WS-Discovery Primer

06 October 2008

Abstract:

This document describes WS-Discovery protocol operation modes, actors and their behavior and message exchange patterns in these operational modes. The primary goal of this document is to increase understanding of WS-Discovery protocol specification and provide clarity of behaviors of actors in an ad-hoc and a managed mode of protocol operation.

Author:

Vipul Modi (Microsoft)

.

Table of Contents

1 Introduction

WS-Discovery [**WS-Discovery**] is a simple, dynamic, extensible web services protocol to locate services. The primary goal of the protocol is to enable discovery of a Target Service by a Client. This document describes WS-Discovery operation modes, actors and behavior of the actors in these operational modes. The document also describes example scenarios involving Discovery Proxy.

1.1 Actors

The WS-Discovery protocol defines three main actors.

Target Service: An endpoint that makes itself available for discovery. The Client is looking for the information on Target Service.

Client: An endpoint that searches for Target Services(s).

Discovery Proxy: This is a network service that facilitates the discovery of Target Service in a managed mode (see Section 1.2 Operation Modes). It helps to reduce multicast traffic on an ad-hoc network, enables discovery beyond the reach of ad-hoc networks and enables managed discovery with custom security policies.

1.2 Operation Modes

There are two main operational modes of discovery, ad-hoc and managed.

To understand these discovery modes let's consider a scenario where Ms. Jane Doe at the airport facilities need to locate and talk to an employee named Mr. John Doe.

Using the public broadcasting system Ms. Jane Doe announces following; "Mr. Jon Doe please pick the white paging telephone." Upon hearing this broadcast message, Mr. Jon Doe picks up the nearest white paging telephone and talks to Ms. Jane Doe. This mode of discovery is called an ad-hoc mode.

Alternatively, Mr. Jon Doe can enter his whereabouts in a central computer system every time he goes to a different area of the airport. Ms. Jane Doe can now look up the whereabouts of Mr. Jon Doe in the central computer system. In this scenario the central computer system assisted in discovery of Mr. Jon Doe, this mode is called a managed mode.

1.2.1 Ad-hoc Discovery Mode

This is a mode of discovery in which the Target Services are responsible for advertising their presence on the network and responding to discovery queries from Clients. In this mode the protocol messages are sent multicast on the network.

A network in which the discovery of Target Services is carried out in an ad-hoc manner is called an ***ad-hoc network***.

1.2.2 Managed Discovery Mode

This is a mode of discovery in which the discovery of Target Services is assisted by a network service called Discovery Proxy. In this mode the protocol messages are sent unicast to Discovery Proxy.

A network in which the discovery is carried out in a managed manner is called a ***managed network***.
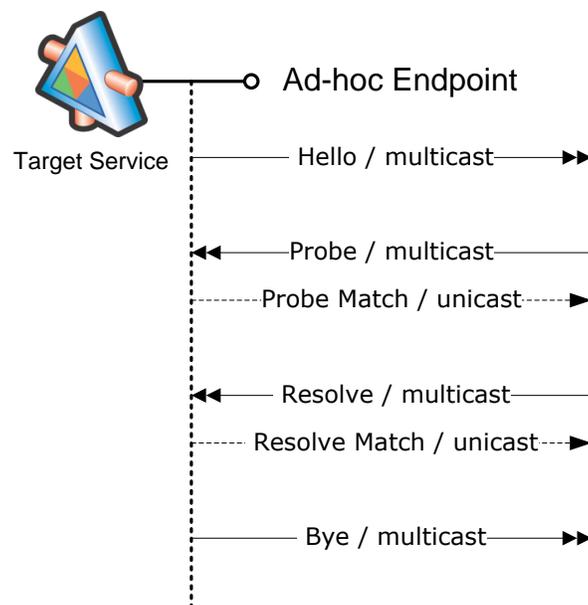
2 Target Service

This section describes the behavior of a Target Service in an ad-hoc and a managed mode. A Target Service can operate in an ad-hoc mode, a managed mode or both modes, depending upon its configuration.

2.1 Ad-hoc Mode

In an ad-hoc mode, a Target Service,

- Announces its availability by sending a multicast Hello message.
- Listens for and responds to multicast discovery queries Probe and Resolve.
- Announces its departure by sending a multicast Bye message.

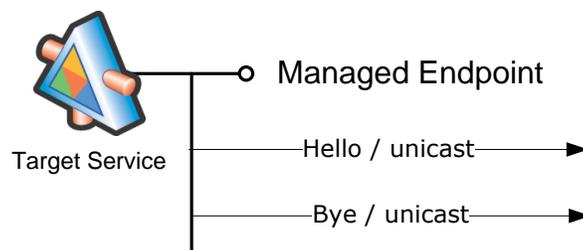Figure 1 shows message exchanges of a Target Service operating in an ad-hoc mode.

Figure 1: Message exchanges of a Target Service in an ad-hoc mode.

2.2 Managed Mode

In a managed mode a Target Service,

- Announces its availability by sending a unicast Hello to a Discovery Proxy.
- Announces its intent of departure by sending a unicast Bye to a Discovery Proxy.

Figure 2 shows messages exchanges of a Target Service operating in a managed mode.

**Figure 2: Message exchanges of a Target Service in a managed mode.**

57   A Target Service needs an address of a Discovery Proxy to operate in a managed mode. A Target
58   Service can acquire this information from a number of ways such as explicit Probe for a Discovery Proxy
59   on an ad-hoc network, explicit configuration, DNS or DHCP.

60

61   Note that even though a managed mode interaction is defined in the current specification, many of the
62   services and devices shipped today support only ad-hoc mode and this is fine. As mentioned above a
63   Target Service may operate ether in an ad-hoc mode or a managed mode or both based on its
64   configuration. Figure 3 shows an example Target Service configured to operate in an IP multicast ad-hoc
65   network and two managed networks DP1 and DP2. This Target Service multicasts announcement
66   messages (Hello and Bye) on an IP multicast ad-hoc network and unicasts them to both DP1 and DP2. It
67   also listens for multicast Probe and Resolve messages sent by Clients on the IP multicast ad-hoc network
68   and responds appropriately with Probe Match and Resolve Match messages.

69
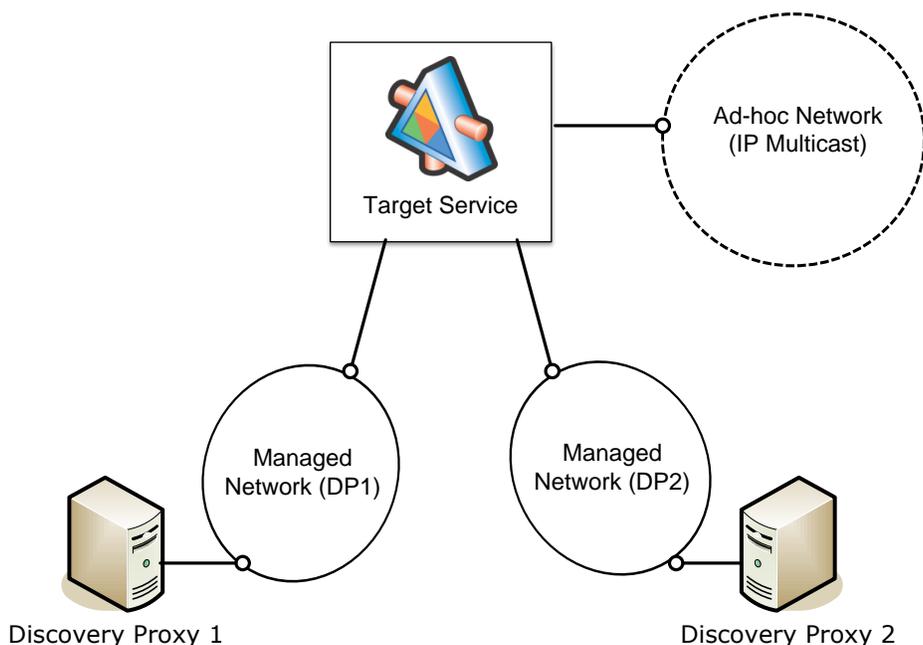
70
71   **Figure 3: A Target Service operating in more than one mode**

72   It is possible that a Target Service may not support managed mode directly due to implementation
73   limitations. If such Target Services wants to participate in the managed mode discovery, they may
74   consider using an agent that works on behalf of one or more Target Services and coverts the ad-hoc
75   mode announcement messages to a managed mode. The agent may be provided by the Target Service
76   or by a Discovery Proxy implementation.

77 3 Client

78 This section describes the behavior of a Client in an ad-hoc and a managed mode. A Client can be
79 configured to operate in an ad-hoc mode, a managed mode or switch dynamically from one to the other
80 as described below.

81 3.1 Ad-hoc Mode

82 In an ad-hoc mode a Client,

83 • Discovers Target Services by sending multicast Probe and Resolve messages.
84 • Listens for multicast Hello and Bye messages.

85 Figure 4 below shows messages exchanges of a Client operating in an ad-hoc mode. As indicated in the
86 figure a Client may receive Hello message in response to a multicast Probe / Resolve. This is described
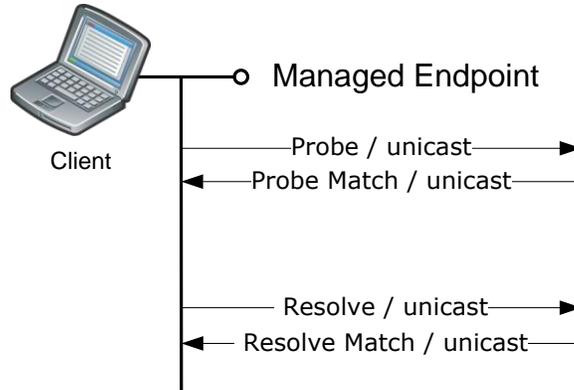87 in the Section 3.3 Dynamic Mode Switching.
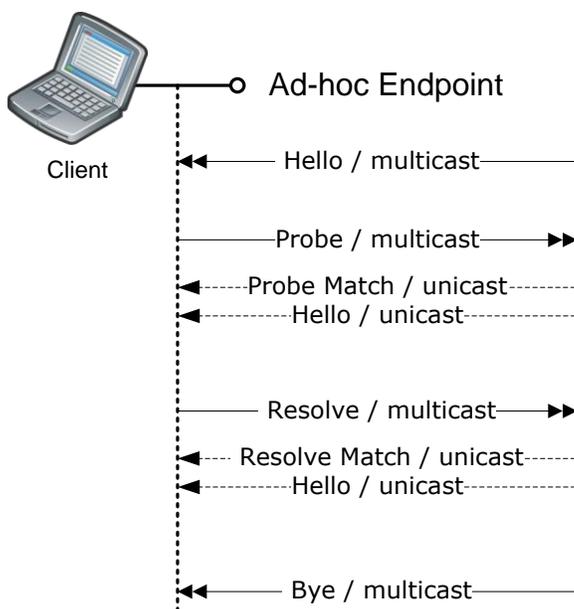
88

89 **Figure 4: Message exchanges of a Client in an ad-hoc mode.**

90 3.2 Managed Mode

91 In a managed mode a Client,

92 • Discovers Target Services by sending unicast Probe and Resolve messages to a Discovery
93 Proxy.

94 Figure 5 below shows message exchanges of a Client operating in a managed mode.

Managed Endpoint

————Probe / unicast————▶
◀————Probe Match / unicast————

————Resolve / unicast————▶
◀————Resolve Match / unicast————

Client

Figure 5: Message exchanges of a client in a managed mode.

97 To operate in a managed mode, a Client needs an address of the Discovery Proxy. A Client can acquire
98 this information from a number of ways such as explicit Probe for a Discovery Proxy on an ad-hoc
99 network, explicit configuration, DNS or DHCP. One such method that reduces the multicast traffic on an
100 ad-hoc network and allows Client to dynamically switch from an ad-hoc mode to a managed mode is
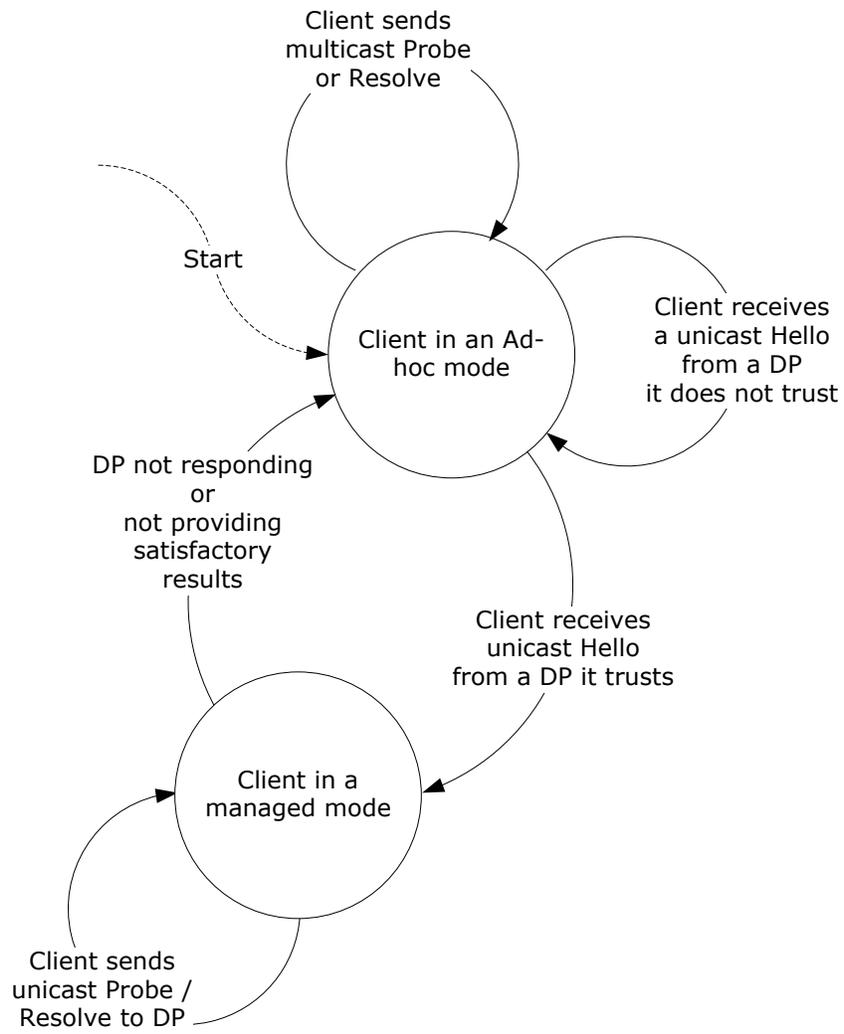101 called "*multicast suppression*" as described below.

3.3 Dynamic Mode Switching

103 A Client may be configured to dynamically switch from an ad-hoc to managed mode and vice versa,
104 based on the presence of a Discovery Proxy on the network. In this configuration a Client starts in an ad-
105 hoc mode and multicast Probe/Resolve requests. If there is a Discovery Proxy on the network that can
106 effectively represent the Target Services on that network it will send a multicast suppression Hello
107 message in response to a Probe/Resolve message. Upon receiving this message Client can assume that
108 a Discovery Proxy has a sufficient knowledge of the Target Services on that ad-hoc network and should
109 use the Discovery Proxy instead of multicasting the network. The Client then can use this Discovery
110 Proxy for future requests instead of multicasting the requests to the ad-hoc network.

111 Note that upon receiving a Hello message Client may continue to operate in an ad-hoc mode because of
112 variety of reasons including but not limited to; a) explicit configuration to operate in ad-hoc mode or b)
113 security policies.

114 Once in managed mode, a Client may dynamically switch back to ad-hoc mode for reasons including but
115 not limited to; a. unsatisfactory response from DP, b. DP being unresponsive.

116 The figure below shows the state transition for a client that is configured to dynamically switch from an
117 ad-hoc to a managed mode and vice versa.

Client sends
multicast Probe
or Resolve

Start

Client in an Ad-
hoc mode

Client receives
a unicast Hello
from a DP
it does not trust

DP not responding
or
not providing
satisfactory
results

Client receives
unicast Hello
from a DP it trusts

Client in a
managed mode

Client sends
unicast Probe /
Resolve to DP

118

119   **Figure 6: State transitions of a Client configured to switch operational modes dynamically.**

4 Discovery Proxy

120

121 This section describes the behavior of a Discovery Proxy in an ad-hoc and a managed mode. A
122 Discovery Proxy can be configured to operate in a managed mode or ad-hoc mode or both. Additionally it
123 can be configured to act as a multicast suppression agent in an ad-hoc mode as described below.

124 In this section let's first describe the managed mode aspect of a Discovery Proxy.

4.1 Managed Mode

125

126 A Discovery Proxy in a managed mode can be thought of a "service" that facilitates/brokers the discovery
127 of other Target Services. This "service",

128 • Listens for unicast Hello and Bye messages from a Target Service and stores and updates this
129   information in its internal cache/store.
130 • Listens for and responds to unicast Probe and Resolve message from Clients on behalf of the
131   Target Services it represents, i.e; the Target Services that are present in its cache/store.

132 Figure 7 shows the message exchanges of a Discovery Proxy operating in a managed mode.
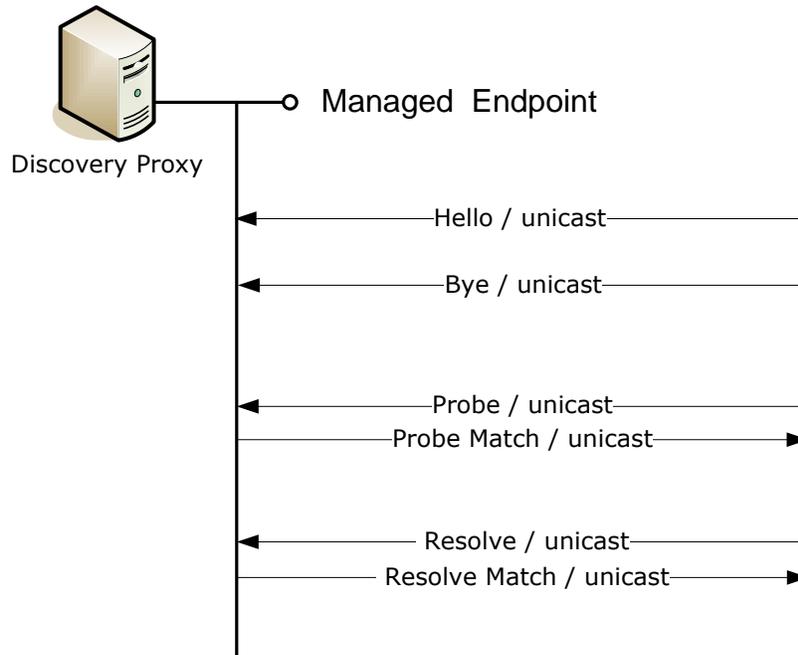
133

134 **Figure 7: Message exchanges of a Discovery Proxy in a managed mode.**

4.2 Ad-hoc Mode

135

136 The "service" called Discovery Proxy described in previous section facilitates/brokers the discovery of
137 other Target Services. This service needs to be known to the Target Services and Clients, so that they
138 can make use of it. Thus it advertises itself on an ad-hoc network as a Discovery Proxy providing the
139 information about its endpoint operating in the managed mode. It also listens for Probe/Resolve requests
140 on an ad-hoc network and responds to them if they are for Discovery Proxy, again providing the
141 information about its managed endpoint.

142 In addition to this a Discovery Proxy may be configured to reduce multicast traffic on the network by
143 effectively collecting the information and representing all of the Target Services on that network. It does
144 that by using one or more ad-hoc discovery mechanisms such as listening for multicast Hello and Bye
145 from the Target Services and/or sending regular multicast Probe. It then offers the Clients to query this
146 information via managed mode. It also notifies the Client to switch to the managed mode via "multicast

147 suppression" mechanism; i.e. sending a Hello message with the information about the managed mode
148 endpoint in response to multicast Probe/Resolve requests from the client.

149 Based on the description above a Discovery Proxy in an ad-hoc mode,

150 • Acts as a Target Service and advertises itself as a Discovery Proxy.
151 - Sends multicast Hello and Bye message containing information about its managed
152 mode endpoint.
153 - Listens for and responds to multicast Probe/Resolve and responds to the matching
154 ones with the information about its managed mode endpoint.
155
156 • Acts as a multicast suppression agent.
157 - Collects the information about Target Services operating on an ad-hoc network by
158 listening for multicast Hello and Bye messages from Target Services and probing for
159 Target Services.
160 - Represents the Target Services operating on an ad-hoc network
161 - Hosts a managed endpoint that allows querying for these services in a managed
162 mode.
163 - Respond to multicast Probe and Resolve messages from Client that are looking for
164 these Target Services by responding with multicast suppression Hello message and
165 redirecting them to the managed endpoint that can respond to these querying in a
166 managed mode.
167

168 Figure 8 shows the message exchanges of a Discovery Proxy operating in an ad-hoc mode.
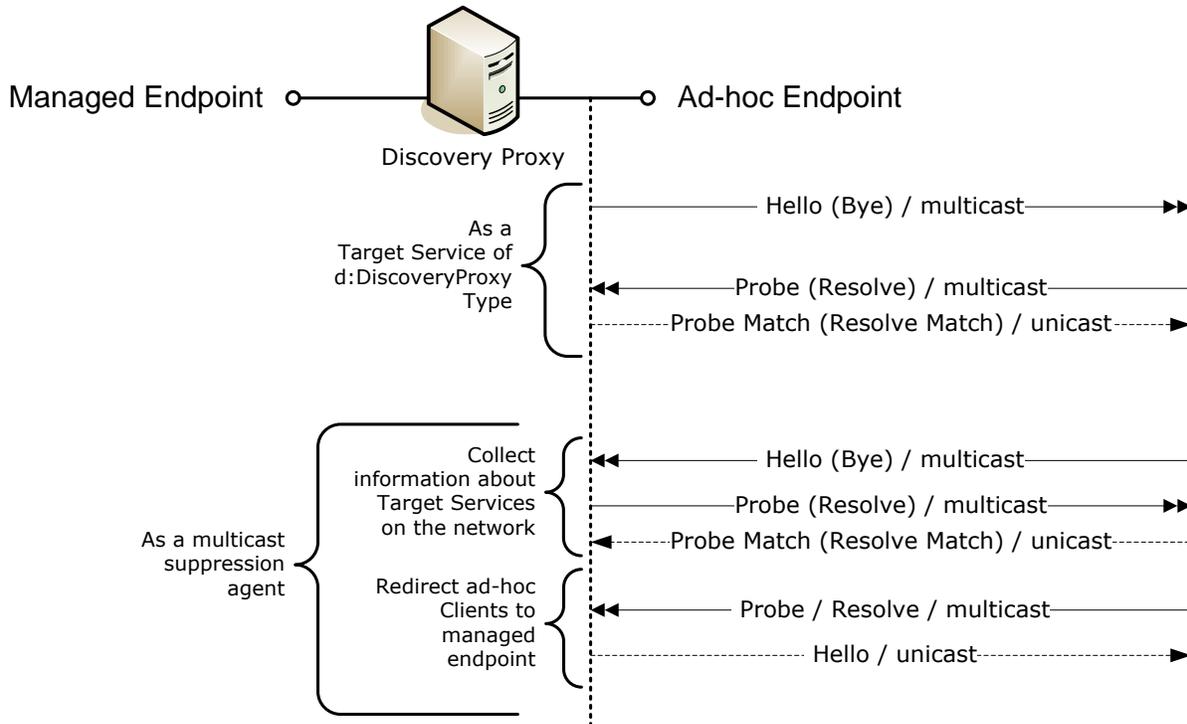
169
170

171 **Figure 8: Message exchanges of a Discovery Proxy in an ad-hoc mode.**

172 5 Discovery Proxy Scenarios

173 This section describes typical scenarios that can be supported by an implementation of Discovery Proxy.
174 Note that different implementations may have different features and may support different scenarios.

175 5.1 Multicast Suppression

176 This scenario illustrates the use of Discovery Proxy as multicast suppression agent on an ad-hoc network.
177 Figure 9 shows the scenarios and the sequence of events.

178
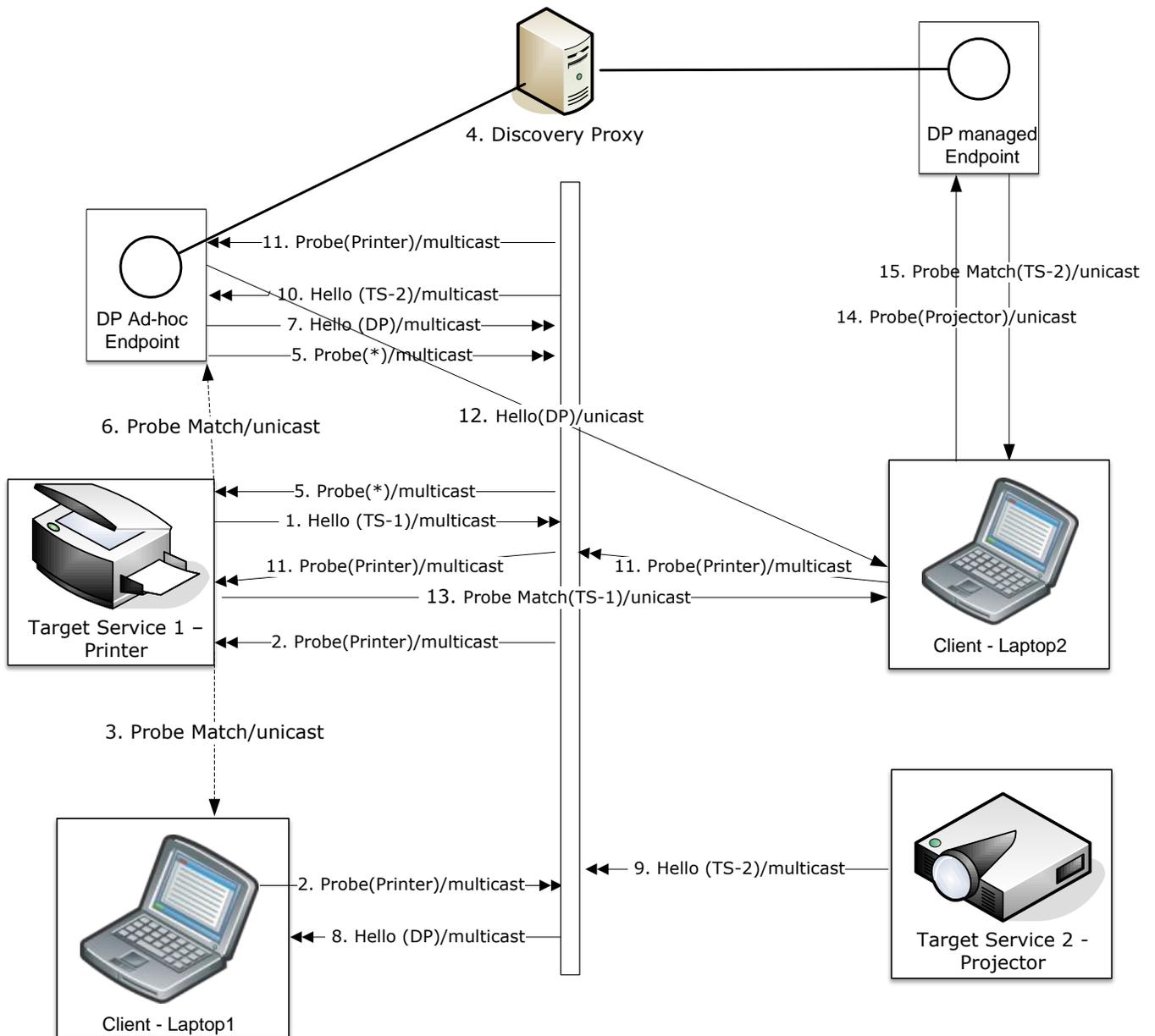
179
180

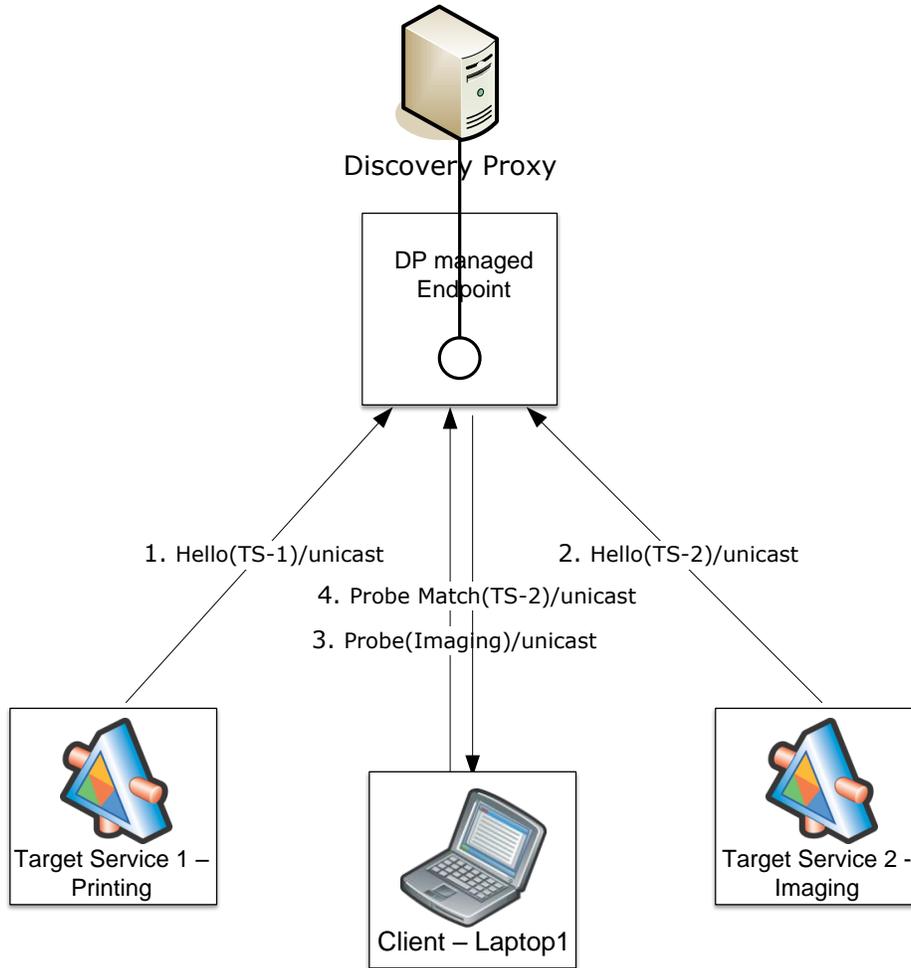181 **Figure 9: Discovery Proxy in a multicast suppression scenario.**

182

183   Following is the description of the scenario and interaction between the actors involved in the scenario.

184

1. Target Service 1 – Printer (TS-1) comes online and sends a multicast Hello on the network.

2. Client – Laptop1 joins the network and is looking for Printer services on the network. It sends a multicast Probe.

3. Target Service 1 – Printer receives the multicast Probe and responds to Client – Laptop1. The Client – Laptop1 gets the information about TS-1.

4. To reduce the multicast traffic related to discovery queries from the Clients, a Discovery Proxy (DP) is deployed to the network.

5. The Discovery Proxy sends a Probe to get information about all Target Services available on the network.

6. The Target Service 1 – Printer responds normally as it would to any other Client. Discovery Proxy stores this information to its cache.

7. The Discovery Proxy sends a multicast Hello announcing its managed endpoint.

8. The Client – Laptop1 receives a multicast Hello from Discovery Proxy and stores it to use it for the next query.

9. A Target Service 2 – Projector (TS-2) comes online and sends a multicast Hello on the network.

10. The Discovery Proxy receives the multicast Hello from the Target Service 2 – Projector and updates its cache.

11. A Client – Laptop2 joins the network and is looking for Printers; being unaware of the Discovery Proxy it sends a multicast Probe message.

12. The Discovery Proxy receives the multicast Probe and sends a multicast suppression Hello message containing the information about its managed endpoint. The Client – Laptop2, upon receiving multicast suppression Hello message from a Discovery Proxy switches to a managed mode.

13. The Target Service 1 – Printer and Target Service 2 – Scanner receives the multicast Probe and Target Service 1 – Printer responds normally with unicast Probe Match.

14. The Client – Laptop2 needs to now look for Projector services, being switched to a managed mode; it sends a unicast Probe to the Discovery Proxy.

15. Discovery Proxy responds to the Client – Laptop2 and provides information about Target Service 2 – Projector.

5.2 Enterprise Service Registry

230   This scenario shows the use of Discovery Proxy as an enterprise service registry that provides discovery
231   of services in a completely managed environment. In this scenario Target Services and Clients know a
232   Discovery Proxy to communicate with. They could have obtained this information in variety of ways such
233   as explicit configuration, DHCP, DNS, and explicit Probe for DP etc. Figure 10 below shows the scenario
234   and the sequence of events.

Figure 10: Discovery Proxy as an enterprise service registry.

Following is the description of the scenario and interaction between the actors involved in the scenario.

1. A Target Service 1 - Printing comes online and sends a unicast Hello to the Discovery Proxy. The Discovery Proxy stores information about TS-1 in its cache / registry.

2. A Target Service 2 - Imaging comes online and sends a unicast Hello to the Discovery Proxy. The Discovery Proxy stores information about TS-2 in its cache / registry.

3. A Client – Laptop1 looking for Imaging services sends a unicast Probe to the Discovery Proxy.

4. The Discovery Proxy responds with Probe Match containing information about TS-2.

247 References

248   [**WS-Discovery**] Web Services Dynamic Discovery (WS-Discovery), April 2005

249   http://schemas.xmlsoap.org/ws/2005/04/discovery