BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 4

DCA2203

SYSTEM SOFTWARE

Unit 11

Universal Plug and Play

Table of Contents

1. INTRODUCTION

We learned about PCI drivers and USB drivers in the prior unit. You have a thorough understanding of how these gadgets function when they are linked to computers. This unit deals with UPnP technology that offers pervasive peer-to-peer network connectivity with computing devices of all forms, intelligent appliances, and wireless devices.

Everyone wants to be able to plug in their devices and use them everywhere. Many people may need to learn how to solve the intricacies of installing the device drivers. Majority wants Plug and Play types of devices without installing the device's drivers. This unit will introduce you to the technology and protocol working for running the UPnP-based devices.

1.1 Learning Objectives:

After studying this unit, the learners should be able to:

- *Explain what is UPnP*
- *Description of the working of UPnP-based devices*
- *Discuss the various UPnP protocols stack*
- *Describe how UPnP-based devices are addressed and discovered*
- *Explain about UPnP based devices*
- *Explain how the UPnP-based devices control, perform eventing and presentation*

2. UNIVERSAL PLUG AND PLAY: UPNP INTRODUCTION

UPnP stands for Universal Plug and Play. This extends an existing technology called PnP (Plug and Play). The organization behind UPnP is known as the UPnP Forum, formed on October 18, 1999, to develop the Device Control Protocol (DCP). It is a group of companies and individuals who wish to create a standard way to allow devices to configure themselves. Over 200 companies signed on at the beginning, including Intel, IBM, Sun, HP, AOL Time Warner, TI (and many others) to develop and deploy this concept related to the DCP. The main contributor to UPnP is Microsoft, which supplied the architecture that the specifications are built around. This evolved into UPnP. The Universal Plug and Play Forum define UPnP Device and Service Descriptions.

With UPnP technology, users can add devices to the home or office network without installing drivers or configuring them before using them. It is much easier to add peripherals like webcams and printers to a system that supports plug-and-play. Devices and their drivers can be set up automatically, allowing the device to relate to minimum problems. UPnP extends this functionality to the entire network, enabling other UPnP devices to be discovered and controlled. It can also make devices hot-swappable, connecting and disconnected without restarting the computer system.

2.1 UPnP architecture

The UPnP architecture is designed to offer pervasive peer-to-peer network connectivity of networked devices such as Personal Computers (PCs) of all form factors, intelligent appliances, and wireless devices. The UPnP architecture is a distributed, open networking architecture that leverages existing standards such as TCP/IP, HTTP, and XML instead of inventing new underlying mechanisms to enable seamless proximity networking, in addition, to control and data transfer among networked devices in the home, office, and everywhere in between. The architecture consists of a set of standardized protocols that each UPnP technology-enabled device implements to provide for discovery, control, and data transfer between UPnP devices (See Figure11.1).

The UPnP architecture provides:

- Device connectivity: The UPnP architecture defines the protocols for interacting with other devices. UPnP devices can join and leave the network transparently, advertise their services, discover other devices and services, send events, and control other devices.
- Ad-Hoc networking: UPnP devices can come together to form a network dynamically without the need for dedicated networking infrastructure services. These instantaneous ad hoc networks allow for device communication without requiring manual configuration.
- Zero-configuration networks: The UPnP architecture supports zero-configuration networking where the user is not required to configure devices before they are used on the network.

Standards-based architecture: The core of the UPnP architecture is an array of existing and proposed open standards.

Standard Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) protocols include IP, TCP, UDP, HTTP, XML, and SOAP.

- Platform independence: UPnP devices can be developed on any platform – on any specific operating system, language, or hardware.
- Media and device independence: UPnP technology can run on any medium with an IP stack, including phone lines, power lines, Ethernet, RF, and IEEE1394.
- Programmatic and manual device control: The UPnP architecture enables applications to programmatically control home networking devices. In addition, users can manually control devices using the device's browser-based administrative interface.

2.2 Basic principles of UPnP

The basic principle of UPnP is to allow **invisible** networking, as referred to by the UPnP Forum. A network's IP Address, a unique identifier, is automatically assigned to the UPnP-enabled device when linked to an appropriate network. Every UPnP-enabled device can communicate with every other device via the network, so each can learn the presence of the other and their capabilities. UPnP is independent of any specific particular programming

language or operating system and is available to everyone. UPnP technology can be supported on any common operating system or hardware platform. It works with almost any type of physical networking media – wired or wireless – providing maximum user and developer choice.

The basic building blocks of a UPnP-enabled network consist of three main components. They are (i) **Devices** (ii) **Services**, and (iii) **Control Points**. Figure 11.1 shows the basic architecture of UPnP and where the UPnP Control Points, Devices, and Services are interlinked for communication in the network.

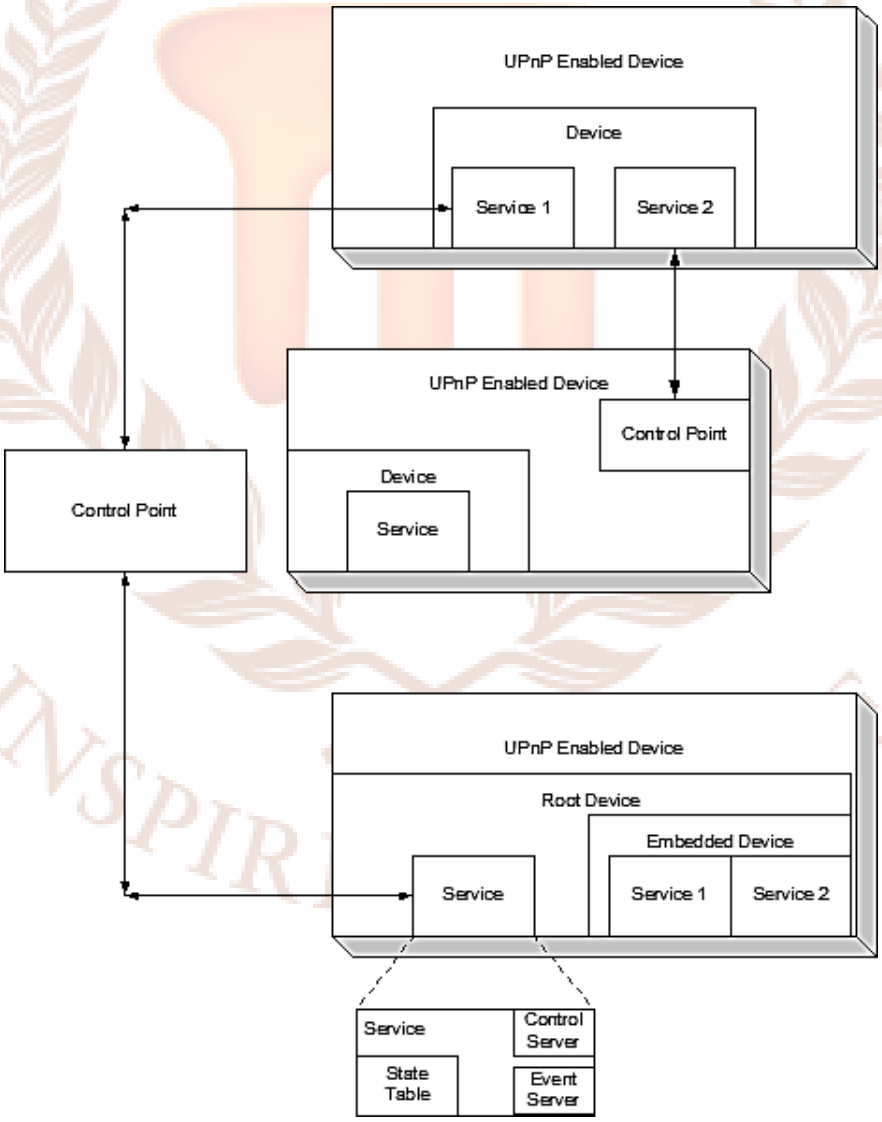


Figure 11.1: UPnP Control Points, Devices, and Services

(i) **Devices:** A Device acts as a container that holds several services. Modern cell phones, an example of devices with UPnP capabilities. A nested device might also be present in the device. A nested device may include

Another device is built into the main device. A common example of a nested device found in phones is the digital camera.

The Device Description Document file is the brains of any UPnP device. This file is written in **XML** so any device or computer to discover the device properties can view it.

(ii) **Services:** A Service is the set of functions that a Device supports. The available services are listed in the **Device Description Document**. Each Service on the **Service List** links to its **XML** file, which provides a detailed description of the Service. Services are supported by two main values: an **Action** and a **State**.

Action: An Action might be "receive a call" or "send a file," for instance, on a UPnP-capable mobile device.

State: A State describes the current status of a device. The state of the device changes depending on the situation. As a typical example, the device's state is **busy** if a telephone is already taking a call.

A typical UPnP device will have three functions that deal with Services:

- **State Table:** This takes the current state of the Service, e.g., Busy or Waiting, and records it. It will be updated when the State value changes.
- **Control Server:** This response to requests for action. The Service's current State value will be updated.
- **Event Server:** This is responsible for letting other devices (i.e., their services) know when the State of the Service changes, e.g., it can now accept incoming connections.

(iii) **Control Points:** A control point discovers and then controls other devices it finds on the network. It retrieves the Device Description Document file and the Service list from each device.

2.3 Uses And Applications

UPnP is a service-based technology that relies on state changes (of the environment) to determine what happens on the network. A few of the uses and applications of UPnP-based devices are:

- Adding network devices and networked programs to a network.
- Configuration of devices by themselves in the network.
- Build networked applications.
- Connect computing hardware devices such as routers, modems, and wireless gadgets.
- Automating a house or workplace by figuring out what's going on in the neighborhood.

Let us understand the concept of components of UPnP:

- Addressing
  - UPnP uses IP addressing; so it acts as a DHCP client to assign IP itself
  - If there is no server (DHCP) found, then it assigns itself an IP; this process is called AutoIP
- Simple Service Discovery Protocol (SSDP)
  - To locate one another, gadgets employ this protocol.
  - Devices can receive messages from other devices on the same network thanks to this protocol.

The next two components include device description and service calls.

- Device Description
- Devices share data in XML forms to be aware of one other's information.
  - Name of the model, year of manufacture, etc., may be included in this data.
- Service calls
  - The device can make a service call after learning more about the other device.
  - This is accomplished with the aid of SOAP (Simple Object Access Protocol)

Now, another two components include GENA and presentation:

- General Event Notification Architecture (GENA)
  - This architecture responds to service calls
  - Control point is used to keep track of device model variables; it is informed of any changes.
- Presentation
- The gadget contains a URL for the manufacturer.
  - From the web browser, this data can be utilized to modify device settings.

2.4 Benefits Of Upnp Technology

UPnP is media and device independence. UPnP technology can run on any network using any communications media, including Radio Frequency (RF, wireless), phone line, power line, IrDA, Ethernet, and IEEE 1394. The benefits of UPnP-based devices are as follows:

i) Platform independence: Vendors can use any operating system and programming language to build UPnP products.
ii) Internet-based technologies: UPnP technology is built upon IP, TCP, UDP, HTTP, and XML, among others.
iii) UI Control: UPnP architecture enables vendor control over the device user interface and browser interaction.
iv) Programmatic control: UPnP architecture enables conventional application programmatic control.
v) Common base protocols: Vendors agree on base protocol sets on a per-device basis.
vi) Extendable: Each UPnP product can have value-added services layered on top of the basic device architecture by the individual manufacturers.

2.5 Advantages/Disadvantages Of Upnp

Advantages

- It allows true plug-and-play compatibility with all UPnP-enabled devices.
- It is simple for the consumer: plug in and go, so it is ideal for home care scenarios.

- Since UPnP is backed by some very large corporations, e.g., Microsoft and Intel, it can be commonplace for all developers.

Disadvantages

- UPnP will cause heavy network traffic due to communication of every other device on the network, slowing the network down if only limited bandwidth is available.
- Security can become an issue if UPnP has been used to set up a home network without expert advice. Shared files or folders could become available to external sources via the Internet, so third-party security software may be required to block this.
- UPnP seems to be a slow-moving technology. There are products that are UPnP enabled, but they are difficult to find in typical electrical outlets and are often not marketed as UPnP compatible.

2.6 Steps in UPnP device addressing

All UPnP devices must follow the same steps in acquiring an IP address. The steps, as specified by the UPnP device architecture, are shown in Figure 11.3.

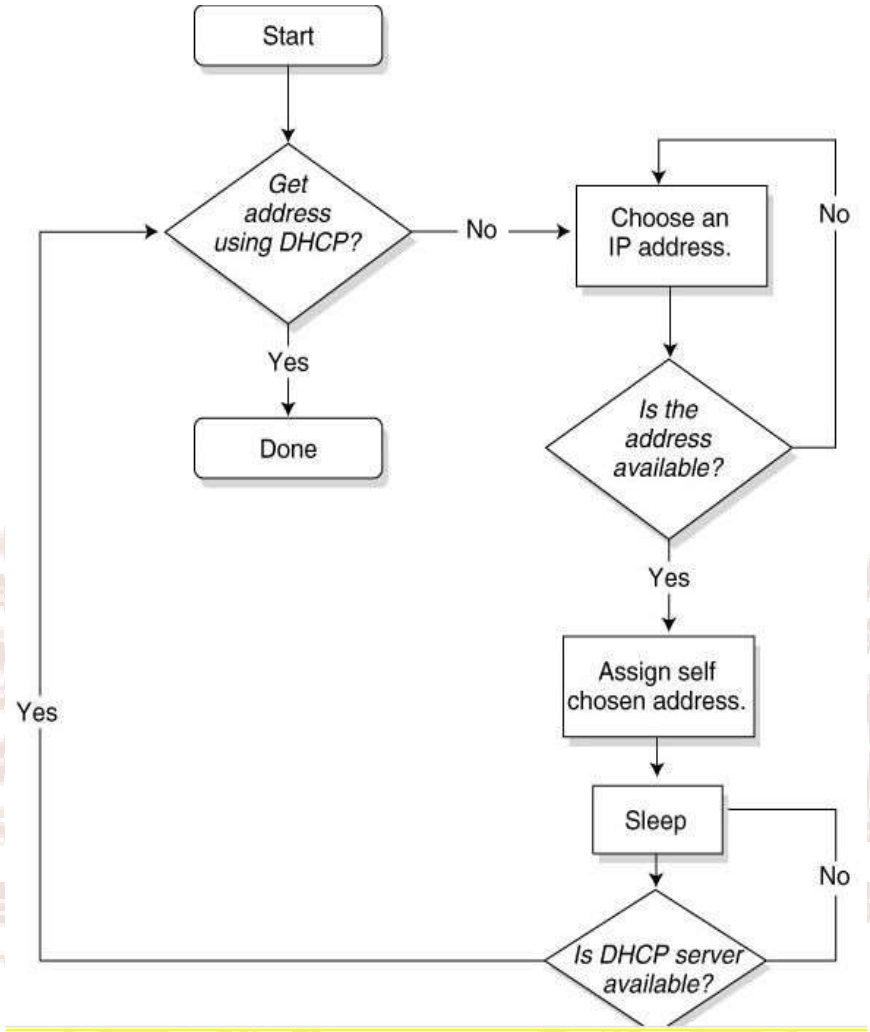


Fig 11.3: UPnP Device Addressing Flowchart

Step1: Try to obtain an address via DHCP

First, a UPnP device must try to get an address from a DHCP server. If the device successfully acquires an address, it is ready to continue with subsequent UPnP phases.

Step2: Failing DHCP, proceed with Auto-IP

If the UPnP device fails to acquire an address from a DHCP server, it begins selecting and testing an IP address.

Step 2a: Choose an IP address

To help keep clients from becoming stuck in a loop with other clients while trying to allocate an address, clients implementing Auto-IP are expected to randomize their IP address selection algorithm.

Step 2b: Test whether the address is available

When using Auto-IP to select an address, the client tests to determine whether the address is already in use. If so, the client chooses another address and tries again. A certain algorithm is used to ensure clients' auto-configuring on busy auto-configured network segments does not loop infinitely looking for an IP address.

Step 2c: Periodically check for a DHCP server

Whenever the DHCP server is available, the devices must switch to a DHCP-assigned address. UPnP devices configured using Auto-IP must, therefore, periodically test for the availability of a DHCP server. When rechecking, if the device determines that no DHCP server is available, it waits for some time and then tries again.

Step 2d: Upon finding a DHCP server, switch to a DHCP-assigned address

After receiving a response from a DHCP server, the UPnP device must respond and obtain a lease from the server. If the client successfully obtains the lease, it must drop any existing automatically configured IP addresses unless the device supports multiple addresses on the interface being configured.

The implementation defines how the device drops existing connections , but it should allow existing connections to be completed before closing them. In addition, the device should not allow new connections tothe old, automatically configured address. Once all connections on the old address are closed, it can remove the address from the interface and be entirely transitioned to the new address.

Self-Assessment Questions - 1

1. The"_____" Forum defines UPnP Devices and Service Descriptions.
2. A"" device could be another device built into the main device.
3. A control point retrieves the" " file and the Service list from each device.
4. Services in UPnP are supported by two main values: an" " and a.

3. UPNP PROTOCOL STACK

UPnP works as per a series of network protocols designed to make it easier to attach devices to computer-like devices and their networks. Devices on a UPnP network can be connected using any communications media, including Radio Frequency (RF, wireless), phone line, power line, IrDA, Ethernet, and IEEE 1394. Any medium that can be used to network devices together can enable UPnP. The only concern might be that the media being used supports the bandwidth required for the intended use.

UPnP uses open, standard protocols such as TCP/IP, HTTP, and XML. However, other technologies could be used to network devices together for many reasons, including cost, technology requirements, or legacy support. These include networking technologies like HAVi, CeBus, LonWorks, EIB, or X10. These, too, can participate in the UPnP network through a UPnP bridge or proxy.

Generally, Standard protocols like TCP/IP, HTTP, HTTPU, HTTPMU, SSDP, GENA, SOAP, and XML are used for communication in UPnP. UPnP works with a Six "step" protocol involved in UPnP networking. They are: (i) Addressing (ii) Discovery (iii) Description (iv)

Control (v) Eventing (vi) Presentation. Will study these protocols in the next sections of this unit.

Figure 11.2 shows Protocol Stack and its various layers.

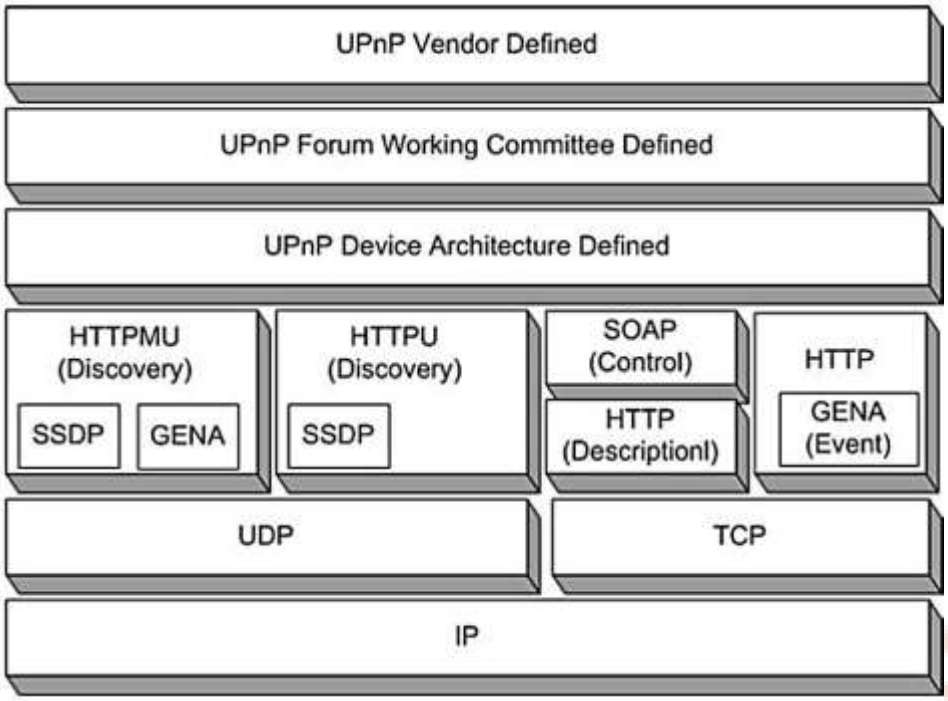


Figure 11.2: Protocol Stack

The UPnP protocol stack consists of three UPnP layers and other layers with standard protocols. Let us read about these layers.

(1) UPnP vendor-defined: It is the top layer, and it gives vendor-specific information (e.g., serial number)

(2) UPnP forum working committee defined: This is the second upper layer and is defined as per the UPnP forum working committee.

(3) UPnP device architecture defined: This layer gives device-specific global information. (e.g., VCR info, DVD player info, etc.)

The other layers in the protocol stack work as per the protocols like SOAP, SSDP, and GENA. They are:

(i) **Simple Object Access Protocol (SOAP):** It is used for Remote Procedure Calls (RPC).

(ii) **Simple Service Discovery Protocol (SSDP):** It is used for broadcast and search. It helps with adding/removing devices from the network. SSDP is used over HTTPMU and HTTPU to provide basic information about services.

(iii) **Generic Event Notification Architecture (GENA):** It is used to subscribe and publish messages. This mechanism handles events. A service that wants to send an event does so by either HTTP or HTTPU to registered listeners.

(iv) **HTTP-over-Multicast (HTTPMU):** Although HTTPMU is an expired IETF draft and is not a W3C standard, it was invented to support UPnP. HTTPMU is expected to use the syntax of HTTP while changing the semantics. For HTTPMU, the contents of the datagram are HTTP requests.

(v) **HTTP-over-UDP (HTTPU):** HTTPU sends a single datagram over UDP to a host. The recipient may reply to the host and port that sent the datagram. Again, standard HTTP requests are not expected to be sent, only that the syntax is obeyed.

The lowest three layers work as per the standard protocols like TCP, UDP, and IP. UPnP relies heavily on IP and the TCP and UDP stacks which are the Internet standards. It uses SOAP for method calls, which rely on HTTP, which in turn needs TCP. It uses HTML user interfaces, again requiring HTTP and TCP.

Self-Assessment Questions - 2

5. Which protocol is used for Remote Procedure Calls (RPC) in UPnP?
   a) Generic Event Notification Architecture (GENA)
   b) Simple Object Access Protocol (SOAP)
   c) Simple Service Discovery Protocol (SSDP)
   d) HTTP-over-Multicast (HTTPMU)
6. Which of the following is used to subscribe and publish messages in UPnP?
   a) Generic Event Notification Architecture (GENA)
   b) Simple Object Access Protocol (SOAP)
   c) Simple Service Discovery Protocol (SSDP)
   d) HTTP-over-Multicast (HTTPMU)
7. HTTP-over-Multicast (HTTPMU)is an IETF draft and is a W3C standard. (True/False)

4. ADDRESSING

In any communication delivery system, communicating endpoints must have a unique address. If you want a UPnP to be networked, then the first logical step in networking is to obtain an address. The way UPnP devices acquire, manage and release addresses arecalled addressing. Addressing is the first step in UPnP networking; without an address, a device cannot proceed with subsequent UPnP phases, such as discovery where it offers its services to control points on the network.

UPnP devices are built upon the foundation of the TCP/IP protocol suite, which provides the network layer connectivity devices needed to communicate. Each endpoint on an IP network has an address that uniquely identifies it among all the endpoints on the network. Generally, every user would want their UPnP device configured automatically through some automatic addressing mechanism rather than manually configured.

There are two addressing protocols available for the automatic configuration of UPnP. They are: (i) Dynamic Host Configuration Protocol (DHCP) and

(ii) Auto-IP (Without DHCP Server).

With DHCP, the device takes the IP address or domain name assigned to it. Without a DHCP server, the devices use an Auto IP addressing protocol to get an address. Auto IP is a protocol in which a system chooses its IP address from a given set of addresses.

4.1 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network, including the host's IP address, subnet mask, default gateway, and domain name server. A client/server protocol uses UDP as its transport. DHCP clients send messages to DHCP servers on port 67 and receive responses from servers on port 68. A DHCP server manages a pool of IP addresses, automatically assigning addresses to network hosts and reusing released addresses. Using a DHCP server to assign addresses to IP endpoints centralizes the management of IP addresses, ensuring that each.

Endpoint receives a unique address and avoids problems that arise with manual configuration.

There are three mechanisms DHCP can use to assign IP addresses to clients. They are:

- ***Automatic allocation:*** The DHCP server assigns a permanent IP address to a client.
- ***Manual allocation:*** The network administrator determines the address assignment for each host. The DHCP server conveys the address to the clients when they request an address from the DHCP server.
- ***Dynamic allocation:*** This is the common mode of operation where the DHCP server assigns an IP address to the client for a limited time. The client is said to have a lease on the address. Once the lease expires or is released by the client, the server may assign this address to another client.

Each UPnP device is required to have a built-in DHCP client. When a UPnP device is first connected to a network, it searches for a DHCP server to acquire an IP address. In theory, a DHCP server servicing a network of UPnP devices could use any of the three mechanisms. However, dynamic allocation provides the best match as it requires no administrative configuration per client.

4.2 Auto-Ip

Using DHCP to assign addresses to a dynamically changing set of devices has a difficulty that a DHCP server may not be running all the time without administrative support. As per the zero-administration philosophy, the designers of the UPnP architecture want UPnP devices to acquire addresses on networks without a DHCP server. Auto-IP is the solution to comply with such a philosophy.

Auto-IP is a method by which an endpoint on an IP network may automatically choose an IP address and subnet mask in the absence of a DHCP server. Auto-IP does not replace DHCP but augments it, making clients more robust by allowing them to acquire addresses without DHCP services. UPnP devices use the Auto-IP mechanism only if a DHCP server is not present or if the DHCP process fails. In addition, the UPnP device architecture specifies how a UPnP

device has configured its address using Auto-IP must. It must periodically check for the presence of a DHCP server to smoothly transition to use a DHCP-assigned address.

4.2.1 Address Selection

UPnP devices use Auto-IP to get an IP address by selecting a candidate address. The address selection must fall within a range of 169.254/16 addresses that are non-routable IP addresses. Addresses in this range will not cross gateways, so they will never make it outside an organization and onto the Internet. After selecting an address, the client configures itself with a default class B subnet mask of 255.255.0.0.

The Internet Assigned Numbers Authority (IANA) has reserved this range for private IP address, so no one can use it on the Internet. This range is known as the ***LINKLOCAL net***. Also, the first and last 256 addresses are reserved for future use and must not be selected.

4.2.2 Resolving Address Conflicts

Once the UPnP device has selected an address, it must verify that it is not already being used by another device on the network. The UPnP device uses the Address Resolution Protocol (ARP) to do this .

Self-Assessment Questions - 3

8. Two addressing protocols are available for the automatic configuration of UPnP. They are"_____" and"_____" .
9. DHCP clients send messages to DHCP servers on port"_____" and receive responses from servers on port .
10. UPnP devices use the"_____" mechanism only if a DHCP server is not present, or if the DHCP process fails.

5. AD-HOC NETWORKS

Using Auto-IP for address assignment, it is possible for hosts to come together and form an ad-hoc network without having the assistance of pre-existing network infrastructure, including DHCP and DNS servers.

6. DISCOVERY

Once a UPnP device acquires an address, it is ready to provide its services to control points on the network. Discovery is the next phase in UPnP device operation. Controllers look for any devices of interest, and devices look for a controller. Control points to search for devices and services on the network and find ones that meet its search criteria.

Service discovery is the mechanism by which devices and network-based services make themselves available to clients, and clients can discover devices and services. Simple Service Discovery Protocol (SSDP) is the discovery protocol used by UPnP devices. SSDP was designed to discover HTTP-based resources based on Uniform Resource Identifiers (URI). SSDP uses a decentralized model of communication that requires no user administration. SSDP's balanced scheme of discovery requests and presence announcements minimizes network traffic. UPnP adds conventions for using SSDP, including predefined service types and the composition of URIs to search for devices and services.

7. SIMPLE SERVICE DISCOVERY PROTOCOL (SSDP)

The Simple Service Discovery Protocol (SSDP) is a simple discovery solution for HTTP-based resources on the local area network that doesn't require any configuration, management, or administration. SSDP doesn't attempt to address the problem of Internet-wide HTTP-based resource discovery. Other protocols, such as Universal Description Discovery and Integration are left to handle that issue (UDDI).

8. SERVICE IDENTIFICATION

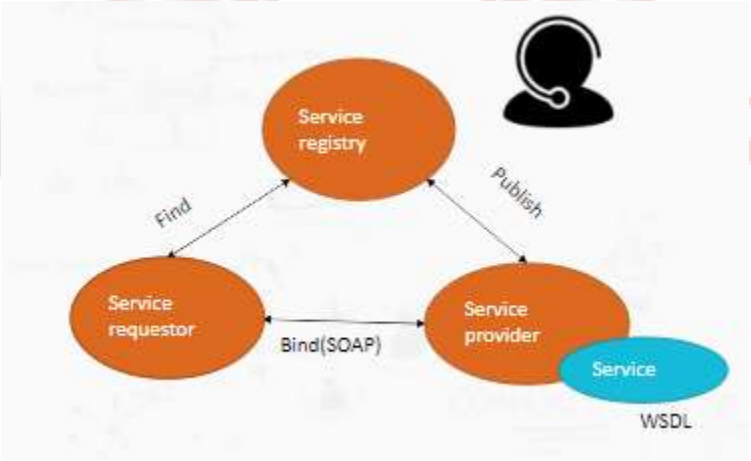
SSDP introduces two concepts related to service identification, the *service type* and the *Unique Service Name (USN)*. A service type is a URI that identifies the type or function of a particular resource – a printer service, for example. SSDP does not define service types but provides the mechanisms for discovering them. The UPnP working committees for each standard device type specify the service types for UPnP devices and services.

A Unique Service Name is a URI used to uniquely identify an instance of a particular service, allowing SSDP clients to differentiate between two services with the same service type. AUSN typically contains a Universally Unique Identifier (UUID)—a 128-bit number used to uniquely identify an object.

The benefits of service-oriented approaches are as follows:

- Benefits of a service-oriented approach
  - The binding of services may be postponed by application till they are delayed.
  - Services can be used concurrently by multiple applications because they are independent.
  - Any service provider may offer services.

Service-oriented Architecture Diagram:



The service-oriented architecture diagram is important to understand its functionalities:

Service Provider:

- It develops a web service and gives the service registry its details. Each service provider disputes a variety of hows, and whys, including which service to expose, which to prioritize—security or accessibility—and many more. Additionally, the service provider must choose what category the product should be classified under for a specific broker service and what trading partner agreements are necessary to use the product.

Service broker, service registry, or service repository:

Its primary purpose is to provide any potential requester access to the web service's information. Whoever implements the broker determines the broker's scope. Public brokers are accessible to everyone, whereas only a small portion can access private brokers. An early attempt to provide Web services discovery was UDDI, which is no longer actively supported.

Service requester/consumer:

It uses a variety of find operations to find entries in the broker registry before binding to the service provider and calling one of its web services. Any service that the service users require must be obtained from the brokers, bound to the required service, and then used. If the service offers various services, they can access them all.

Let us look at the benefits of Service-oriented Architecture:

- Local service providers or third parties can be used to deliver services.
- Services are available in any language.
- It is possible to protect investments in legacy systems.

In general, a resource may have multiple representations, and they can exist in different formats:

- Resource Operations
  - Create: Make the resource available

- Read: Obtain a replica of the resource back
- Update: Change the value of the resource
- Delete: Make the resource inaccessible

Let us now learn about resources and actions:

The resource is a data element, such as a medical record.

General resource actions:

We have CREATE(),READ(),UPDATE(),DELETE().

Web resources:

We have POST(),GET(),PUT(),DELETE().

Let us see the types of ad hoc networks:

- Mobile ad hoc networks (MANET) : A wireless, self-organizing network of portable devices is known as a mobile ad hoc network.
- Wireless sensor networks (WSN): Mobile devices called wireless sensor networks are used to collect specific environmental data like temperature, humidity, traffic volume, etc.
- Wireless mesh networks (WMN): Based on the mobility pattern, wireless mesh networks create wireless meshes.
- Vehicular ad hoc networks (VANET): The formation of a vehicular ad hoc network is communication between moving vehicles.

Ad hoc networks have the following benefits:

- Decoupling from central network administration
- Self-configuring nodes acting as routers.
- Scalability includes the addition of extra nodes;
- Self-healing through ongoing reconfiguration.
- In any scenario involving several wireless devices, mobility enables the instantaneous creation of ad hoc networks.

Understanding the issues of the ad hoc network:

- Low quality communication
- Time-varying protocol
- Scalability
- Energy conservation
- Hidden node problem
- Exposed node problem

9. COMMUNICATION MODEL

SSDP uses a decentralized approach to service discovery whereby no central store maintains information about resources, their location, and their availability. Instead, each client directly queries the network, and each resource responds directly to these requests.

10. DISCOVERY REQUESTS AND PRESENCE ANNOUNCEMENTS

There are two types of SSDP requests (i) discovery requests and (ii) presence announcements.

Discovery requests allow SSDP clients to look for SSDP resources. Presence announcements allow SSDP resources to announce their presence on the network. SSDP's balance of discovery requests and presence announcements is designed to make the protocol efficient, reducing network traffic. When a resource comes online, it announces its presence. This lets all clients know that the resource is available. From then on, the resource does not need to send out any other presence announcements, except when it is going offline. Any clients that come on- line after the resource has announced its presence send out discovery requests. If the resource supports the requested service, it responds to the client. The client does not need to repeat the discovery request because any resources that come on-line after it has issued the request will announce their presence. The result is that neither client nor server need send out steady streams of messages.

11. NETWORK TRANSPORT

SSDP uses HTTP over multicast UDP to send messages to every SSDP peer on the network. SSDP client's multicast HTTPMU discovery requests to the address 239.255.255.250:1900, which is SSDP's reserved multicast address and port that has local administrative scope, limiting the delivery of the multicast packet to an administrative domain.

SSDP services listen to the SSDP multicast channel to hear the discovery requests. If an SSDP resource receives a multicast HTTPMU discovery request that matches the service it offers, it responds by sending a response directly to the SSDP client that issued the search using the HTTPU.

The features of TCP:

- Features of TCP
  - Stream Data Transfer
  - Reliability
  - Flow Control
  - Multiplexing
  - Logical Connection
  - Full Duplex

Let us understand the features of TCP in detail:

- Stream Data Transfer: The stream of bytes is transported across the internet by the virtual circuit.
- Logical connection: The socket, sequence number, and window size together
- Full Duplex: Data can be transferred in both directions at the same time
- Multiplexing: combines two or more connections to data streams
- Flow Control: It controls the flow of data transfer
- Reliability: It adheres to the error-control mechanism and flow.

The features of UDP:

- Features of UDP
  - Source port address
  - Destination port address
  - Checksum
  - Total length

The features of UDP:

- Provides the sender's source port address in the source port field.
- Total Length: Contains information about the message's total bytes.
- Provides the receiver's destination port address in the destination port address field.
- Checksum: Offers the checksum technique to reduce error.

Let us look at the responsibilities that are provided by the transport layer:

- Transport layer services
  - End-to-End delivery
  - Addressing
  - Reliable delivery
  - Flow Control
  - Multiplexing

Self-Assessment Questions - 4

11. Which of the following is the discovery protocol used by UPnP devices?
    a) Simple Service Discovery Protocol (SSDP)
    b) Universal Description Discovery and Integration (UDDI)
    c) Universally Unique Identifier (UUID)
    d) Unique Service Name (USN)
12. SSDP introduces two concepts related to service identification _____ and the"____"_____.
13. There are two types of SSDP requests:"_____" and_____.

12. DESCRIPTION

The description phase of UPnP comes after discovery. It enables control points to discover details about devices and the services they implement. After a UPnP control point discovers a device, it only contains the information in the discovery message. Those discovery messages are the device's type, its universally unique identifier, and a URL to its description document. The control point collects description documents from the device to learn additional information about the device, including the services and operations it supports.

Device and service description documents are XML documents that follow a standard schema defined by the UPnP Forum. The contents (elements) of specific devices and service descriptions are defined by various working committees of the UPnP Forum and correspond to the required information that a standard UPnP device must have.

12.1 Upnp's Description Phase

The description phase is the link between UPnP's discovery and control phases. In the discovery phase, devices advertise their presence to control points on the network, while control points search for devices. Once a control point receives these advertisements and finds a device of interest, it gets the description documents directly from the device to learn more about the device and its services. Once a control point has processed the description documents and understands the device's capabilities, it is ready to control the device.

12.2 Description Document Standards

Device and service descriptions are simply XML documents that conform to the UPnP Template Language. The UPnP ForumThe UPnP Forum defines the XML syntax defines the XML syntax for creating device and service descriptions. This basic template language is used by the various working committees of the UPnP Forum to define standard devices and the services they must contain.

Self-Assessment Questions - 5

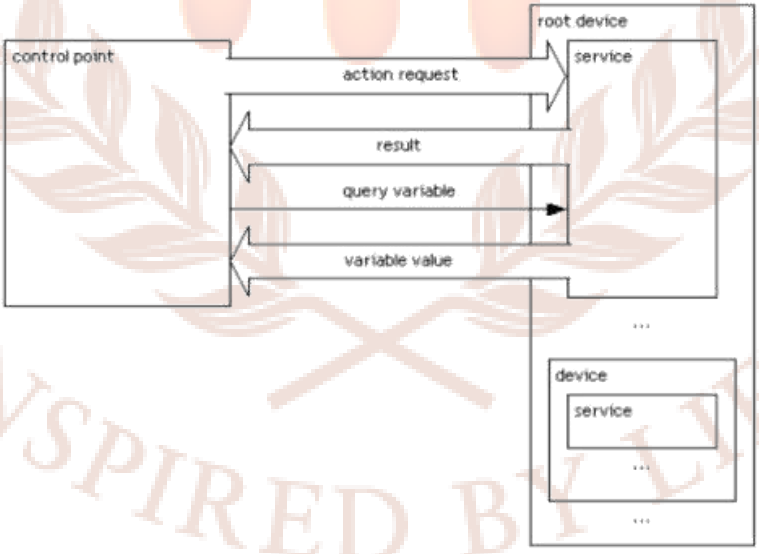
14. The"_____"phase is the link between UPnP's discovery and control phases.
15. Device and service description documents are"_____"documents that follow a standard schema defined by the UPnP Forum.

13. CONTROL

After a UPnP device acquires an IP address and advertises its presence on the network, control points can discover the device and invoke any of the actions provided by the device's services. In UPnP terminology, this invocation process is called control.

The control point sends a suitable control message to the control URL for the service provided in the device description. Control messages are also expressed in XML using the Simple Object Access Protocol (SOAP). The control protocol used between UPnP control points and devices is called Simple Object Access Protocol (SOAP). SOAP is a messaging and remote procedure call technology that can be used over a variety of transports but is primarily used over HTTP. UPnP control points use SOAP to invoke actions provided by services contained on a device. In response to the control message, the service returns any action-specific values.

In the description steps, different kinds of methods are used.



They are mentioned below. The most often used methods are device and service description, UPnP Device and Service Template.

- Device Description
- UPnP Device Template
- Service Description

- UPnP Service Template
- Non-Standard Vendor Extension
- UPnP Template Language for Devices
- UPnP Template Language for Services
- Retrieving a Description

Now let us see the protocol and action under control:

- Control messages at the top layer include vendor-specific data like parameter values.
- Vendor material is augmented with data from a UPnP Forum working group, including names for statements, actions, and variables.

Action Invoke

- For remote procedure calls, the Simple Object Access Protocol (SOAP) specifies the use of XML and HTTP.
- Control messages are sent to devices via SOAP, and results or errors are returned to control points.

Action Response

- Within 30 seconds, including estimated transmission time, the service must finish invoking the action and respond.

Now let us see the protocol and action under control:

- Control messages at the top layer include vendor-specific data like parameter values.
- Vendor material is augmented with data from a UPnP Forum working group, including names for statements, actions, and variables.
- Next, we have a query for the variable:
- Query Invoke
- To query a state variable's value, a control point must send a request in the following format.
- Query Response:

- To answer a query for the value of a state variable, the service must respond within 30 seconds, including the expected transmission time.
- If the service fails to respond within this time, whatever the control point does should be application specific. The service must send a response in the following format.

Self-Assessment Questions - 6

16. Control messages are also expressed in XML using the _____ .
17. UPnP control points use SOAP to invoke actions provided by services contained on a device. (True/False)

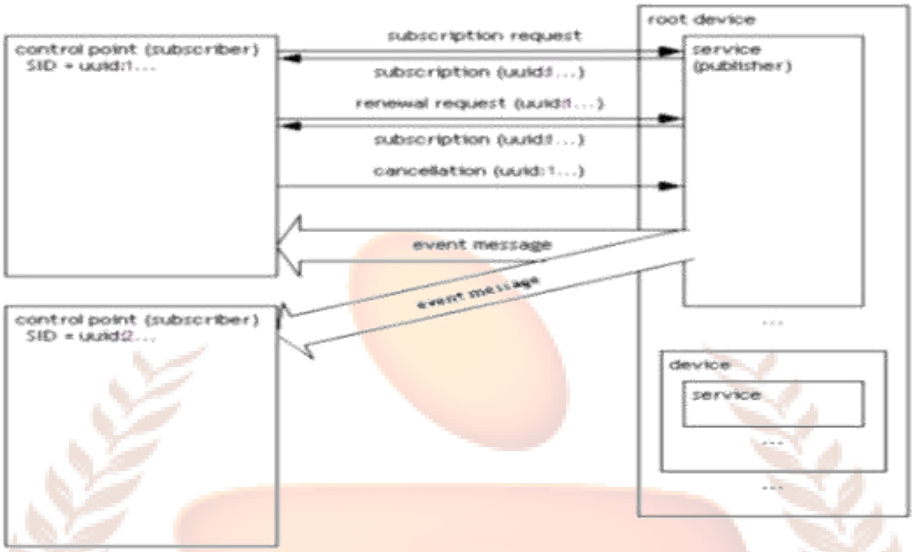
14. EVENTING

While an UPnP device is being controlled, its service changes states. This sends event messages to any subscribed controllers. A special event is generated when a controller subscribes to a device. This event causes the device to send names and values of state variables to the controller. This allows the controller to initialize its state model for that service. With the help of the Eventing protocol, a device will notify all subscribers when state changes occur. Eventing enables groups of UPnP devices and control points to be dynamic, responding automatically to state changes. Eventing allows control points to register to a device when state changes occur. Control points receive a notification and may wish to respond to that notification by invoking an action. In contrast to a synchronous remote procedure calls, eventing in a distributed system call mechanisms such as RPC. Events are expressed in XML and sent over to General Event Notification Architecture (GENA). GENA gives ability to subscribe/publish.

The UPnP architecture uses GENA for eventing, adding conventions of its own. In particular, the UPnP architecture uses GENA to publish changes to a service's evented state variables. A publisher is a service that accepts registrations from clients interested in receiving notifications. A subscriber is called a "client" and will subscribe to a publisher. If a subscriber does not wish to receive any event notifications, they may unsubscribe from the publisher. The publisher will then stop sending event messages on state changes. Subscriptions may expire over time. To keep receiving message notifications, a renewal subscription must be submitted by the client.

GENA uses HTTP as the transport layer for communication between publishers and subscribers. To achieve this GENA has introduced three new HTTP methods for subscription and notification:

- SUBSCRIBE to register for events and receive notifications.
- This is also used for renewing existing subscriptions.
- UNSUBSCRIBE to cancel subscriptions.
- NOTIFY to send events to the subscriber.



In eventing, different kinds of methods have also been used. They are as follows:

- Subscription
- Event Messages
- UPnP template language for eventing
- Augmenting the UPnP template language

After a control point, has (1) discovered a device and (2) retrieved a description of the device and its services; the control point has the essentials for eventing.

To subscribe to eventing, a subscriber sends a subscription message. If the subscription is accepted, the publisher responds with a duration for the subscription.

The different steps involved in UPnP networking are given below.

Step 1: Discovery explains how devices advertise and control points search and explains the details of the format of discovery messages.

Step 2: Description explains how devices are described and how those descriptions are retrieved by control points.

Step 3: The control section explains the description of actions, state variables, and control message format.

Step 4: The service publishes updates when these variables change, and a control point may subscribe to receive this information. The service publishes updates by sending event messages.

Step 5: The degree to which each of these can be accomplished depends on the specific capabilities of the presentation page and device.

In the description steps, different kinds of methods are used.

They are mentioned below. The most often used methods are device and service description, UPnP Device and Service Template.

- Device Description
- UPnP Device Template
- Service Description
- UPnP Service Template
- Non-Standard Vendor Extension
- UPnP Template Language for Devices
- UPnP Template Language for Services
- Retrieving a Description

Self-Assessment Questions - 7

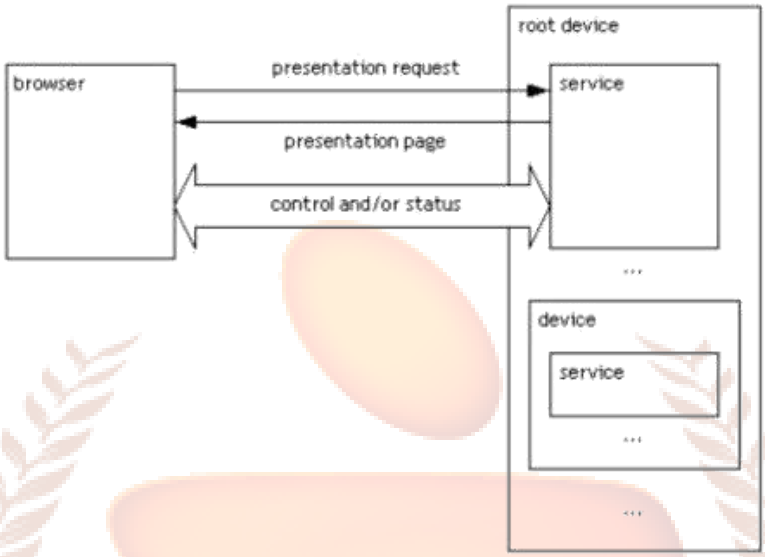
18. Which among the following protocol is used by device to notify all subscribers when state changes occur?
    a) discovery
    b) Eventing protocol
    c) addressing
    d) control
19. The UPnP architecture uses”_____"to publish changes to a service’s evented state variables.

15. PRESENTATION

Presentation exposes an HTML-based user interface for controlling and/or viewing device status. Presentation is complementary to control, where control points send actions to devices and eventing where control points listen to state changes in devices.

UPnP devices have embedded web servers because most of the communications protocols, including XML-based device descriptions, SOAP-based control messages, and GENA's event-related messages, run over HTTP. Every UPnP device can provide a web interface for administrative monitoring and control through the device presentation page. The URL for the presentation is contained within the presentation URL element in the device description. The device description is delivered via a description message. Retrieving a presentation page is a simple HTTP- based process.

The interactions between control points and devices can be entirely automatic, requiring no human intervention. However, it is also possible to manually control UPnP devices using the device's presentation page, a web page provided by the device, and loaded by an administrator using a web browser. PnP technology enables network devices to present their functionality as programmable services to be manipulated by control points. Hence, depending on the device's capabilities, the presentation can be Monitored and Controlled. Although the presentation page is purely an optional administrative interface added to devices for providing a means for direct programmable control. The UPnP Forum does not dictate the required contents, appearance, or capabilities of device presentation pages, but allows these things to be completely determined by the vendor. However, if a device supplies a URL for a presentation page, the control point must be able to retrieve a page from the URL and load it into a browser. Depending upon the capabilities of the page, it must be able to allow a user to control the device and/or view device status.



Given above is the diagrammatic working of presentation:

A presentation request moves from a browser to the service in the root device.

The response is loading of the presentation page.

The entire process is managed via control and/or status request.

Similarly, multiples request and replies move in & out via the browser and the services.

Self-Assessment Questions - 8

20. Every UPnP device can provide a"_____"interface for administrative monitoring and control through the device presentation page.
21. PnP technology enables network devices to present their functionality as programmatic services to be manipulated by"_____"points.

16. SUMMARY

Let us recapitulate the important concepts discussed in this unit:

- The UPnP architecture is designed to offer pervasive peer-to-peer network connectivity of networked devices such as Personal Computers (PCs) of all form factors, intelligent appliances, and wireless devices.
- The Universal Plug and Play Forum define UPnP Device and Service Descriptions.
- The basic building blocks of a UPnP enabled the network to consist of three main components: (i) Devices (ii) Services, and (iii) Control Points.
- Generally, communication in UPnP occurs through standard protocols like TCP/IP, HTTP, HTTPU, HTTPMU, SSDP, GENA, SOAP, and XML.
- UPnP works with a Six "step" protocol in UPnP networking: (i) Addressing (ii) Discovery (iii) Description (iv) Control (v) Eventing and (vi) Presentation.
- The way UPnP devices acquire, manage, and release addresses is called addressing.
- There are two addressing protocols available for automatic configuration of UPnP. They are: (i) DHCP and (ii)Auto-IP
- Service discovery is the mechanism by which devices and network- based services make themselves available to clients, and clients can discover devices and services. SSDP is the discovery protocol used by UPnP devices.
- To find more detail about the device, including the services and actions it supports, the control point retrieves description documents from the device in description phase.
- Control points can discover the device in the network and invoke any of the actions provided by the device's services by the invocation process called control.
- The control protocol used between UPnP control points and devices is the Simple Object Access Protocol (SOAP).
- With the help of the Eventing protocol, a device will notify all subscribers when state changes occur. Events are expressed in XML and sent over General Event Notification Architecture (GENA).
- It is possible to manually control UPnP devices using the device's presentation page, a web page provided by the device and loaded by an administrator using a web browser.

17. GLOSSARY

- Ad-Hoc networking: Dynamic network without the need for dedicated networking infrastructure services.
- Auto-IP: DHCP to assign addresses to a dynamically changing set of devices time without administrative support.
- Home network: Home network is a computer network that facilitates communication among devices within the close vicinity of a home.
- Platform independence: Developed on any platform, no specific operating system, language, or hardware.
- Plug and play: Users can add devices to the home or office network without installing drivers or configuring the devices before using.
- Simple Service Discovery Protocol (SSDP): Simple discovery solution for HTTP-based resources on the local area network that does not require any configuration, management, or administration.
- Zero-configuration network: It is a networking where to configure devices not required to use.

18. TERMINAL QUESTIONS

Short Answer Questions

1. Explain the basic building blocks of an UPnP enabled network.
2. Draw the neat diagram of UPnP Protocol stack and explain each of its layers in brief.
3. Draw the UPnP device addressing flowchart and explain it in stepwise manner.
4. Explain how discovery is performed in UPnP device operation.
5. What is the difference between control and Presentation? Explain.

19. ANSWERS

Self-Assessment Questions

1. Universal Plug and Play
2. nested
3. Device Description Document
4. Action, State
5. b) Simple Object Access Protocol (SOAP)
6. a) Generic Event Notification Architecture (GENA)
7. False
8. DHCP, Auto-IP 9.67,68
9. Auto-IP
10. a) Simple Service Discovery Protocol (SSDP)
11. service type, Unique Service Name (USN)
12. scovery requests, presence announcements
13. XML
14. description
15. Simple Object Access Protocol (SOAP)
16. True
17. b)Eventing protocol
18. GENA
19. web
20. control

Short Answer Questions

1. The basic building blocks of an UPnP enabled network to consist of three main components: Devices, Services, and control Points. (Refer to section 2 for more details)
2. The UPnP protocol stack consists of three UPnP layers and other layers with standard protocols like TCP/IP, HTTP, HTTPU, HTTPMU, SSDP, GENA, SOAP, XML. (Refer to section 3 for more details)

3. The steps are Step 1: Try to obtain an address via DHCP, Step 2: Failing DHCP, proceed with Auto-IP (Refertosection4 formoredetails)
4. Simple Service Discovery Protocol (SSDP) is the discovery protocol to discover HTTP-based resources based on Uniform Resource Identifiers (URI). (Refer to section 7 for more details)
5. Control points invoke any of the actions provided by the device's services by the invocation process called control whereas presentation exposes an HTML-based user interface for controlling and/or viewing device status. (Refer to sections 13 and 15 for more details)

20. SUGGESTED BOOKS

- Jeronimo, M., & Weast, J. (2003). UPnP Design by Example – A Software Developer's Guide to Universal Plug and Play. IntelPress.
- MATCH PROJECT Mobilizing advanced technologies for care at home. (n.d.).Retrieved 08 02, 2012, from What is UPnP? http://www.cs.stir.ac.uk/~kjt/research/match/resources/tutorial/Home Care_Network