



US 20060274743A1

(19) **United States**(12) **Patent Application Publication****Yegin et al.**(10) **Pub. No.: US 2006/0274743 A1**(43) **Pub. Date: Dec. 7, 2006**(54) **SYSTEM AND METHOD FOR A MOBILE DEVICE TO LEARN INFORMATION ABOUT THE ACCESS NETWORKS WITHIN ITS NEIGHBORHOOD****Related U.S. Application Data**

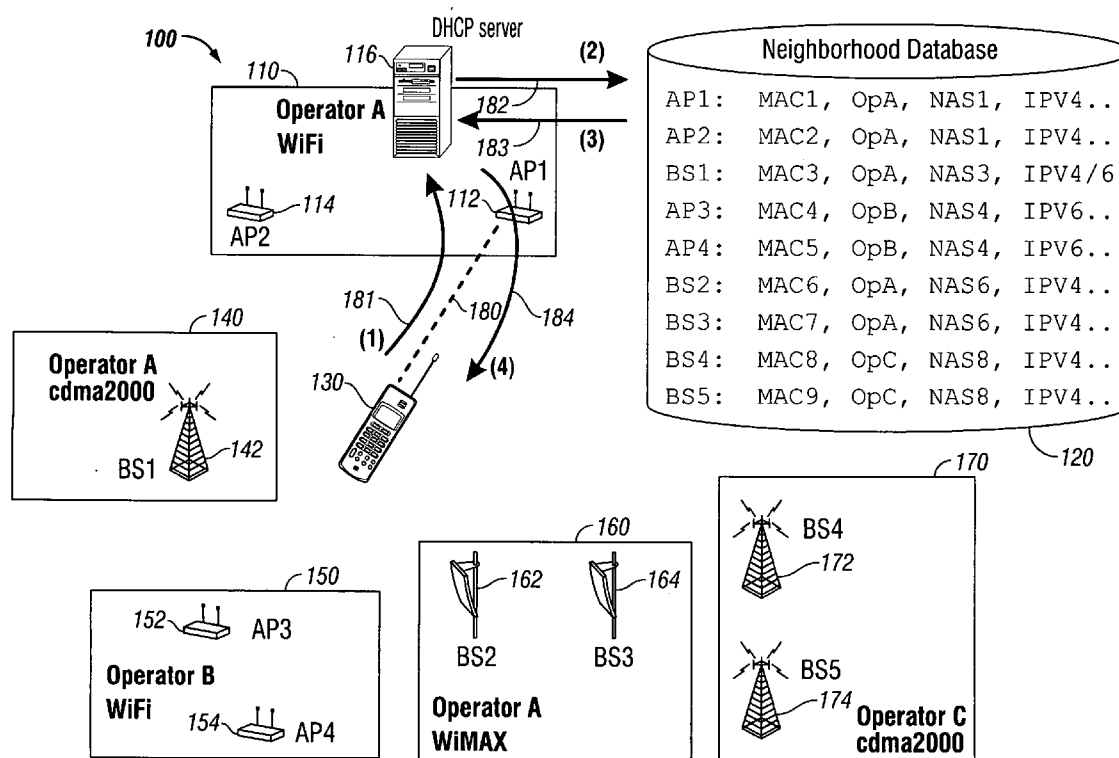
(60) Provisional application No. 60/687,833, filed on Jun. 6, 2005.

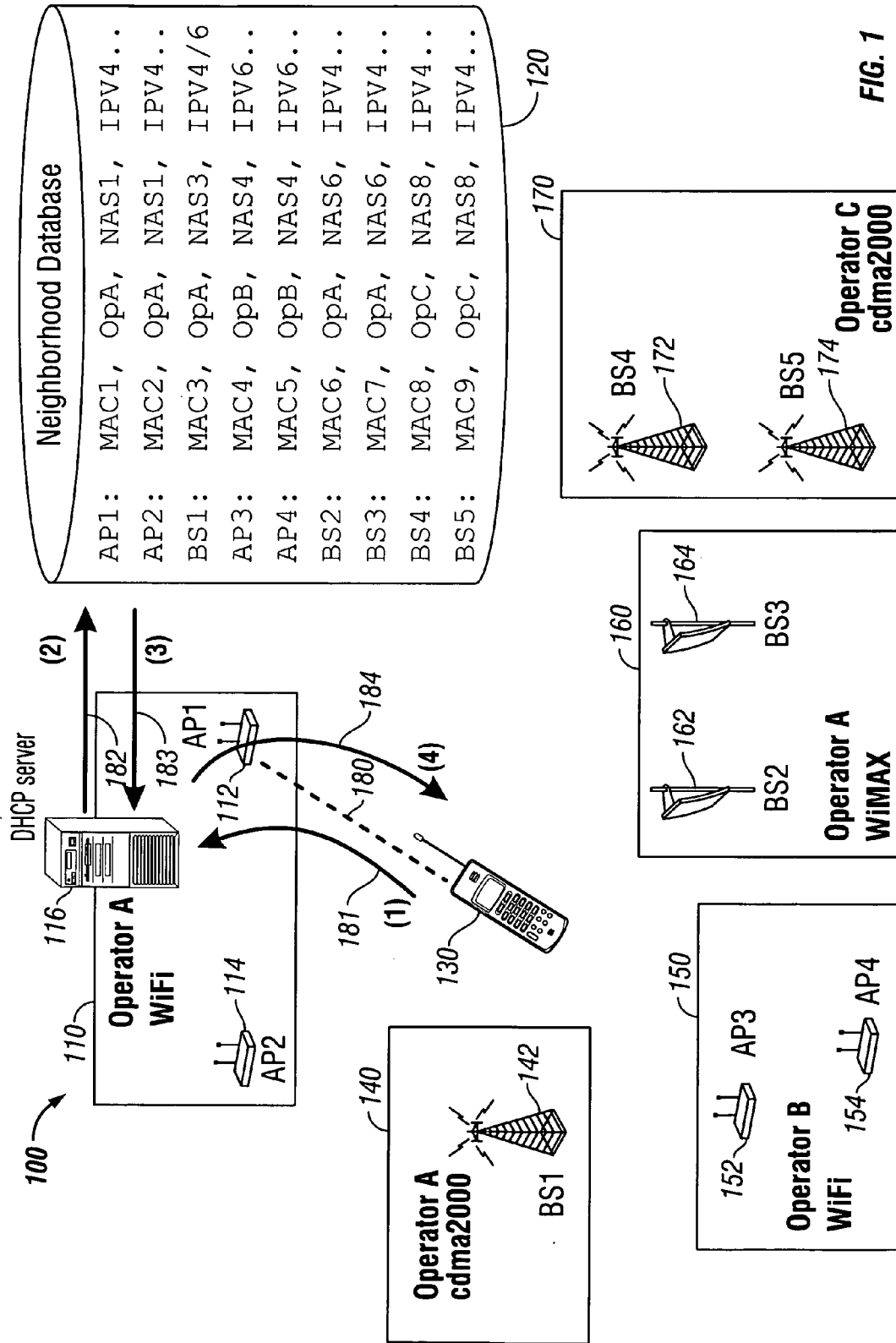
Publication Classification(51) **Int. Cl.**
H04L 12/56 (2006.01)(52) **U.S. Cl.** **370/389**(57) **ABSTRACT**

A system and method for a mobile device to learn information about the access networks within its neighborhood is disclosed. In certain embodiments, information about networks in a neighborhood of a particular network is stored in a database associated with a dynamic host configuration protocol server. Periodic beacons of an access point of at least one network identified in the database are received by mobile stations. One of the mobile stations requests capability and configuration information of one or multiple target networks or all networks in the database. The requested capability and configuration information is provided to the mobile station.

Correspondence Address:

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614 (US)

(21) Appl. No.: **11/342,326**(22) Filed: **Jan. 27, 2006**



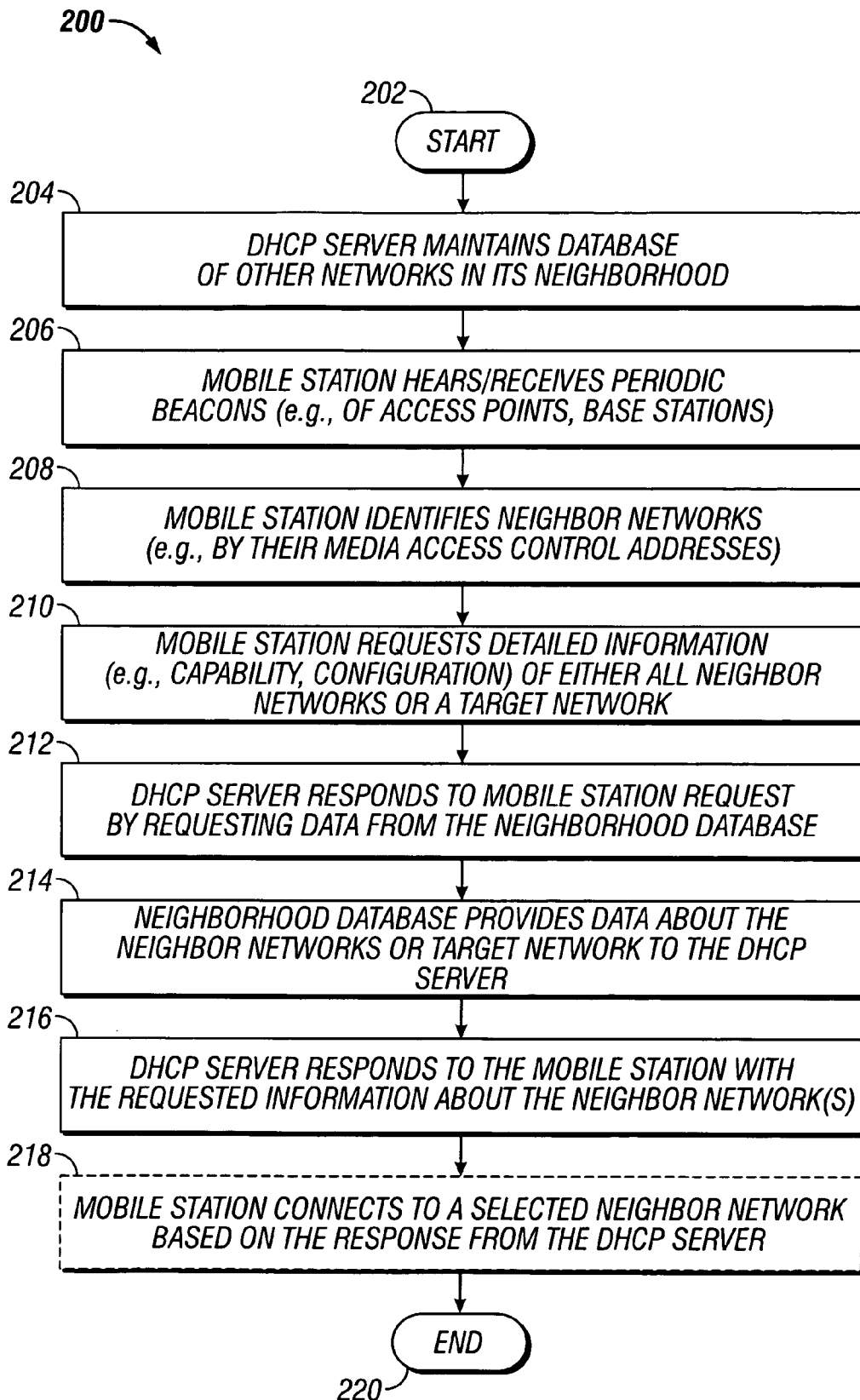


FIG. 2

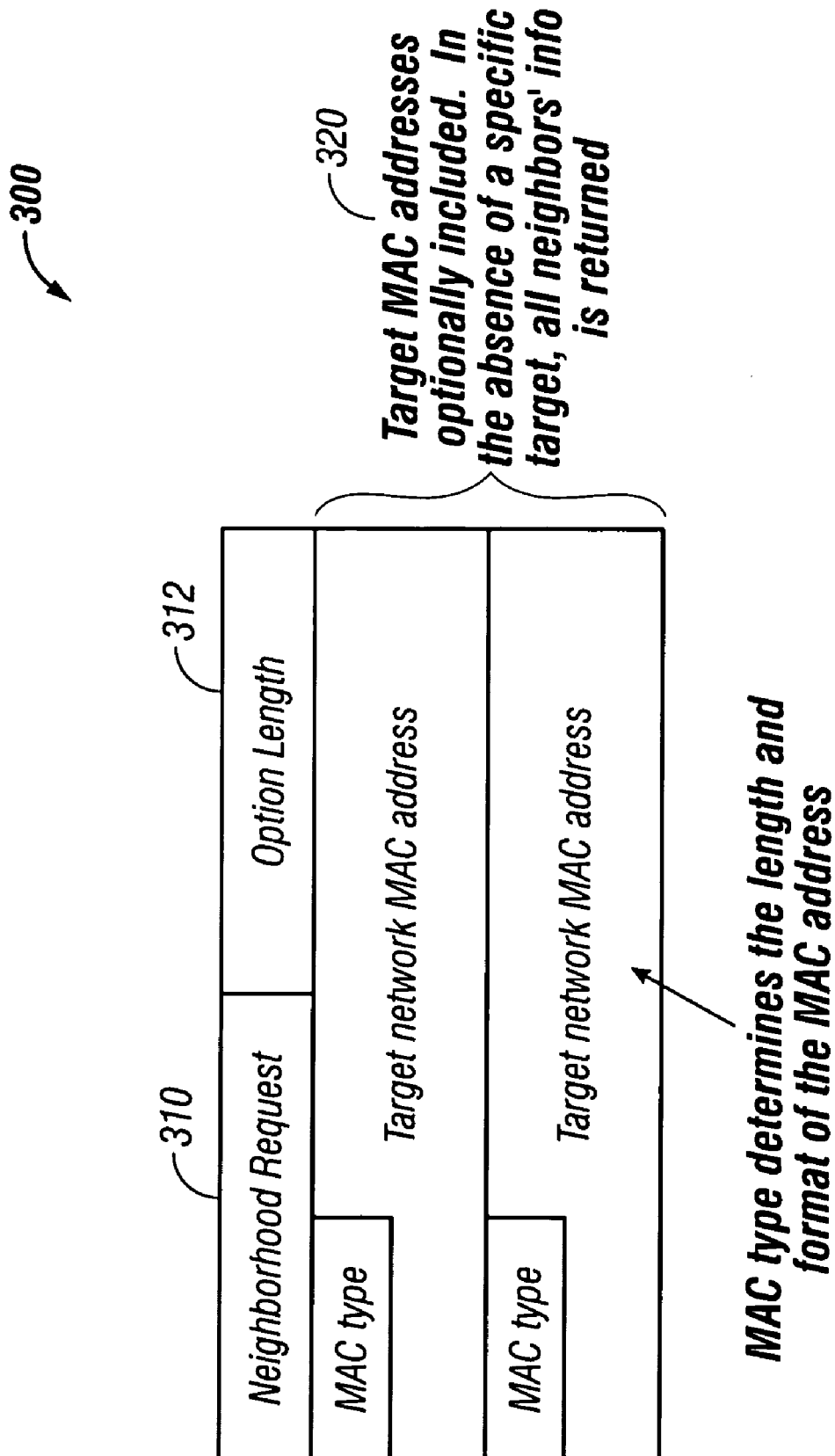


FIG. 3

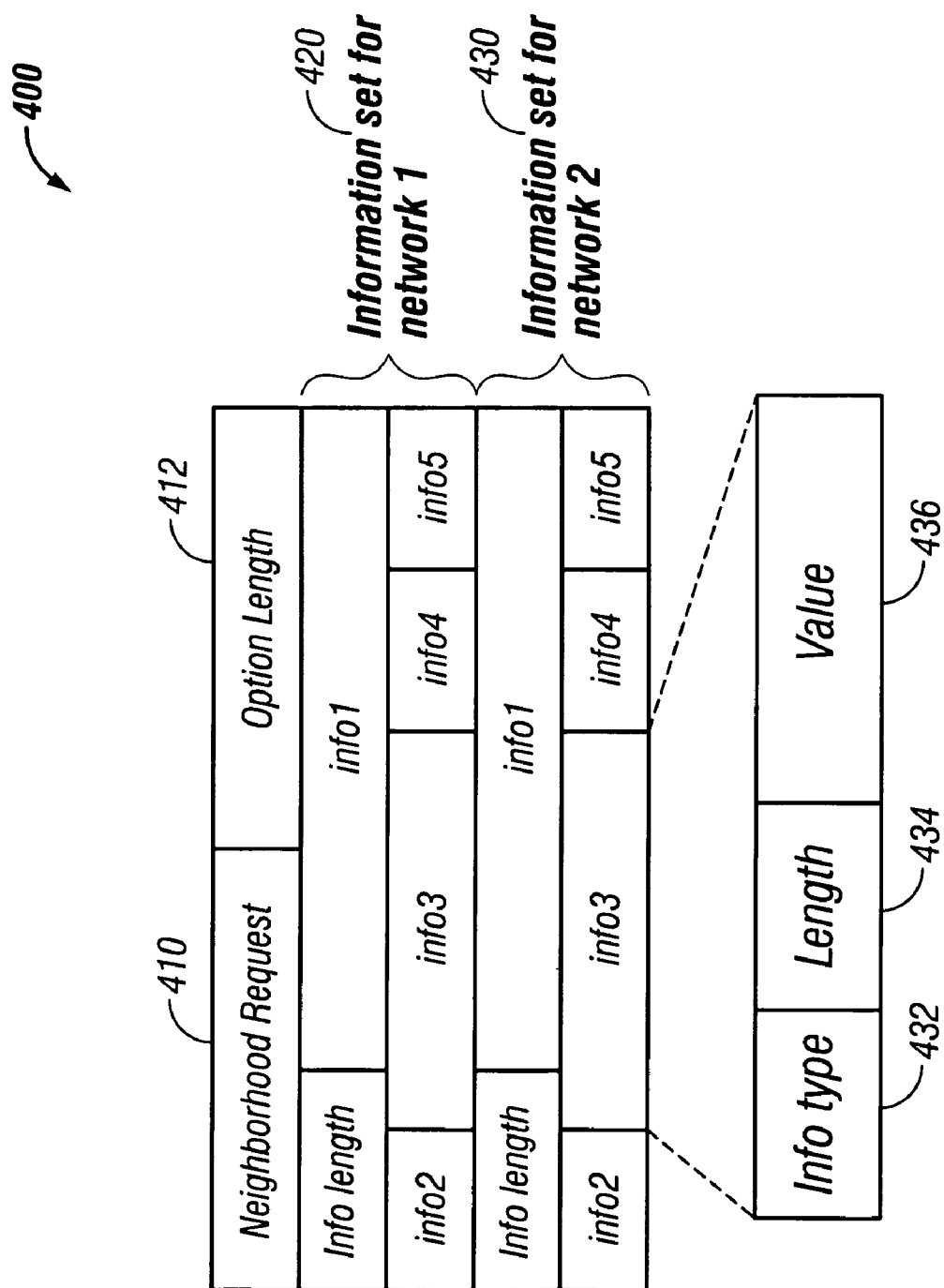


FIG. 4

SYSTEM AND METHOD FOR A MOBILE DEVICE TO LEARN INFORMATION ABOUT THE ACCESS NETWORKS WITHIN ITS NEIGHBORHOOD

RELATED APPLICATIONS

[0001] This application claims the benefit under 35 U.S.C. §119(e) of U.S. Patent Application No. 60/687,833 filed Jun. 6, 2005, for “MOBILE AND WIRELESS NEIGHBORHOOD DISCOVERY USING DHCP”, which is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] This invention relates to wireless networks, and particularly to configuration and capability discovery in Internet Protocol (IP) based wireless networks.

[0004] 2. Description of Related Technology

[0005] Recently a variety of computer network systems have been widely used. Such network systems include a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a wireless local area network (WLAN), a wireless personal area network (WPAN), a general packet radio service (GPRS) network and other wireless network systems, such as wireless fidelity (WiFi), worldwide interoperability for microwave access (WiMAX) and code division multiple access 2000 (CDMA2000). WiFi is a term for certain types of WLANs that use specifications in the IEEE 802.11 family. WiMAX is a form of broadband wireless access based on the IEEE 802.16 standard for MANs. CDMA is also known as IMT-CDMA Multi Carrier or 1×RTT, and is a third generation mobile wireless technology. The network systems allow communication between various end terminals or mobile stations such as a personal computer (desktop, laptop, palm-top or handheld), a mobile phone, or other portable communication devices. It is typical that the above network systems include at least one bridge element such as an access node or access point where user traffic enters and exits a communications network.

[0006] Dynamic Host Configuration Protocol (DHCP) [1] [2] allows a host (a computing device such as an end terminal or a mobile station) to discover the capabilities and configurations associated with a currently serving access network. The DHCP, however, does not provide this information for any of the other networks (target networks) that the host may connect to. Neighbor networks are wireless networks in the vicinity or neighborhood of a mobile station.

[0007] There is some ongoing work to achieve this goal over Media Access Control (MAC) layer designs [2]. Such designs can provide only a subset of the information that is needed for a full discovery. In addition, as Level 2-specific (of the seven layer open system interconnection model) mechanisms, they lack universal applicability (for example, an IEEE 802.11k solution works only on IEEE 802.11 links, and on nothing else). Such designs also cannot be easily applied to legacy networks that are already deployed.

[0008] A very small subset of the target information is incorporated in some specific protocol work, such as Proxy Router Discovery used in Mobile IPv6 Fast Handovers [3]

(e.g., prefix information of the candidate access router). Again, this has very limited applicability and cannot solve the general problem.

[0009] Current solutions lack the fundamental needs of wireless networks:

[0010] Applicability to any IP networks (All-IP)

[0011] Discovering the presence of neighbor networks

[0012] Learning the extensive list of capability and configurations of neighbor networks.

SUMMARY OF CERTAIN INVENTIVE ASPECTS OF THE INVENTION

[0013] Embodiments of a method and system for proactively discovering a capability and configuration of candidate wireless networks in the neighborhood of a mobile station are described. The DHCP enables a mobile station to discover the capabilities and configurations of a currently serving network. Using the method, the mobile station can discover the wireless networks in its vicinity and the respective capability and configurations. This enables the mobile station to make better handover decisions in selecting target networks, take preparatory actions prior to the handover, and expedite the connection setup once the mobile station connects to the target.

[0014] In one embodiment, there is a network having a dynamic host configuration protocol server, comprising a dynamic host configuration protocol (DHCP) server embedded in a network being in a neighborhood of identified wireless networks; a database, in data communication with the DHCP server, configured to store at least media access control (MAC) address of each identified network; and an access point, in communication with the DHCP server, configured to send beacons to at least one mobile station, wherein each beacon has at least a MAC address of the access point; wherein the DHCP server receives a request for configuration and capability information of one or more of the identified networks, obtains the requested information from the database, and provides the requested information to a mobile station that requested the information.

[0015] In another embodiment, there is a network discovery method, comprising maintaining a database of network identifiers associated with a plurality of networks in a neighborhood of a particular network, sending beacons from an access point of at least one network identified in the database, receiving a request for capability and/or configuration information of at least one network identified in the database, and providing the requested capability and/or configuration information to a mobile station.

[0016] In another embodiment, there is a network discovery system, comprising means for storing information about identified networks in a neighborhood of a particular network, means for sending beacons from an access point of at least one network identified in the storing means,

means for receiving a request for capability and/or configuration information of at least one network identified in the storing means, and means for providing the requested capability and/or configuration information to a mobile station.

[0017] In another embodiment, there is a network discovery method, comprising storing information about a plurality

of networks in a neighborhood of a particular network, sending beacons from an access point of at least one of the neighborhood networks, requesting capability and configuration information of at least one network, and providing the requested capability and configuration information to a mobile station.

[0018] In another embodiment, there is a network discovery method, comprising learning information about one or more access networks within a neighborhood of a mobile host via dynamic host configuration protocol (DHCP).

[0019] In yet another embodiment, there is a network discovery method, comprising learning a configuration and capability of a given access network via dynamic host configuration protocol (DHCP) by a mobile station.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] The foregoing and other features of the invention will become more fully apparent from the following description and appended claims taken in conjunction with the following drawings, in which like reference numerals indicate identical or functionally similar elements.

[0021] **FIG. 1** is a diagram illustrating an exemplary configuration of components and related operations of an embodiment of the invention.

[0022] **FIG. 2** is a flowchart of an exemplary process operating on the configuration shown in **FIG. 1**.

[0023] **FIG. 3** is a diagram of an exemplary DHCP request option format as used by the process of **FIG. 2**.

[0024] **FIG. 4** is a diagram of an exemplary DHCP reply option format as used by the process of **FIG. 2**.

DETAILED DESCRIPTION OF CERTAIN EMBODIMENTS OF THE INVENTION

[0025] **FIG. 1** illustrates an exemplary configuration of an embodiment of a wireless network system **100** that proactively discovers a capability and configuration of candidate wireless networks in the neighborhood of an exemplary mobile station (MS) **130**. The network system **100** may be implemented with one or more of an IEEE 802.11 a/11b/11g (WiFi) network, a wireless local area network (WLAN), a metropolitan area network (MAN) (e.g., WiMAX), a wireless personal area network (WPAN), a general packet radio service (GPRS) network, a global system for mobile communication (GSM) network, a code division multiple access (CDMA) network (e.g., CDMA200), a Bluetooth network or other wireless networks. As shown in **FIG. 1**, the system **100** includes a plurality of networks operated by multiple network operators. These networks include a WiFi network **110** operated by Operator A, a CDMA2000 network **140** operated by Operator A, WiFi network **150** operated by Operator B, a WiMAX network operated by Operator A, and a CDMA2000 network operated by Operator C. In the exemplary configuration of **FIG. 1**, WiFi network **110** includes a first access point (AP1) **112**, a second access point (AP2) **114**, and a DHCP server **116** for performing the DHCP. The DHCP server **116** is connected to a neighborhood database **120**, which will be further described below. CDMA2000 network **140** includes a first base station (BS1) **142**. WiFi network **150** includes a third access point (AP3) **152** and a fourth access point (AP4) **154**. WiMAX network **160**

includes a second base station (BS2) **162** and a third base station (BS3) **164**. CDMA2000 network **170** includes a fourth base station (BS4) **172** and a fifth base station (BS5) **174**. The DHCP server **116** may be hosted by an access point, an access router, or a dedicated server of an access network, for example. In other embodiments, some or all of the other networks **140**, **150**, **160** and **170** also have their own DHCP server, similar to DHCP server **116**.

[0026] The exemplary mobile station **130**, e.g., a mobile telephone, is in communication with the network **110** as shown by paths **180**, **181** and **184** of **FIG. 1**. The DHCP server **116** is in data communication with the neighborhood database **120** as shown by paths **182** and **183**. This communication will be further described in conjunction with **FIG. 2** below.

[0027] In one embodiment, the neighborhood database **120** includes a plurality of fields for each access point or base station in the networks of the system **100**. These fields include a media access control (MAC) address, an operator identifier, a network access server (NAS) identifier, and an Internet protocol identifier (e.g., IPv4, IPv6). Naturally, in other embodiments, the database **120** can contain other fields.

[0028] In a wireless network, an access point is generally a station that transmits and receives data to connect users to other users within the network and also can serve as the point of interconnection between the wireless network and a fixed wire network. In a WiFi network embodiment, an example of one or more of the access points **112**, **114**, **152** and **154** can be an Airespace 1200, available from Airespace Inc., an IronPoint, available from Foundry Networks, or an Altitude 300, available from Extreme Networks.

[0029] The mobile station **130** can be referred to as an end terminal or a user device. The mobile station **130** can include, for example, a personal computer (laptop, palm-top), a mobile phone, or other portable communication devices such as a hand-held PC, a wallet PC and a personal digital assistant (PDA).

[0030] Referring to **FIG. 2** (in conjunction with **FIG. 1**), a flowchart of an exemplary process **200** for operating on the exemplary configuration **100** shown in **FIG. 1** will be described. Process **200** begins at a start state **202** and proceeds to state **204** where the DHCP server **116** of the current network **110** maintains the database **120** of other networks in its neighborhood. In certain embodiments, the database **120** can be created and updated manually. The neighborhood coverage of the database **120** depends on local policy. For example, the list can contain:

[0031] All networks from the same operator

[0032] The list may be compartmentalized based on geographic locations (e.g., all WiFi APs in the San Francisco Bay area)

[0033] Or, all networks within the same IP subnet of the operator;

[0034] All networks of the operators that are affiliated or have roaming agreements.

[0035] Proceeding to state **206**, the MS hears or receives periodic beacons from one or more networks in the system, such as from the access points or base stations of the

networks. For the sake of simplicity, an access point is to be considered as including both access points and base stations. In certain embodiments, beacon frames are described as part of the IEEE 802.11 wireless network protocol. Each beacon transmission identifies the presence of an access point and includes information regarding the access point for the mobile stations that are within range. The beacon interval is a variable parameter. For example, path **180** shown in **FIG. 1** represents a beacon from AP**1112**. Advancing to state **208**, in certain embodiments, the mobile station (MS) identifies the neighbor networks by their MAC addresses, such as the base station identifier (BSSID) used by IEEE 802.11 access points. The MAC addresses are readily available (e.g., they are used in beacons) once the MS is within the network coverage region. In one embodiment, this identifier is the best one suited for rapid recognition.

[**0036**] At any given time, but shown as state **210** of process **200**, the MS can either request:

[**0037**] Detailed capability/configuration information on all possible networks in its neighborhood (e.g., get all), or

[**0038**] Detailed capability/configuration information on a selected target network (e.g., get one)

[**0039**] It is assumed that the MS has already identified the MAC address of the target network (e.g., by hearing periodic beacons).

The MS can do one of the previous requests depending on usage. For example, if the MS knows it is only interested in one target network, it can “get one”, but if the MS has not decided yet, it may “get all” and make a decision based on the information it gets. For example, the mobile station requests detailed information via path **181** to the DHCP server **116** as shown in **FIG. 1**. In certain embodiments, the MS requests information about more than one target network. The DHCP server provides both configuration and capability information. For example, a MS can configure an IP address by getting one from the DHCP server, or learn that there is a “Mobile IP home agent” capability in the access network by learning the IP address of one.

[**0040**] Continuing at state **212**, the DHCP server in the currently serving network responds to the MS request by requesting data from the neighborhood database **120**. For example, this request is sent via path **182** to the database **120** as shown in **FIG. 1**. Moving to state **214**, the database **120** provides the requested data about the neighbor networks or target network to the DHCP server **116**. For example, the database **120** sends the requested information via path **183** to the server **116** as shown in **FIG. 1**. Advancing to state **216**, the DHCP server responds to the MS through the access point (or base station, depending on the particular network) with the requested information. For example, the server **116** sends the requested information via path **184** to the MS **130** as shown in **FIG. 1**. Proceeding to optional state **218**, the MS connects to a selected network based on the response from the DHCP server. In certain embodiments, the MS includes a network selection mechanism to select the network. In another embodiment, the MS displays the requested information about the neighbor networks or target networks, and a user selects one of the networks. Process **200** completes at an end state **220**.

[**0041**] Referring to **FIG. 3**, the protocol details for an exemplary DHCP request option **300** will be described. This request option **300** can be the request made by the MS in state **210** of process **200** (**FIG. 2**) and sent across path **181** (**FIG. 1**). The request option **300** includes a neighborhood request **310** and an option length **312**. The neighborhood request **310** indicates the type of DHCP request and the option length **312** is the size (in Bytes) of the option, and both are compliant with the standard DHCP option formats as specified in the DHCP references. A target MAC address(es) section **320** is optionally included. If one or more specific targets are not provided, the information of all neighbors is requested. The section **320** includes a MAC type portion and a target network MAC address portion. The MAC type determines the length and format of the MAC address.

[**0042**] Referring to **FIG. 4**, the protocol details for an exemplary DHCP reply option **400** will be described. This reply option **400** can be the reply sent to the MS in state **216** of process **200** (**FIG. 2**) via path **184** (**FIG. 1**). The reply option **400** includes a neighborhood request **410** and an option length **412**. In this example, information sets are provided for two networks, which is associated with the situation when two target networks are specified in the request or there are only two networks in the system. An information set **420** for network **1** and an information set **430** for network **2** are shown. Each information set includes an information length portion and multiple information portions or fields, e.g., five information fields in one embodiment. Each information field has an information type portion **432**, a length portion **434** and a value portion **436**. The information fields are populated with data from the neighborhood database **120** (**FIG. 1**).

Neighborhood Database

[**0043**] Each access point in the neighborhood is entered as a separate “access network” in the neighborhood database **120** (**FIG. 1**). In reality, from a management or configuration perspective, multiple access points may be part of the same “administrated network,” but from a discovery point of view, this does not matter. In certain embodiments, for performance optimizations, some aggregation can be used in order to prevent repeating the same information for multiple elements of the database.

[**0044**] The database **120** may contain both static and dynamic (e.g., network load) information. While static information can be entered manually, there is a separate mechanism to keep the dynamic information up-to-date.

[**0045**] In certain embodiments, the following are the information items retained in the neighborhood database **120** (**FIG. 1**). Note that these items can be supplemented or replaced by other items according to the desired embodiment.

[**0046**] Network ID: The MAC address of the BS/AP (this is the Key of the database)

[**0047**] Associated NAS id, NAS address

[**0048**] Radio type

[**0049**] In the same IP subnet as the current network

[**0050**] IP subnet configuration (prefix, gateway addresses)

- [0051] Operator name/id
- [0052] List of roaming partners
- [0053] IPv4 and/or IPv6 supported
- [0054] Channel identifier
- [0055] Supports fast MIPv4 and/or MIPv6 handovers
- [0056] Network address translations (NATs) present
- [0057] MIPv4 and/or MIPv6 home address (HA) present
- [0058] Current network load
- [0059] Geographic location
- [0060] Quality of service (QoS) characteristics
- [0061] Pre-authentication capability
- [0062] Security capabilities
- [0063] Pricing plan
- [0064] IP multimedia subsystems (IMS) support present
- [0065] List of location based services
- [0066] Virtual private network (VPN) (IPsec passthrough) support

Exemplary Applications

[0067] Various applications can take advantage of this network neighborhood discovery capability. A few exemplary applications are listed as follows.

[0068] Key scoping in 2.3 GHz Wireless Broadband (WiBro) fast handoffs: (WiBro is a Korean standard, Telecommunications Technology Association Project Group 302, and is part of the IEEE 802.16 family of wireless Internet specifications.)

[0069] In order to use the same pairwise master key (PMK), a WiBro MS needs to know if a given BS is managed by a given network access server (NAS). This discovery needs to happen even before the 3-way handshake with the target BS. The NAS ID delivered via DHCP allows a MS to discover the NAS scope.

[0070] Pre-authentication WiBro/WiFi:

[0071] The NAS identifier discovered by the MS is used to run pre-authentication with the target NAS even before the MS is handed over to the target network.

[0072] Pro-active detection of network attachment (DNA):

[0073] The MS can discover which BSs are connected to the same IP subnet as the currently serving one. That way, as soon as it is attached to one of those, it can readily know that its current IP configuration is still valid.

[0074] Reduced scan time:

[0075] By learning the channel information of the target APs, the MS can avoid sequential radio scanning.

[0076] Advanced network selection:

[0077] The rich information gathered about the target networks can be used in an advanced network selection scheme. In the absence of process 200, most of the

network information cannot be gathered without fully connecting to the target networks.

[0078] Pro-active fast mobile IP handovers:

[0079] By knowing the target foreign agent (FA) or access router in advance, the MS can request bi-casting before it handovers to the target network. Bi-casting is associated with a semi-soft handoff where there is communication with both an old and new point of attachment.

Features of Certain Embodiments

[0080] Certain embodiments of the new DHCP process option provide features and advantages not described in prior DHCP options. These features are as follows:

[0081] Currently defined DHCP options provide limited information about only the serving network. Detailed information about the candidate networks is not defined. The new DHCP process option provides detailed information about the candidate networks.

[0082] There is no candidate other than DHCP to provide neighborhood information in a link-layer agnostic way (i.e., All-IP way).

[0083] The new DHCP process option uses a type-length-value (TLV) structure, which allows addition of new attributes as needed.

[0084] New information can be added to the described system design as it become available or needed for a particular application.

Conclusion

[0085] While specific blocks, sections, devices, functions and modules may have been set forth above, a skilled technologist will realize that there are many ways to partition the system, and that there are many parts, components, modules or functions that may be substituted for those listed above.

[0086] While the above description has pointed out novel features of the invention as applied to various embodiments, the skilled person will understand that various omissions, substitutions, and changes in the form and details of the device or process illustrated may be made without departing from the scope of the invention. Therefore, the scope of the invention is defined by the appended claims rather than by the foregoing description. All variations coming within the meaning and range of equivalency of the claims are embraced within their scope.

REFERENCES

- [0087] [1] Droms, R., "Dynamic Host Configuration Protocol," RFC 2131, March 1997.
- [0088] [2] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., Carney, M., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 3315, July 2003.
- [0089] [3] IEEE 802.11k Working Group Draft
- [0090] [4] Koodli, R. (ed), "Fast Handovers for Mobile IPv6," work in progress, October 2004.

What is claimed is:

1. A network having a dynamic host configuration protocol server, comprising:

a dynamic host configuration protocol (DHCP) server embedded in a network being in a neighborhood of identified wireless networks;

a database, in data communication with the DHCP server, configured to store at least media access control (MAC) address of each identified network; and

an access point, in communication with the DHCP server, configured to send beacons to at least one mobile station, wherein each beacon has at least a MAC address of the access point;

wherein the DHCP server receives a request for configuration and capability information of one or more of the identified networks, obtains the requested information from the database, and provides the requested information to a mobile station that requested the information.

2. The network of claim 1, wherein request for configuration and capability information is for all the identified networks in the database.

3. A network discovery method, comprising:

maintaining a database of network identifiers associated with a plurality of networks in a neighborhood of a particular network;

sending beacons from an access point of at least one network identified in the database;

receiving a request for capability and/or configuration information of at least one network identified in the database; and

providing the requested capability and/or configuration information to a mobile station.

4. The method of claim 3, additionally comprising connecting the mobile station to a selected network based on the provided information.

5. The method of claim 4, wherein the connection is with the mobile station via an access point to the selected network.

6. The method of claim 3, wherein the database is maintained by a dynamic host configuration protocol (DHCP) server.

7. The method of claim 6, wherein the providing is performed by the DHCP server.

8. The method of claim 6, wherein the DHCP server is associated with the particular network.

9. The method of claim 6, wherein the DHCP server is associated with the particular network, and wherein at least one of the networks in the neighborhood of the particular network includes its own DHCP server and database.

10. The method of claim 3, wherein the request for capability and/or configuration information comprises a request for capability and/or configuration information of all the networks in the database.

11. The method of claim 3, wherein the beacons are received by the mobile station.

12. The method of claim 11, wherein the mobile station identifies networks by their media access control addresses.

13. The method of claim 3, additionally comprising displaying the provided capability and configuration information to a user of the mobile station.

14. The method of claim 3, wherein the beacons are periodically sent by the access point.

15. A network discovery system, comprising:

means for storing information about identified networks in a neighborhood of a particular network;

means for sending beacons from an access point of at least one network identified in the storing means;

means for receiving a request for capability and/or configuration information of at least one network identified in the storing means; and

means for providing the requested capability and/or configuration information to a mobile station.

16. The system of claim 15, wherein the means for storing information comprises a database.

17. The system of claim 15, wherein the means for storing information comprises a dynamic host configuration protocol (DHCP) server.

18. The system of claim 15, wherein the means for sending beacons additionally comprises means for identifying networks by their media access control addresses.

19. The system of claim 15, wherein the information includes a media access control address.

20. The system of claim 15, wherein the information includes a network operator identifier, a network access server identifier and an Internet protocol identifier.

21. The system of claim 15, wherein the beacons are periodically sent by the access point.

22. A network discovery method, comprising:

storing information about a plurality of networks in a neighborhood of a particular network;

sending beacons from an access point of at least one of the neighborhood networks;

requesting capability and configuration information of at least one network; and

providing the requested capability and configuration information to a mobile station.

23. A network discovery method, comprising:

learning information about one or more access networks within a neighborhood of a mobile host via dynamic host configuration protocol (DHCP).

24. The method of claim 23, additionally comprising learning a configuration and capability of the identified networks by the mobile host.

25. A network discovery method, comprising:

learning a configuration and capability of a given access network via dynamic host configuration protocol (DHCP) by a mobile station.

* * * * *