation devices consistent with the local network (such as TCP/IP or IrDA).
4. Device lookup and discovery:
 - DNS [2] provides a well-defined protocol for looking up devices in an IP network.
 - In [9], Woodcock and Manning propose Multicast Name Resolution to achieve DNS-like function in the absence of a DNS.
 - LDAP [3] can be used to lookup devices that have been

populated in an LDAP directory.

- Salutation [6] defines a method for looking up other Salutation devices and determining their capabilities.

5. Service lookup and discovery:

- SLP [5] provides a discovery mechanism, based upon an IP multicast (or IP unicast if an optional directory agent exists), as well as a service lookup protocol for both a registry and a service provider, including schema for common services that can be used to match service requests with available services.
- Salutation [6] provides a discovery mechanism, based upon point-to-point or broadcast communications, as well as a service lookup protocol and API for a service provider, including schema for common services that can be used to match service requests with available services.
- Jini [7] provides a discovery mechanism and service registry where services can be advertised, as well as a service lookup facility that leverages the Java platform.
- LDAP [3] can be used to look up services that have been populated in an LDAP directory.
- UPnP proposes IP multicasts to discover services and to announce service availability, and can use IP unicast if an (optional) directory exists.

Technology-to-Requirements Matrix

The above mapping is also presented in table form in Figure 1 on page 8. The table does not include the physical connection, link and transport requirement (as noted above, this is not the primary purpose of this document) nor the Security and Device constraint requirements (while these must be considered in a solution, they cross the other requirements).

	Device ID and IP Addr Assignment	Naming	Device Lookup, Discovery	Service Lookup, Discovery	
DHCP	Global (IP)				
DNS		Yes (IP)	Lookup (IP)	Lookup (static)	
LDAP			Lookup (LDAP)	Lookup (LDAP)	
UPnP	Local (IP)	Yes (IP)	Lookup (IP), Discovery (IP)	Multicast Discovery, Unicast Directory Discovery, Directory Lookup	
SLP				Multicast Discovery, Unicast Registry Discovery, Registry Lookup	
Salu- tat- ion		Yes (Saluta- tion)	Lookup (Salutation) Discovery (Salutation)	Broadcast or Unicast Discovery, Registry Lookup	
Jini				Registry discovery, Registry Lookup	

Figure 1. Technology-to-Requirements Matrix

Cited References

- [1] Droms, R., "Dynamic Host Configuration Protocol", [RFC2131](#), March 1997.
- [2] Mockapetris, P., "Domain Names -- Concepts and Facilities", STD13, [RFC1031](#), November 1987.
- [3] Yeong, W., Howes, T., and Kille, S., "Lightweight Directory Access Protocol", [RFC1777](#), March 1995.
- [4] Microsoft Corp., "A Universal Plug and Play Primer", <http://www.microsoft.com/hwdev/homenet/upnp.htm>, January 1999.
- [5] Veizades, J., Guttman, E., Perkins, C. and Kaplan, S., "Service Location Protocol", [RFC2165](#), June 1997.
- [6] Salutation Consortium, Inc., "Salutation Architecture: an Overview", <http://www.salutation.org/tour/index.html>.
- [7] Sun Microsystems, "Jini Technology Executive Overview", <http://java.sun.com/products/jini/>, January 1999.
- [8] Troll, R., "Automatically Choosing an IP Address in an Ad-Hoc IPv4 Network", [draft-ietf-dhc-ipv4-autoconfig-03.txt](#),

January 1999.

- [9] Woodcock, B. and Manning, B., "Multicast Discovery of DNS Services", [draft-manning-multicast-dns-01.txt](#), December 1998.

INTERNET-DRAFT
[draft-miller-homedisc-req-00.txt](#)

Miller et al.
IBM Corp.

Notices

Java(TM) and Jini(TM) are registered trademarks of Sun Microsystems. Salutation(TM) is a registered trademark of The Salutation Consortium, Inc.

Authors' Addresses

Brent A. Miller
IBM Corporation
3039 Cornwallis Road
Research Triangle Park, NC 27709 USA
email: bamiller@us.ibm.com

Thomas Narten
IBM Corporation
3039 Cornwallis Road
Research Triangle Park, NC 27709 USA
email: narten@us.ibm.com

Marcia Peters
IBM Corporation
3039 Cornwallis Road
Research Triangle Park, NC 27709 USA
email: mlpeters@us.ibm.com

John Tavs
IBM Corporation
3039 Cornwallis Road
Research Triangle Park, NC 27709 USA
email: tavs@us.ibm.com

