International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.772

(11/2015)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

IPTV multimedia services and applications for IPTV – IPTV service discovery up to consumption

IPTV terminal device discovery

Recommendation ITU-T H.772

International Telecommunication Union

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence	H.420–H.429
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	**H.770–H.779**
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Personal health systems	H.810–H.819
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.772

IPTV terminal device discovery

Summary

Recommendation ITU-T H.772 describes mechanisms for Internet protocol television (IPTV) terminal device (TD) discovery that make IPTV terminal devices discoverable and selectable to one another within a public or local network environment. For example, terminal device discovery is useful for services that allow users to share content with other terminal devices. This Recommendation also describes the connection model and functional architecture for IPTV terminal device functional blocks to support the IPTV terminal device discovery mechanism. Moreover, the procedures of IPTV terminal device discovery are given in this Recommendation. In addition, the reference point, the related protocols, elements and attributes to be used in the communication messages are also specified in this Recommendation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.772	2015-11-29	16	11.1002/1000/12650

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T H.772

IPTV terminal device discovery

1 Scope

This Recommendation describes the mechanisms for Internet protocol television (IPTV) terminal device (TD) discovery. These mechanisms enable IPTV terminal devices to provide end-users with effective ways to discover and select terminal devices.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.721] Recommendation ITU-T H.721 (2015), *IPTV terminal devices: Basic model*.

[ITU-T H.722] Recommendation ITU-T H.722 (2014), *IPTV terminal device: Full-fledged model*.

[ITU-T H.770] Recommendation ITU-T H.770 (2015), *Mechanisms for service discovery and selection for IPTV services*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 acquisition [b-ITU-T Y.1901]: The process of obtaining content by the end-user.

NOTE – For content with accessibility features, this means that the content will be available in a form that can be used by the end-user.

3.1.2 application [b-ITU-T Y.1901]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.3 end user [b-ITU-T Y.1910]: The actual user of the products or services.

NOTE – The end-user consumes the product or service. An end-user can optionally be a subscriber.

3.1.4 functional architecture [b-ITU-T Y.2012]: A set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

NOTE 1 – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementations and between administrative domains.

NOTE 2 – This definition is taken from [b-ITU-T Y.2012] and therefore relates to NGN. However, it is also valid for other networks, e.g., networks supporting IPTV terminal device.

3.1.5 home network (HN) [b-ITU-T H.622]: Home network is the collection of elements that process, manage, transport, and store information, thus enabling the connection and integration of multiple computing, control, monitoring, communication and entertainment devices in the home.

3.1.6 Internet protocol television (IPTV) [b-ITU-T Y.1901]: Multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability.

3.1.7 IPTV TD [b-ITU-T Y.1901]: A terminal device which has ITF functionality, e.g., a STB.

3.1.8 IPTV terminal function (ITF) [b-ITU-T Y.1901]: The end-user function(s) associated with a) receiving and responding to network control channel messages regarding session set-up, maintenance, and teardown, and b) receiving the content of an IP transport from the network and rendering.

3.19 service discovery (SD) [ITU-T H.770]: The mechanisms for service provider discovery, service discovery and selection for IPTV services. The mechanisms enable IPTV terminal devices to provide the end-users with effective ways for consuming IPTV services.

3.1.10 service provider [b-ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider can optionally operate a network. A service provider can optionally be a customer of another service provider.

NOTE – Typically, the service provider acquires or licenses content from content providers and packages this into a service that is consumed by the end-user.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 multiple device service: The mechanisms for a multi-device service, which includes the entire system architecture, core functional requirement of multi-device enabled systems, technologies that support the multi-device service, service prospects, system API and interface.

3.2.2 terminal device discovery: A procedure that allows IPTV terminal devices to discover other IPTV terminal devices and their capabilities, as required for the provisioning of convergent, multi-device IPTV services.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
DNS	Domain Name System
HN	Home Network
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IPTV	Internet Protocol Television
MDS	Multi-Device Service
RP	Reference Point
SD	Service Discovery
SP	Service Provider
STB	Set-Top Box
TD	Terminal Device
TDD	Terminal Device Discovery

UI	User Interface
URL	Uniform Resource Locator
XML	extensible Mark-up Language

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction

With the proliferation of digital content and the expanding variety of connected and IP-enabled Internet protocol television (IPTV) terminal devices (TDs) such as the basic model [ITU-T H.721], full-fledged model [ITU-T H.722] and mobile model [b-ITU-T H.IPTV-TDES.4], consumers can access and share IPTV services seamlessly inside or outside their home network (HN).

For the purpose of IPTV services sharing between IPTV TDs, after finishing the service provider (SP) service discovery (SD) procedure, as is defined in [ITU-T H.770], an IPTV TD will initiate the terminal device discovery (TDD) procedure to connect with other IPTV TDs for the convergent IPTV services. Several steps towards terminal device discovery and device capability acquisition are included, as illustrated in Figure 6-1.

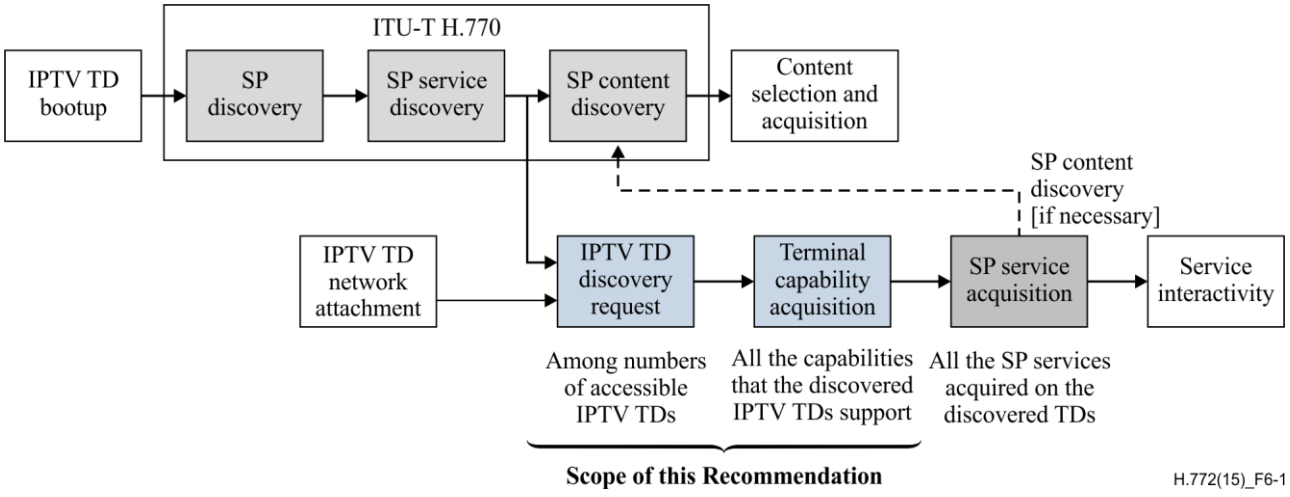

Figure 6-1 – Scope of this Recommendation and the TDD procedure in general

NOTE:

– IPTV TD discovery request: request for discovering all available IPTV TDs; information on the discovered TDs would be listed in this step.

– Terminal capability acquisition: acquisition on the capability of the discovered IPTV TDs, including hardware, software and services supported.

– Terminal device discovery can optionally start from SP discovery by using its defined SP discovery records. For more information on SP discovery, SP service discovery and SP content discovery please refer to [ITU-T H.770]. Appendix I provides an example of retrieving the entrance address for registration-based terminal device discovery (see clause 8.1) by means of service discovery record defined in [ITU-T H.770]. Appendix II provides an example of registration server backup issues. Additional use cases where terminal device discovery is useful can be found in [b-ITU-T HSTP.IPTV-SMTD].

6.1 Overview of terminal device discovery

The target of terminal device discovery is to list the available terminal devices so as to be aware of an interested terminal device. But considering the different device connection model, the terminal device discovery mechanism is different as well.

A discovery request message is recommended to be used to initiate the terminal device discovery procedure. According to different cases, the information involved in the response message may be different. The following clause provides a brief description.

6.1.1 Terminal device discovery in indirect connection mode

In the indirect connection mode, an intermediate entity connects both terminal devices. The intermediate entity can be one of various types. For example, it could be a home gateway, or a remote service platform or just a hub. In a discovery stage, the discovery request message will be transferred through the intermediate device. According to the different working modes, the intermediate device could work as a simple message transfer, or it could manage each possible message route for all terminals.

Figure 6-2 summarizes the steps for terminal device discovery in indirect connection mode.

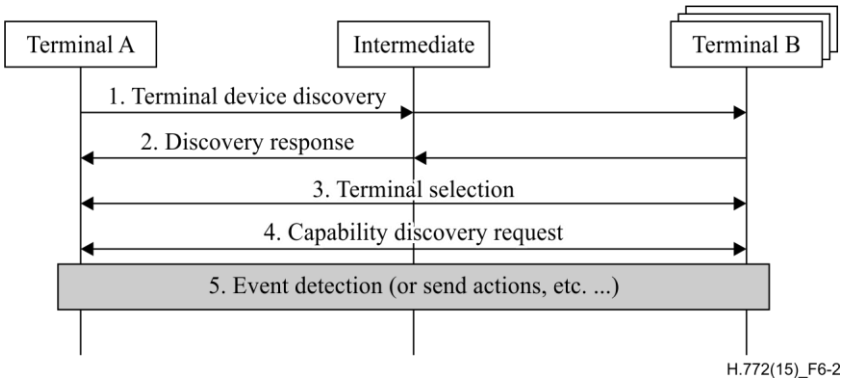

Figure 6-2 – Terminal device discovery for indirect connection mode

1. Terminal A (source) sends out a discovery request message to an intermediate device by broadcast/multicast/unicast mechanism. The intermediate device forwards that message to any possible Terminal B (targets).
2. Terminal B receives the discovery request message and sends back a response message with its identifier through the intermediate device. Otherwise, the discovery request message will be dropped by Terminal B.

3. According to the response message, Terminal A is able to select one or more Terminal B(s) and to initiate a communication request. Then, a communication channel will be established.
4. A capability discovery request message is exchanged between/among all interconnected terminals.
5. After terminal device discovery is completed, the specific application, such as a multi-device application, could be implemented by monitoring events, actions, etc.

6.1.2 Terminal device discovery in direct connection mode

In the direct connection mode, the messages are only transferred between two terminals. The procedure for terminal device discovery is simple. Client-server mode is commonly used; usually this is conducted by non-IP connection means such as infrared or Bluetooth.

Figure 6-3 describes the overview steps of terminal device discovery in direct connection mode.

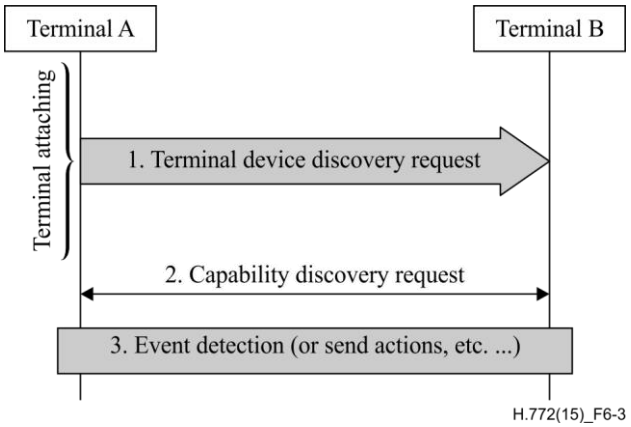

Figure 6-3 – Terminal device discovery for direct connection mode

1. The terminal device discovery request procedure is completed with terminal attaching. Both terminals can be aware of their identifier information (e.g., device name, device ID) within the terminal attaching procedure.
2. A capability discovery request message is exchanged between the two terminal devices.
3. After terminal device discovery is completed, the specific application, such as a multi-device application, could be implemented by monitoring events, actions, etc.

7 Functional architecture of terminal device discovery

Two mechanisms are introduced here: registration-based solution and broadcast-based solution. In IPTV terminal functions, these two mechanisms may have the different requirements for the terminal device discovery functions. In this Recommendation, the discovery agent refers to an IPTV terminal device with an embedded discovery client application. For example, an agent could be regarded as one of the function components of multiple device service (MDS) enabler functions [b-ITU-T H.IPTV-MDS]. The discovery server refers to an IPTV terminal device or an IPTV server platform with an embedded a discovery server application. Both the discovery agent and server should provide the necessary functions to support the terminal device discovery procedure.

Figure 7-1 presents the functional architecture of the discovery agent and server within the common application functions.

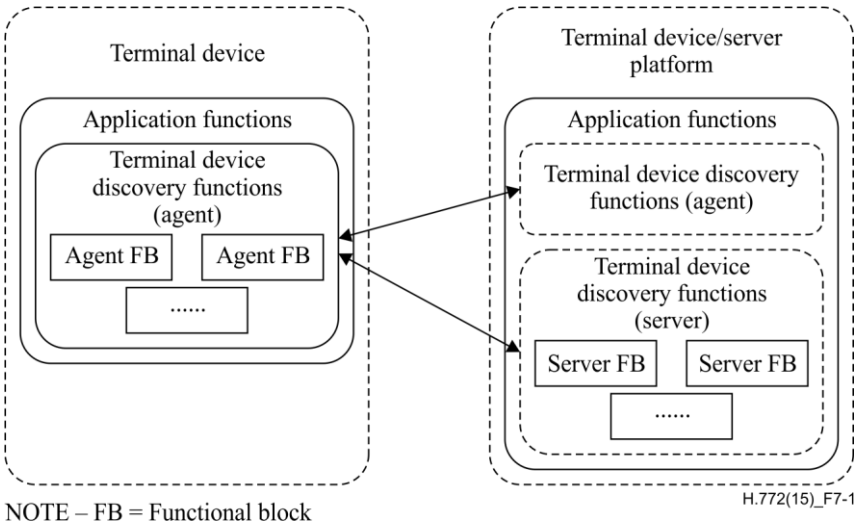

Figure 7-1 – Functional architecture of discovery agent and server

In the public network environment, the client-server model is recommended to be used with the registration-based solution. The discovery server works as an information centre. All terminals should connect to the server for acquiring other terminal information.

In a local network environment, especially in a peer-to-peer network, the discovery may happen directly between terminal devices with a broadcast-based solution. The terminal's information could be shared among all the terminal devices or among special grouped terminals within a local network.

It is noted that, in some powerful terminal devices, e.g., [ITU-T H.722], it might be possible to install both agent and server applications for supporting two functional roles.

Therefore, the functional requirements for the discovery agent and server can be summarized in the following contexts.

7.1 Agent functional block

The agent functional block shall be able to:

– support multicast/unicast based transport protocols;

– register/announce its identification information to other agents/server;

– able to detect the registration/announcement information from other agents;

– translate/encapsulate the registration/announcement information to another format as a proxy for the connected terminal devices;

– collect terminal information from its own terminal device;

– access or allow access to the discovered terminal device for its capability information or service information.

7.2 Server functional block

The server functional block shall be able to:

– detect and receive the registration/announcement information from the connected agents;

– (temporarily) store or maintain terminal device information, including capability information or service information;

– authenticate or transmit an authentication request for terminal devices;

– provide a response for the agent discovery request, and provide a categorized result according to the given search criteria, e.g., the terminal belongs to the same user ID or a group ID;
– forward a discovery request from one terminal device to the other terminal devices by working as a proxy;
– request terminal device information from a third party platform which already has terminal device information stored in it.

8 Terminal device discovery process

Two mechanisms are introduced here: registration-based terminal device discovery and broadcast-based terminal device discovery. Each related step in these two mechanisms is specified correspondingly with the context of procedure description.

8.1 Registration-based terminal device discovery process

In an open network, e.g., the Internet, terminal devices may be allocated in many different networks. In this case, broadcast-based discovery may not be an appropriate solution.

By using a registration-based terminal device discovery mechanism, a registration server and registration agent(s) are required. See Figure 8-1. The registration server is used to receive the register message that is sent from an agent in a certain network. The register message is used to register the information about the agent or a terminal device in the same network while the agent is working as a proxy.

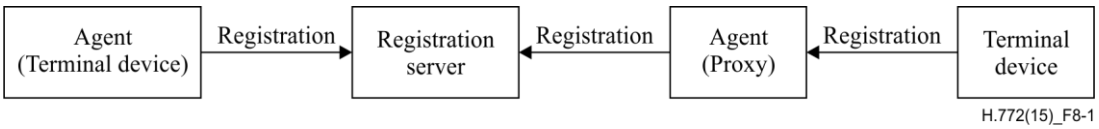

Figure 8-1 - Overview of registration-based terminal device discovery

The registration server is also used to store and maintain the registered information. According to that information, terminal devices may be categorized according to a predefined index keyword(s) or parameters. Therefore, one device in a certain network could share its media resource with a terminal device in another network by using a media sharing message or other similar mechanisms.

For security purposes, the registration server is recommended to verify the authentication of an agent or terminal devices after the registration message is received. If valid, the registration process can be continued and completed.

Figure 8-2 shows the scenario of registration-based terminal device discovery.

In this scenario, Agent A (Terminal device) and Agent B (Proxy) can both use a certain capability X (e.g., Media X is any media that can be consumed on a device such as a video, image, or audio). Each agent registers itself with a Registration server. The Registration server manages the list of agents that can use capability X. Under Agent B (Proxy), multiple devices may exist.

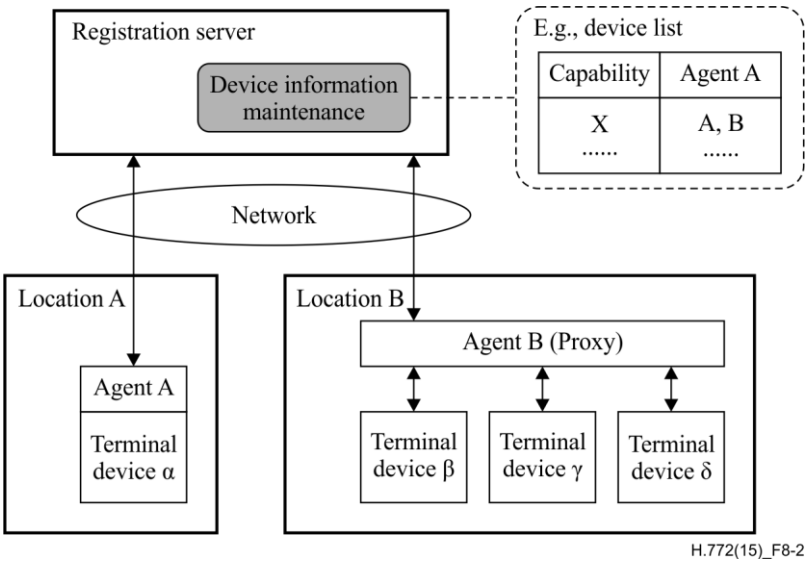

Figure 8-2 – Registration-based scenario of terminal device discovery

8.1.1 Terminal device registration

Figure 8-3 shows the steps in the terminal device registration stage.

The agent sends a registration message to the registration server (Server). In some cases, the registration message may only be sent once. Subsequently, terminal devices only need to send an authentication request instead of the registration message. In other cases, the registration and authentication steps could be combined into one step when a terminal device is first registered to a server.

Figure 8-3 shows the steps in the terminal device registration stage.

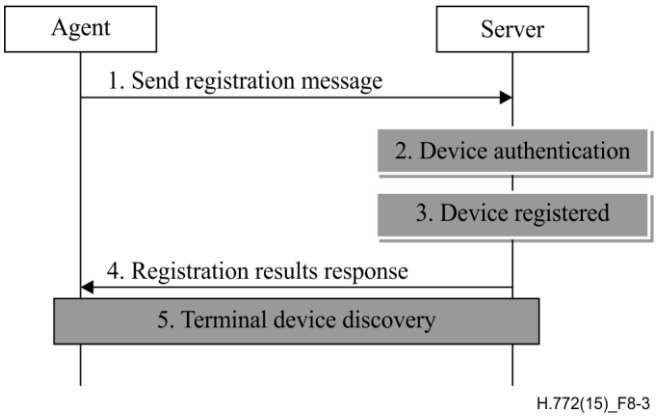

Figure 8-3 – Agent registration

1. The agent sends a registration message to the registration server (Server). Different agents may send messages at asynchronous times. It is noted that the registration process could be auto-start or manually start.
2. After receiving this message, the registration server will first verify the device authentication information.

   NOTE – The authentication step can be optionally implemented in this procedure. It is dependent on the actual implementations. The authentication procedure can be found in clause 8.1.2.
3. If the device authentication is valid, the device information is registered and stored. In this step, the device information could also be categorized by a certain index, such as, user ID, network ID, etc.

4. The registration result will return to the source device for future usage.
5. The device may initiate terminal device discovery immediately or later.

8.1.2 Terminal device authentication

Figure 8-4 shows the steps in the terminal device authentication stage.

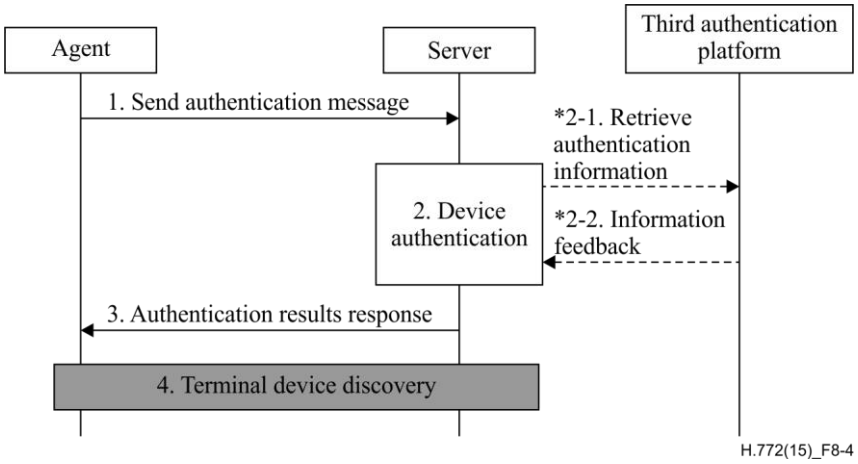

Figure 8-4 – Agent authentication

1. The agent sends an authentication message to the registration server. Different agents may send message in asynchronous time. It is noted that the authentication could be auto-start or manually start.
2. After receiving this message, the registration server will verify the device authentication. If a third authentication platform is used, the registration server may need to communicate with it to retrieve authentication information for future processing.

   *NOTE – Steps 2-1 and 2-2 are optional steps if the registration server does not have the authentication function or it does not have a stable authentication information database.
3. If the device authentication is valid, the authentication results will return to the source device.
4. The device may initiate terminal device discovery immediately or later.

8.1.3 Terminal device discovery

Figure 8-5 shows the steps in the terminal device discovery stage.

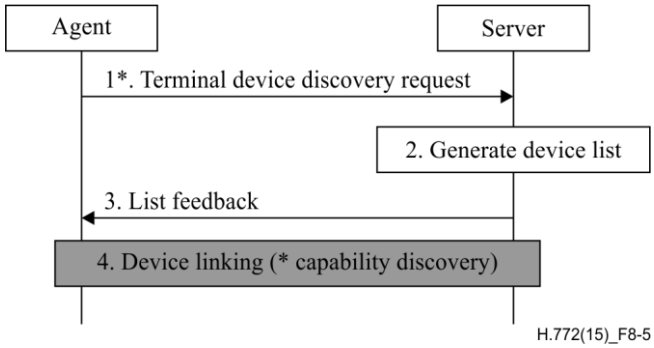

Figure 8-5 – Registration-based procedure of terminal device discovery

1. If the agent wants to be aware of the availability of other agents, it could send a terminal device discovery request message to the registration server.

NOTE 1 – If the agent has already received the device list form the registration steps (see clause 8.1.1), it could omit the following step and initiate device linking or capability discovery directly.

2. After receiving the request, the registration server will generate a registered device list. All devices in this list should be categorized by a certain index. For example, those terminal devices which belong to the same user ID are able to be grouped in the list.

   NOTE 2 – During this step, the server could alternatively check all registered terminal devices' status and make sure all statuses are updated.

3. The list will be sent back with a discovery result, such as the device list with its present status.

4. With the list, the source device could select the appropriate device and try to link with it.

   NOTE 3 – If the source device could not extract a device capability form the device list, it needs to implement capability discovery after linking with the target device.

8.1.4 Terminal device status update

In most cases, the terminal device or agent should report its status periodically. With these reports, the registration server could update all devices' status in the list.

Figure 8-6 shows the steps in the terminal device status update stage.

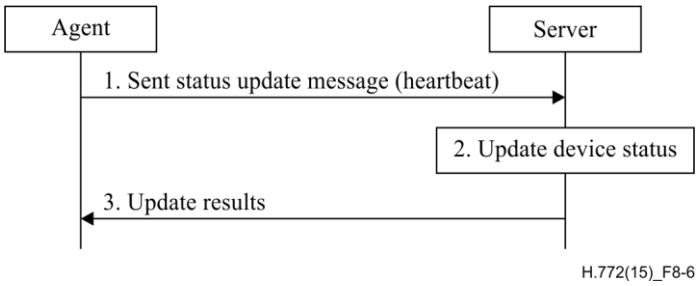

Figure 8-6 – Terminal status update

1. The agent sends a status update (heartbeat) message periodically to the registration server (Server). If the agent works as a proxy, then it receives status update messages from each connected terminal device forwards them to the registration server.

2. The registration server updates its device status according to the received status update messages.

3. The registration server sends back an update result to the agent. If the agent fails to receive that result or the result is not valid, it may launch the registration or authentication process again.

8.2 Broadcast-based terminal device discovery process

In a local network, e.g., a home network, each terminal device may allocate a different address but they will all have the same network domain. In this case, a broadcast mechanism is more efficient than other message transfer mechanisms. See Figure 8-7.

A broadcast message will be sent by a source device and be received by any interested terminal device. One of these terminal devices may send back a response message for future contacting. Authentication may be implemented in the source device after the response message is received.

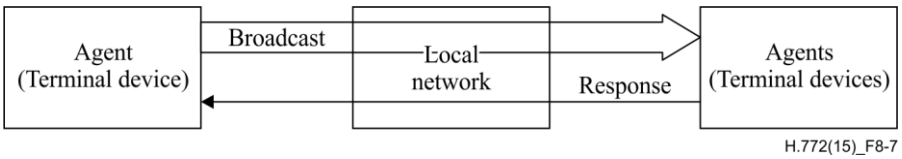

Figure 8-7 – Overview of broadcast-based terminal device discovery

After completing device discovery, the authentication device information list may be cached on each terminal. Once a terminal device changes its status or is offline, it needs to start discovery again for updating the device list.

Figure 8-8 shows the scenario of broadcast-based terminal device discovery.

Agent A (Terminal device) sends a broadcast/multicast message with the terminal device discovery request within a local network. Agents from terminal devices B to F that are interested in this message will reply to its request. Terminal devices hold the list of terminal device information.

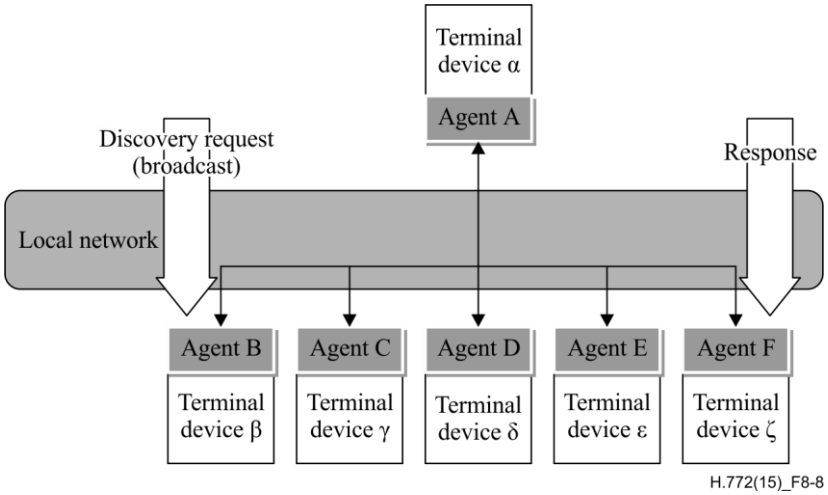

Figure 8-8 – Broadcast-based scenario of terminal device discovery

8.2.1 Terminal device announcement

Figure 8-9 shows the steps in the terminal device announcement stage.

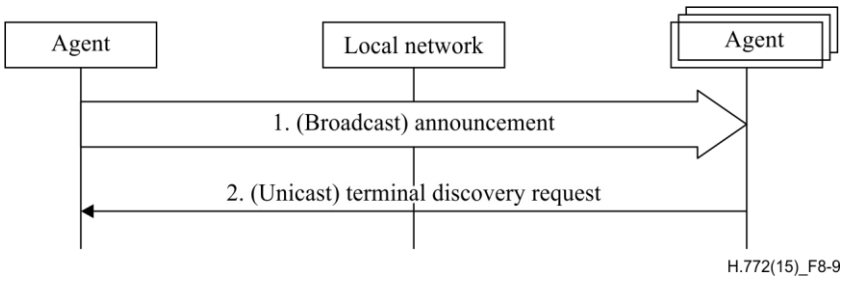

Figure 8-9 – Broadcast-based procedure of terminal announcement

1. When a new agent is added into a local network, it is recommended to send an announcement message by a broadcasting/multicasting mechanism. The information of announcement message can be found in Table 9-2.
2. If one agent is interested in that agent announcement message, it could send a unicast terminal device discovery request to that particular agent.

   NOTE – If the agent is not interested in the announcement message, it does not need to respond the message.

8.2.2 Terminal device discovery request

Figure 8-10 shows the steps in the terminal device discovery stage.

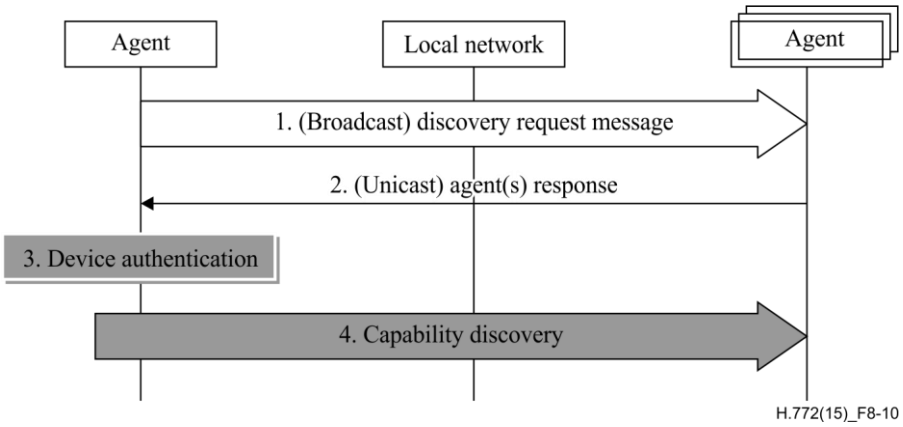

Figure 8-10 – Broadcast-based procedure of terminal device discovery

1. If an agent does not have a particular target agent to be connected, it could send out a terminal device discovery request message by a broadcasting mechanism in the local network and every available agent in this network will receive that message.
2. If an agent wants to respond, it will send back a response message directly to the source agent according to the information in the discovery request message.
3. When the source agent receives the response, device authentication may be implemented for security purposes. It is noted that authentication also could be implemented within later steps. Device authentication is based on a preconfigured policy, e.g., a white list, password control, IP or media access control (MAC) address filter.
4. With the information in response, the source agent sends a capability discovery message to those responded agents.

8.3 Capability discovery

Once the authenticated agent has received the target agent's essential information, such as target IP address or a capability description uniform resource locator (URL), it could initiate a capability discovery procedure. The device information and its supported services lists should be collected into a description file, which can be accessed by other terminals. However, different discovery mechanisms and capability exchanges can be implemented in certain situations:

– normally, for registration-based terminal device discovery and broadcast-based terminal device discovery, if the terminal device is authenticated, the capability discovery procedure should be initiated consequently;

– for both mechanisms, if the agent receives the target agent status update notification, such as new device join, device reboot, etc., it is recommended to implement capability discovery again for updating.

Figure 8-11 shows the steps of terminal devices capabilities discovery.

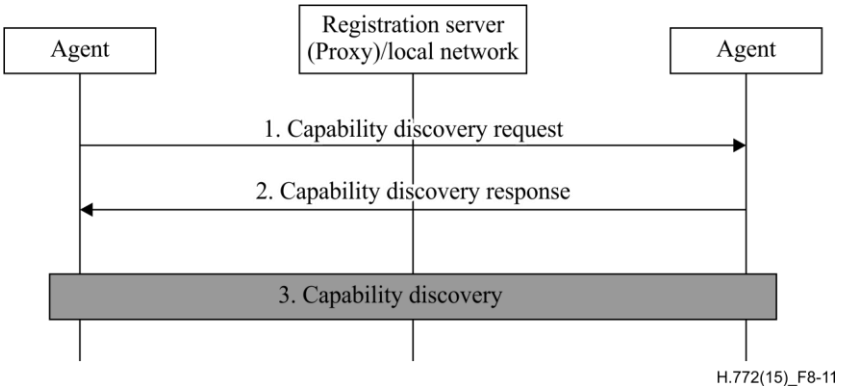

Figure 8-11 – Capabilities discovery

1. An agent sends a capability discovery request to a particular agent. In registration-based discovery mode, the request message may be transmitted by the registration server, which works only as a proxy.
2. The target agent will send back a capability file with the attributes in a certain data structure, e.g., an extensible mark-up language (XML) schema. These attributes will be carried by capability discovery response.
3. The agent retrieves the detailed service information from the capability description attributes (the structure and contents of service information is out of scope of this Recommendation).

When an agent registers its device information on a registration server, it may also register its capability information directly on that server accompanied with the registration request, instead of a capability description URL. During the capability discovery stage, if one agent is not able to access the other agent temporarily (e.g., the capability description URL is not available), it could send a capability discovery request to the registration server alternatively if that information is maintained on the registration server synchronously.

Figure 8-12 shows the capability discovery in the above scenario.

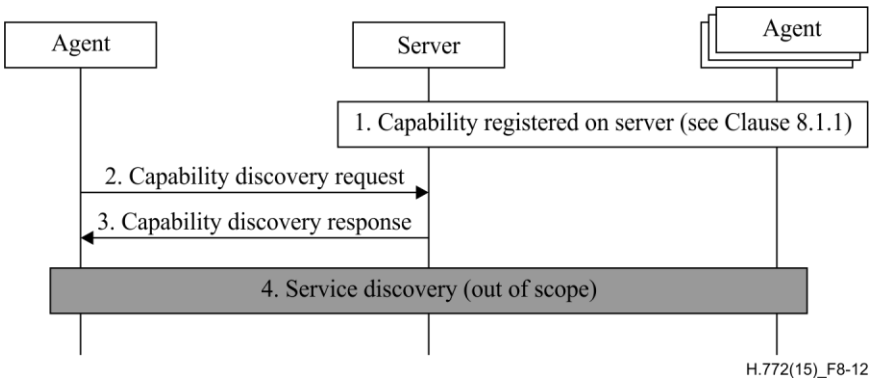

Figure 8-12 – Capabilities discovery on server

1. In the agent registration process, an agent may register its capability information simultaneously with its terminal device information registration.
2. In some cases, if one agent is not able to access its target agent temporarily, it may send a capability discovery to the registration server optionally.
3. If the target agent's capability information is maintained on the server, the registration server could send back the information by capability discovery response message.
4. The agent discovers the detailed service information from the capability description attributes (structure and the contents of service information is out of scope).

It is noted that the server-based capability discovery may optionally be implemented in terminal device discovery stage, if an agent only wants to list some terminal information with a specific terminal capability and the registration server is required to keep capability information maintaining on its database.

Each capability discovery request may contain multiple capability filters. These capability filters are recommended to be connected by one or more logical operators such as "AND", "OR", "NOT", etc. For example, *Capability filter = "capability 1" AND ("capability 2" OR "capability 3")*.

A discovery result such as a relevant device information list should be returned. Each device on that list must be matched on the condition provided by a capability filter.

9 Reference point and protocols

In general, the device discovery protocol allows a new added terminal device to initiate a discovery message by broadcast/multicast/unicast mechanism. Other devices listen to the message and send a response message. They can then exchange the device information description message and communicate with each other.

9.1 Reference points

Figure 9-1 presents the reference points (RPs) between the discovery server and the discovery agents.

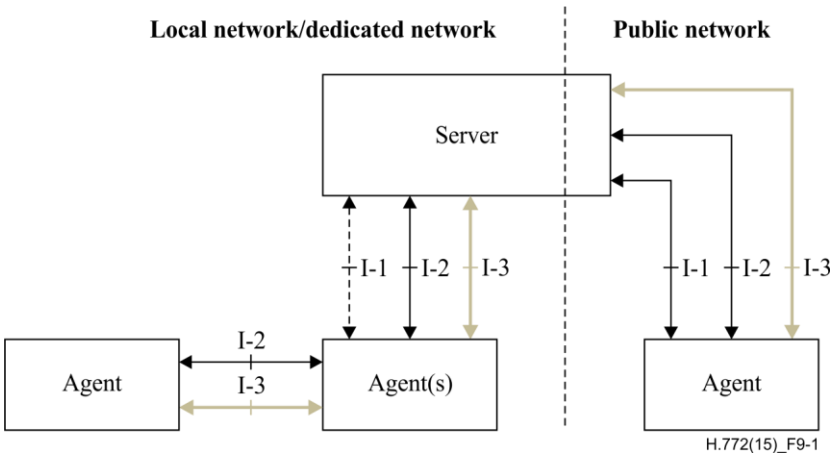

Figure 9-1 – Relevant reference points for terminal device discovery

It is recommended to implement the three reference points I-1, I-2 and I-3, which can be categorized as follows:

– **Reference point I-1:** registration and status report

This RP is used to transmit a registration message and report terminal status.

Depending on the different terminal device discovery models, this RP will have different uses:

- Registration-based mode: this RP is necessary for sending a registration message and status report to the registration server.
- Broadcast-based mode: this RP may not necessarily be used because the server will be aware of all terminal devices by the broadcast or multicast discovery messages. It is noted that, if the broadcast-based mode is used, a status report message could be combined with a discovery message and sent by RP I-2.

– **Reference point I-2:** terminal authentication and discovery

This RP is used to request authentication or security for a terminal device. Once the authentication is valid, this RP is also used to send discovery messages.

There are, however, two special situations:

- If all terminal devices (Agent) are located in a local network or a dedicated network, such as IPTV network, which is also a public network, this RP may not be used for service authentication because authentication will be completed when the terminal device is logging on to a dedicated system.
- If a terminal device is located in an open public network, such as Internet, and it wants to discover a terminal in a dedicated network, this RP is necessary and a service authentication message should be sent from this RP for further security check.

It is noted that RP I-2 is also to be used when all terminal devices are located in the public network.

Also, depending on the different working models, the discovery mechanism may use different protocols:

- If broadcast-based mode is used, such as a local network connection, it is recommended to use a broadcast or multicast mechanism to send discovery messages or announcements. A predefined multicast address and port should be given.
- If registration-based mode is used, such as IPTV network or Internet, it is recommended to use a unicast mechanism to send discovery messages. A unicast address and port should be defined.

– **Reference point I-3:** message exchange

The service related message includes service discovery information, transaction message, or other application-level messages. The detailed information is out scope of this Recommendation. Examples will be found in [b-ITU-T H.IPTV-MDS].

9.2 Protocols

According to the different discovery mechanisms, the protocols may be different for carrying discovery related messages.

9.2.1 Protocols used by registration-based service discovery

The following table gives the potential protocols that could be used on the reference points.

Table 9-1 – Protocols on RP used by registration-based mode

RP	Message type	Direction	Protocols	Description
I-1	Registration request	Agent → Server	UDP/ Unicast	A terminal device sends a registration message to a registration server.
	Registration response	Server → Agent	UDP	The server sends back a result of registration status.
	Status report	Agent → Server	UDP	A terminal device sends status message to a registration server.
	Update response	Server → Agent	UDP	The server sends back a result for confirming device status.

Table 9-1 – Protocols on RP used by registration-based mode

RP	Message type	Direction	Protocols	Description
I-2	Authentication request	Agent → Server	HTTP/ HTTPS	A terminal device sends a service authentication message to a server. Some security mechanism is recommended to be used, such as passkey, etc.
	Authentication Response	Server → Agent	HTTP/ HTTPS	The server sends back the service authentication result. It is noted that, some other information could be also sent back with a response message, e.g., a device list.
	Discovery request	Agent → Server	HTTP	A terminal device sends a message for discovering the other devices.
	Discovery response	Server → Agent	HTTP	The server sends back a device list.
	Capability discovery request	Agent →Server →Agent or Agent →Server	HTTP	One terminal sends a capability discover request message to a target terminal or registration server. The message may be transmitted by a registration server (as a proxy).
	Capability discovery response	Agent →Server →Agent or Server →Agent	HTTP	The target or registration server returns the capability description within response. The capability description may be a URL for accessing capability elements or the actual elements as a certain data structure. The message may be transmitted by registration server (as a proxy).

9.2.2 Protocols used by broadcast-based service discovery

The following table gives the potential protocols that could be used on the reference points.

Table 9-2 – Protocols on RP used by broadcast-based mode

RP	Message type	Direction	Protocols	Description
I-2	Discovery request	Agent → Agent(s)	UDP/Multicast	A terminal device sends a message for discovering the other devices.
	Discovery request (Note)	Agent → Agent	UDP/unicast	A terminal device sends a message specially to a known address terminal for quickly checking status.
	Discovery response	Agent → Agent	UDP/Unicast	The interested device sends back the device information.
	Announce (Status report)	Agent → Agent(s)	UDP/Multicast	A terminal device sends a status report to notify all the potential agents of its current status.
	Capability discovery	Agent →Agent	HTTP	One terminal device sends a capability discover request message

Table 9-2 – Protocols on RP used by broadcast-based mode

RP	Message type	Direction	Protocols	Description
	request			to a target terminal device.
	Capability discovery response	Agent →Agent	HTTP	The target agent returns the capability description within response.
NOTE – Unicast discovery request is optionally used for quick terminal status checking.				

10 Discovery information

This clause specifies the attributes and elements that carry the terminal device information. The information is exchanged in the terminal device discovery procedure (see clause 8) by using the recommended protocols (see clause 9). With this information, terminal devices in the network will be discoverable and selectable.

10.1 Attributes/elements used in registration-based terminal device discovery request

It is recommended that the information in Tables 10-1 through 10-7 be used in the registration-based terminal device discovery mechanism.

Table 10-1 – Attributes/elements for registration request

Attributes	Description	M/O/C	Cardi-nality	Type	Length (byte)	Example
User ID	A unique identifier which indicates who the device belongs to	C	1	String	40	00000x1
Group ID	A unique identifier which indicates which group the device belongs to	C	1-n	String	40	g0001
Device ID	A unique identifier to indicate a certain device, the Device ID construction should be based on a known standard	M	1	String	50	001011000003
Transaction ID	A unique identifier for a certain terminal register request	M	1	String	40	00000x56
Device type	A symbol which indicates what the terminal device type is	O	0-n	Integer	4	0:H.721, 1:H.722, 3:b_TDES.4
Device name	A special name for the terminal device	O	0-n	String	50	"my STB"
Timestamp	A timestamp which marks the time when the request is sent	M	1	String	14	YYYYMMDD HHMMSS "20120302081500"

Table 10-1 – Attributes/elements for registration request

Attributes	Description	M/O /C	Cardi-nality	Type	Length (byte)	Example
Device roles	Predefined roles which indicate the capability of the terminal device	O	0-n	String	40	Media server, controller [b-ITU-T H.IPTV-TDES.5]
Supported protocols	The possible supported communication protocols for future service usage	O	0-n	String	40	HTTP, TCP
Capability description URL	A URL that allows other terminal devices to access this device for retrieving capability or service description	M	1	String	256	http://<device ip>:<port>/description.xml or null
Login IP	The IP address of the server where the terminal device logs in	C	1	String	40	198.51.100.100
Agent IP address (private)	The IP address allocated by a local network	C	1	String	40	192.168.1.100
Agent IP address (public)	The IP address allocated by a public network	C	1	String	40	203.0.113.11
NOTE 1 – User ID is used when authentication is covered by a registration procedure. NOTE 2 – Group ID is used if the terminal device is previously grouped with other terminal devices. NOTE 3 – Login IP, Agent IP (public and private) are all mandatory if they have different values. Otherwise, one of them is mandatory at least.						

Table 10-2 – Attributes/elements for registration response

Attributes	Description	M/O /C	Cardi nality	type	Length (byte)	Example
Transaction ID	A unique identifier for a certain terminal register response	M	1	String	40	00000x57
Result	A symbol which indicates the registration result	M	1	String	8	0:success, 1:fail, 2:redirect
Redirect address	The IP address of the actual serving server. If the registration request is redirected to another server, this attribute is returned.	C	1	String	40	198.51.100.100

Table 10-2 – Attributes/elements for registration response

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Heart timer	The frequency for responding status report. If their server does not receive status report in a given heart timer, the terminal may be regarded as "not available". It's configurable.	C	1	Integer	2	5
Result description	A text description to explain the discovery result	O	0-n	String	256	"Server busy", "Time out"
NOTE 1 – Redirect address is mandatory used in case there is more than one registration server. NOTE 2 – Heart timer is mandatory, used when the device keep-alive mechanism is applied during the whole terminal device discovery procedure.						

Table 10-3 – Attributes/elements for status update request

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Transaction ID	A unique identifier for a certain terminal update request	M	1	String	40	00000x58
Device ID	A unique identifier to indicate a certain device	M	1	String	50	001011000003
Timestamp	A timestamp which marks the time when the request is sent.	M	1	String	14	YYYYMMDDHHMMSS "20120302081503"
Operation	A flag which indicates the status that a terminal device wants to report	M	1	Integer	4	0: not available 1: alive 2:byebye

Table 10-4 – Attributes/elements for status update response

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Transaction ID	A unique identifier for a certain terminal update response	M	1	String	40	00000x59
Result	A symbol which indicates the discovery result	M	1	String	8	0:success, 1:fail, 2:re-register
Result description	A text description to explain the discovery result	O	0-n	String	256	"status updated!", "status update failed"

Table 10-5 – Attributes/elements for authentication/terminal device discovery request

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Transaction ID	A unique identifier for a certain terminal device discovery request	M	1	String	40	00000x58
User ID	A unique identifier which indicates who the device belongs to	C	1	String	40	00000x1
Device ID	A unique identifier to indicate a certain device	M	1	String	50	001011000003
Timestamp	A timestamp which marks the time when the request is sent	M	1	String	14	YYYYMMDDHHMMSS "20120302081503"
Operation	A flag which indicates what the terminal device wants to do	M	1	Integer	4	0: authentication 1: discover terminal devices
Capability filter	A predefined condition which is used to filter the response as an expected result Logical operators (OR, AND, NOT) are recommended to be used for including multiple capabilities in the filter.	O	0-1	String	256	"media server", "media player", "all available capabilities" "media server" OR "media player"; "media server" AND "media player"
NOTE – User ID must be provided if the operation is 0 (authentication).						

Table 10-6 – Attributes/elements for authentication/terminal device discovery response

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Transaction ID	A unique identifier for a certain terminal device discovery response	M	1	String	40	00000x59
Result	A symbol which indicates the discovery result	M	1	String	8	0:success, 1:fail
Result description	A text description to explain the discovery result	O	0-n	String	256	"authentication success", "discovery result OK"
Device information list	A list which collects all terminal information about the available terminal device	C	1	Container	variable length	See Table 10-9 or Null
NOTE – Device information list is mandatory when that message is a discovery response message.						

Table 10-7 – Attributes/elements for capability discovery request

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Transaction ID	A unique identifier for a certain capability discovery request	M	1	String	40	00000x58
User ID	A unique identifier which indicates who the device belongs to	C	1	String	40	00000x1
Device ID	A unique identifier to indicate a certain device	M	1	String	50	001011000003
Timestamp	A timestamp which marks the time when the request is sent	M	1	String	14	YYYYMMDDHHMMSS "20120302081503"
Operation	A flag which indicates what the terminal device wants to do	M	1	Integer	4	0: filter-based capability discovery 1: target-based capability discovery
Target IP address	A specific IP address that the agent wants to access	C	1	String	40	198.51.100.100
Capability filter	A predefined condition which used to filter the response as an expected result Logical operators (OR, AND, NOT) are recommended to be used for including multiple capabilities in the filter.	C	0-1	String	256	"media server", "media player", "all available capabilities" "media server" OR "media player"; "media server" AND "media player"
NOTE 1 – User ID is used for where authentication is combined with capability discovery. NOTE 2 – Target IP and Capability filter is only used depending on the capability discovery operation.						

Table 10-8 – Attributes/elements for capability discovery response

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Transaction ID	A unique identifier for a certain capability discovery response	M	1	String	40	00000x59
Result	A symbol which indicates the discovery result	M	1	String	8	0:success, 1:fail
Result description	A text description to explain the discovery result	O	0-n	String	256	"Discovery result OK", "no target found!"
Capability information list	A list which collects all capability information about the available terminal device	M	1	Container	variable length	See Tables 10-13, 10-14, 10-15 or Null

Table 10-8 – Attributes/elements for capability discovery response

Attributes	Description	M/O /C	Cardinality	type	Length (byte)	Example
Device information list	A list which collects all terminal information about the available terminal device	C	1	Container	variable length	See Table 10-9 or Null
NOTE – Device information list is returned only when the capability discovery request is filter based.						

Table 10-9 – Attributes/elements for device information

Attributes	Description	M/O /C	Cardinality	type	Length (byte)	Example
User ID	A unique identifier which indicates who the device belongs to	C	1	String	40	00000x1
Group ID	A unique identifier which indicates which group the device belongs to	C	1-n	String	40	g0001 or null
Device ID	A unique identifier to indicate a certain device	M	1	String	50	001011000003
Device name	A special name for the terminal device	O	0-n	String	50	"my STB"
Device type	A symbol which indicates what the terminal device type is	O	0-n	Integer	4	0:H.721, 1:H.722, 3:b_TDES.4
Device roles	Predefined roles which indicate that the capability of the terminal device	O	0-n	String	40	Media server, controller [b-ITU-T H.IPTV-TDES.5]
Capability description URL	A URL that allows other terminal devices to access this device for retrieving capability or service description	M	1	String	256	http://<device ip>:<port>/description.xml or null
Supported protocols	The possible supported communication protocols for future service usage	O	0-n	String	40	HTTP, TCP
Login IP	The IP address of the server where the terminal device logs in	C	1	String	40	198.51.100.100
Device status	A current status of the terminal device	C	1	Int	4	0:unknow, 1:online, 2:off-line
NOTE – USER ID, Group ID, login IP and device status are all mandatory if these attributes are available. If these attributes are different from previous records, they are all mandatory used when the device information list is returned.						

10.2 Attributes/elements used in broadcast-based terminal device discovery request

It is recommended to use the information in Tables 10-10 to 10-12 in the broadcast-based terminal device discovery mechanism.

Table 10-10 – Attributes/elements for broadcast-based terminal device discovery request

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Device ID	A unique identifier to indicate a certain device	C	1	String	50	001011000003
Source Agent IP address (private)	The IP address allocated by a local network, indicates where the message is sent from	C	1	String	40	192.168.1.100
Operation flag	A flag which indicates what the terminal device wants to do	M	1	Integer	4	0: terminal device discovery 1: status report (alive)
Discovery type	If this is a discovery request, this attribute indicates which discovery type is used.	C	1	Integer	4	0: all type terminal 1: target terminal
Target address	If one terminal is known with its address, this address should be embedded into the request message	C	1	String	40	192.168.1.102
NOTE 1 – Device ID and IP address will be conditionally used as a mandatory attribute depending on if the connection is an IP connection or not. NOTE 2 – Discovery type is used when Operation flag is set to 0: terminal device discovery. NOTE 3 – Target address is used when Discovery type is set to 1: target terminal l.						

Table 10-11 – Attributes/elements for broadcast-based terminal device discovery response

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Device ID	A unique identifier to indicate a certain device	C	1	String	50	001011000004
Responded Agent IP address (private)	The IP address allocated by a local network, indicates where the message is sent from	C	1	String	40	192.168.1.101
Device type	A symbol which indicates what the terminal device type is	O	0-n	Integer	4	0:H.721, 1:H.722, 3:b_TDES.4
Capability description URL	A URL that allows other terminal devices to access this device for capability or service description	M	1	String	256	http://192.168.1.101:53 or null
NOTE – Device ID and IP address will be conditionally used as a mandatory attribute depending on if the connection is an IP connection or not.						

Table 10-12 – Attributes/elements for broadcast-based terminal device discovery announcement

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Device ID	A unique identifier to indicate a certain device	M	1	String	50	001011000004
Responded Agent IP address (private)	The IP address allocated by a local network, indicates where the message is sent from	C	1	String	40	192.168.1.101
Status report (announcement)	To notify other terminal devices with the current status of source terminal device.	M	1	Integer	4	1:alive 0:byebye 2:update
Supported protocols	To indicate which discovery protocols could be supported	O	0-n	String	40	1: UPnP 2: mDNS 3: Miracast
Authentication type	To indicate which authentication mechanism is used	O	0-n	Integer	4	1:no auth 2: advanced encryption standard (AES)
NOTE – The Responded Agent IP address attribute is mandatory in the case of a device that is assigned a new IP address (e.g., a device that was temporarily offline and rejoins the local network).						

10.3 Attributes/elements used in terminal capability discovery description

The attributes/elements in Tables 10-13, 10-14, 10-15 are recommended to be adopted in capability description schema.

Table 10-13 – Attributes/elements for terminal capability description

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Device description	The list of the attributes about the physical device features	M	1	Container	variable length	See Table 10-14 or Null

Table 10-14 – Attributes/elements for device description

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Device type	A symbol which indicates what the terminal device type is	M	1	Integer	4	0:H.721, 1:H.722, 3:b_TDES.4
Device name	A special name for the terminal device	O	0-n	String	50	"my STB"

Table 10-14 – Attributes/elements for device description

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Device roles	Predefined roles which indicate the capability of the terminal device	M	1-n	String	40	Media server, controller [b-ITU-T H.IPTV-TDES.5]
Manufactory information	The information about the manufactory attributes	O	0-n	String[]	variable length	Mode name, serial number, etc.
Multi-device enabled service description	The list of the attributes about the service features which support multi-device service.	M	1	Container	variable length	See Table 10-15 or Null

Table 10-15 – Attributes/elements for multi-device enabled service description

Attributes	Description	M/O/C	Cardinality	type	Length (byte)	Example
Service type	Predefined roles which indicated the capability of the terminal device	M	1-n	String	40	Media server, controller, presentation [b-ITU-T H.IPTV-TDES.5]
Service ID	A serial number for identifying the service	M	1	String	50	0000102456045
Service access URL	A URL for accessing that service.	M	1	String	256	http://<device ip>:<port>/description.xml or null
Control URL	A URL for controlling that service. The detailed action, arguments are defined in the file which URL refers to.	M	1	String	256	http://<device ip>:<port>/description.xml or null
Event URL	A URL for event subscription. The detailed action, arguments are defined in the file which URL refers to.	O	0-1	String	256	http://<device ip>:<port>/description.xml
Presentation URL	A URL for service presentation. The detailed action, arguments are defined in the file which URL refers to.	O	0-1	String	256	http://<device ip>:<port>/description.xml
Supported protocols	The possible supported communication protocols for future service usage	O	0-n	String	40	HTTP, TCP

Appendix I

Informative procedure of registration-server address acquiring regarding the MDS

(This appendix does not form an integral part of this Recommendation.)

Terminal device discovery should be one of the functional components which is combined with other application functional components. For example, an IPTV multi-device service [b-ITU-T H.IPTV-MDS] should be initiated with terminal device discovery. Therefore, in service discovery, the MDS service record should give all the information that is used by each functional component.

In this Recommendation, for terminal device discovery procedure, especially for registration-based terminal device discovery, the registration server address must be known before the terminal device discovery procedure starts. Therefore, this address should be acquired during IPTV service discovery.

[ITU-T H.770] (IPTV service discovery), gives the elements and attributes of a service discovery record and service offer information. The registration server address should be filled in that record and be discovered by IPTV terminal.

There are three main steps to acquire the target registration server address, as illustrated in Figure I.1.

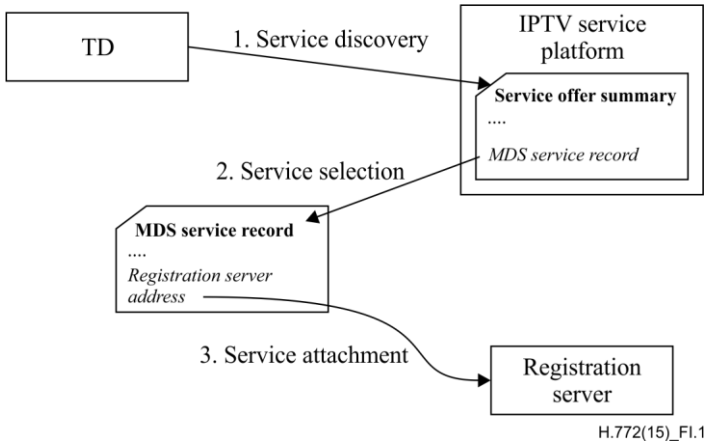

Figure I.1 – Procedure flow for registration server address acquisition

1. The IPTV terminal device initiates the service discovery procedure to retrieve the SP information record.
2. Based on the element in the SP information record, IPTV terminal device can find the service offer summary and find a service which needs to provide a terminal device discovery, e.g., a MDS service record.
3. The detailed MDS service information contains the necessary information that is used by terminal device discovery, e.g., a registration servicer IP address.

With the above information, if an IPTV user wants to start a multi-device service, the related application, e.g., an application user interface (UI), could guide a user to perform the terminal device discovery procedure.

It is noted that the registration server address in the service discovery record may not be the final allocated registration server. According to the different architecture of the registration server, the loading balance mechanism may be used. If there are many servers, the terminal should be finally allocated to an available server with sufficient capability of the registration service.

Appendix II

Example of registration server group deployment

(This appendix does not form an integral part of this Recommendation.)

The registration server may consist of many distributed servers, as illustrated in Figure II.1. These servers may be built up as a two- or three-layer network deployment. In these server groups, the top layer consists of several servers with different roles. One of these servers is a centre server that provides the capability of TDD service. The other server(s) may provide the backup function in the event that the centre server has crashed.

There are also one or two lower layers that consist of many edge servers. These servers are managed by the centre server for loading balance and provide the actual service for the IPTV terminal devices. If there is more than one layer, the servers in the middle layer also act as the centre server and manage the edge servers, but they themselves are managed by the top centre server.

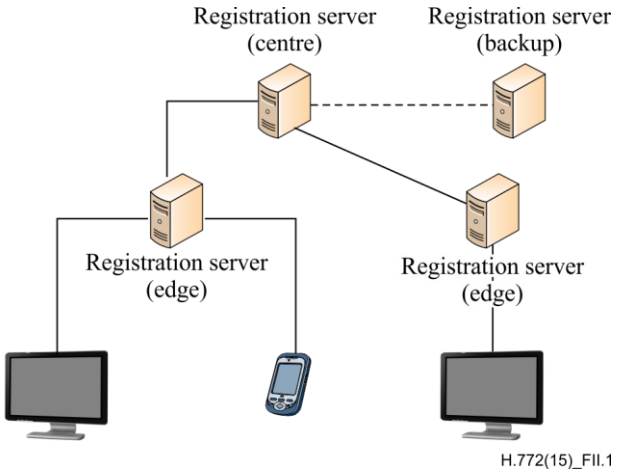

Figure II.1 – Network architecture for registration server group

With the above group architecture, the IPTV terminal device registration process may work as illustrated in Figure II.2 and described in the following procedure flows:

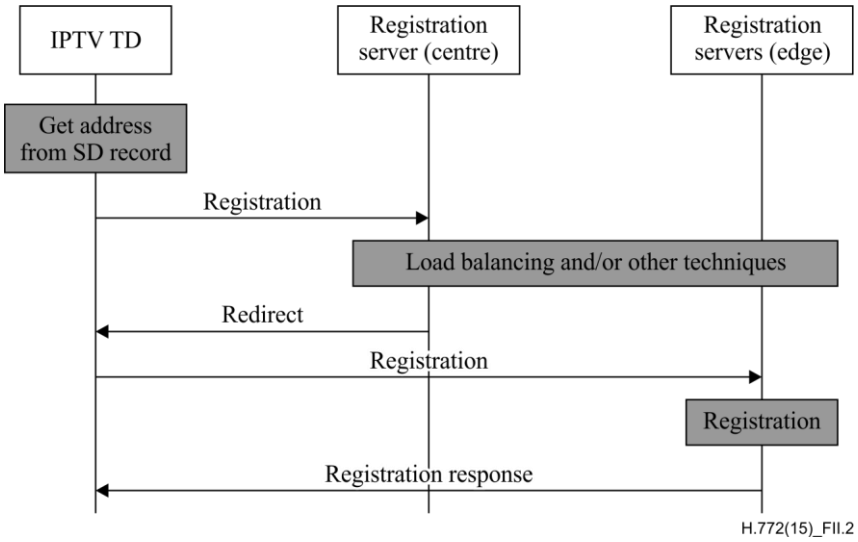

Figure II.2 – Procedure for registration server group loading balance

1. The IPTV terminal device gets a centre registration server address by analysing the SD record.
2. The IPTV terminal device imitates a registration process by sending a registration message to that centre registration server.
3. The centre registration server may select an available edge registration server based on some techniques, e.g., load balancing. That edge server address will be returned to the IPTV terminal device.
4. The IPTV terminal device sends the registration message again to the edge registration server.
5. The edge registration server completes registration and returns the registration results back to IPTV terminal device.

Once registered, the IPTV terminal device may not need to connect to the centre registration server again. Instead, the edge address may be stored and the IPTV terminal device can connect to that edge server directly when it boots up again.

Bibliography

[b-ITU-T H.622] Recommendation ITU-T H.622 (2008), *A generic home network architecture with support for multimedia services*.

[b-ITU-T M.1400] Recommendation ITU-T M.1400 (2015), *Designations for interconnections among operators' networks*.

[b-ITU-T Y.1901] Recommendation ITU-T Y.1901 (2009), *Requirements for the support of IPTV services.*

[b-ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture*.

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[b-ITU-T H.IPTV-MDS] ITU-T draft Recommendation H.IPTV-MDS, *IPTV Multiple Device Service*.
(under development at the time of publication of this Recommendation)

[b-ITU-T H.IPTV-TDES.4] ITU-T H.IPTV-TDES.4, *IPTV Terminal Device: Mobile model*.
(under development at the time of publication of this Recommendation)

[b-ITU-T H.IPTV-TDES.5] ITU-T draft Recommendation H.IPTV-TDES.5, *IPTV terminal device – interworking enabled mode of multiple devices*.
(under development at the time of publication of this Recommendation)

[b-ITU-T HSTP.IPTV-SMTD] ITU-T draft Technical Paper HSTP.IPTV-SMTD, *Technical Paper: IPTV service over multiple terminal devices*.
(under development at the time of publication of this Recommendation)

[b-DLNA guidelines] DLNA Guidelines (2014), *Digital living network alliance (DLNA) guidelines, Part 1: Architecture and protocols*.
<http://www.dlna.org/guidelines/>

[b-UPnP Device Control Protocol] Open Connectivity Foundation, UPnP Forum, *UPnP Device Architecture Version 1.0*.
<http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0-20081015.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016