

METHOD TO CONTROL RADIO DEVICES BASED ON USER ENVIRONMENT POLICY REQUIREMENTS

5

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates in general to the field of information handling
10 systems and more specifically, to automatically enforcing wireless-enabled device
usage policies within a predetermined environment.

Description of the Related Art

As the value and use of information continues to increase, individuals and
businesses seek additional ways to process and store information. One option
15 available to users is information handling systems. An information handling system
generally processes, compiles, stores, and/or communicates information or data for
business, personal, or other purposes thereby allowing users to take advantage of the
value of the information. Because technology and information handling needs and
requirements vary between different users or applications, information handling
20 systems may also vary regarding what information is handled, how the information is
handled, how much information is processed, stored, or communicated, and how
quickly and efficiently the information may be processed, stored, or communicated.
The variations in information handling systems allow for information handling
systems to be general or configured for a specific user or specific use such as financial

transaction processing, airline reservations, enterprise data storage, or global communications. In addition, information handling systems may include a variety of hardware and software components that may be configured to process, store, and communicate information and may include one or more computer systems, data
5 storage systems, and networking systems.

The use of wireless communication devices, including information handling systems configured as portable units, has grown in popularity over the last several years. It is common for a user to carry one or more such devices into a variety of environments, some of which have usage requirements or restrictions pertaining to
10 their acceptable use. For example, commercial airlines require that wireless devices be disabled at certain times. Some devices, such as cell phones and pagers are required to be turned off at all times because they have transmitters that may interfere with navigation equipment. Likewise, wireless-enabled notebook computers are required to be turned off at all times unless the wireless function is disabled.
15 Similarly, users are often asked to silence or turn off their wireless communications devices in business meetings and classrooms, or public places such as movie theaters, religious gatherings and community meetings so others are not disturbed. Wireless device users may also enter restricted areas where photography is prohibited, resulting in being asked to temporarily surrender their cell phone or turn it off if it is enabled
20 with a camera. As a result, the user is inconvenienced when complying with the request as they lose the primary function of the phone due to it happening to possess photographic capabilities.

Currently, there is no automated method of powering down or silencing these devices when required. Nor is there an automated way to disable predetermined device features while retaining other functionalities. Stated another way, usage policies cannot be easily and efficiently put into effect within a given environment.

5 Instead, they have to be manually enforced. For example, airline flight attendants make announcements requesting that passengers either turn their wireless devices off or put them into a required operating mode. However, currently available statistical information indicates that a double-digit percentage of phones and pagers are left on during flights, showing that this solution is not as effective as desired. As another

10 example, posters are displayed, slides are projected, and audio announcements are made requesting that wireless devices be placed in silent mode or turned off in movie theaters and other public venues. But since there is no current way of enforcing these requests, disturbances continue to occur.

At the present time, some manufacturers have attempted to address these

15 issues by incorporating a dedicated switch into their wireless devices that allow a user to disable wireless communication functions so that the device can be used otherwise. In other cases, wireless functionality can be disabled by pressing a predetermined sequence of keys (e.g., Fn-F2). The Consumer Electronics Agency (CEA) has proffered that an icon or other indicator be incorporated into wireless devices to

20 display the status its various functions. These enhancements result in the devices costing more and they have not been widely adopted. While facilitating the disablement of wireless and other device functionalities, these approaches still require manual effort on the part of the user and do not automatically enforce local wireless

device usage policies. Another approach uses power monitoring units (PMUs) to define disabling zones that prevent cell phones from making and/or receiving calls. In this approach, active cell phones are identified by their electronic serial number (ESN), and if located within the disabling zone, their network access is disallowed, thereby
5 preventing incoming or outgoing calls as well as disruptive call tones or ringing. However, the transmitter of the cell phone is not turned off, which can cause interference with other communications and/or navigation equipment in some environments. In view of the foregoing, there is a need for communications and other functionalities of wireless-enabled devices to be controlled such that predetermined
10 usage policies of an environment or venue can be automatically enforced.

SUMMARY OF THE INVENTION

In accordance with the present invention, a system and method is disclosed for automatically enforcing wireless-enabled device usage policies within a predetermined environment.

15 In a first aspect, there is provided a system for controlling operation of wirelessly-enabled devices. The system includes a wireless usage policy manager operable to generate commands for enforcing a plurality of wireless device usage policies, and at least one wirelessly-enabled device operable to execute a wireless policy enforcement application, thereby causing the wirelessly-enabled device to respond to
20 the commands generated by the wireless usage policy manager. The wireless usage

policy manager is operable to override default wireless usage policies of a wireless usage policy domain based on information on the at least one wirelessly-enabled device.

In a second aspect, there is provided a method for controlling operation of wirelessly-enabled devices. The method includes using a wireless usage policy manager to generate commands for enforcing a plurality of wireless device usage policies, and executing a wireless policy enforcement application on at least one wirelessly-enabled device, thereby causing the wirelessly-enabled device to respond to the commands generated by the wireless usage policy manager. The wireless usage policy manager is operable to override default wireless usage policies of a wireless usage policy domain based on information on the at least one wirelessly-enabled device.

In different embodiments of the invention, a wireless usage policy manager enforces predetermined usage policies by automatically disabling or limiting the operation of wireless-enabled devices as they enter the predetermined boundaries of the wireless policy management environment. When the wireless-enabled devices exit the predetermined boundaries of the wireless policy management environment they are automatically restored to their prior operational state without user actions. Wireless-enabled devices include, but are not limited to, cellular phones, portable computers, personal digital assistants (PDAs), pagers and/or similar devices. Wireless-enabled device functionality that can be disabled or limited

by the usage policy manager includes, but is not limited to, power on/off state, communications bands and/or protocols, audible/silent/vibrate 'ring' mode, and/or digital camera operation.

In different embodiments of the invention, additional or extended information elements are implemented with wireless communications protocols known to those of skill in the art, including but not limited to, Global Services for Mobile communication (GSM), General Packet Radio Service (GPRS), Enhanced Data rates for Global Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), Bluetooth, ultra wideband (UWB), IEEE 802.16 (WiMAX) and IEEE 802.11 (WiFi). These information elements are implemented to communicate and/or enforce predetermined wireless usage policies as wireless devices enter the boundaries of a wireless usage policy domain established by a wireless access point comprising a wireless usage policy manager. The communication and/or enforcement of the additional or extended information elements occurs at the time of handover, when the subject wireless devices switch from their current wireless transmitter connection to the local transmitter of wireless access point comprising the wireless usage policy manager. In an embodiment of the invention, the boundaries of a wireless usage policy domain are formed by the coverage of a wireless access point comprising the wireless usage policy manager. In another embodiment of the invention, the boundaries of a wireless usage policy domain are formed by the coverage of two or more wireless access points comprising wireless usage policy managers that further comprise a common usage policy database. In both embodiments, the location of the wireless access point comprising the wireless usage

policy manager may be fixed (e.g., a movie theater) or mobile (e.g., a commercial airliner that is in-route).

In other embodiments of the invention, extensibility mechanisms in beacons, control fields, probe requests/responses, service discovery algorithms, etc. are

5 implemented without altering existing technology specifications and/or standards.

Furthermore, extension elements can be introduced without changes to the underlying hardware and/or software comprising wireless-enabled devices, allowing rapid

adoption in existing as well as new products. Those of skill in the art will understand that many such embodiments and variations of the invention are possible, including

10 but not limited to those described hereinabove, which are by no means all inclusive.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features and advantages made apparent to those skilled in the art by referencing the accompanying drawings. The use of the same reference number throughout the

15 several figures designates a like or similar element.

Figure 1 is a generalized illustration of an information handling system that can be used to implement the method and system of the present invention;

Figure 2 depicts a wireless communications network that can be used to implement the method and apparatus of the invention;

20 Figure 3 depicts a wireless usage policy enforcement system as implemented in accordance with an embodiment of the invention;

Figure 4 is generalized block diagram of a wireless usage policy negotiation system as implemented in accordance with an embodiment of the invention;

Figure 5 is a generalized flowchart depicting a wireless usage policy enforcement system as implemented in accordance with an embodiment of the invention; and

Figure 6 is a generalized depiction of the flow of information element extensions as implemented in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

A system and method is described for the automatic enforcement of wireless-enabled device usage policies within a predetermined environment. A wireless usage policy manager enforces predetermined usage policies by automatically disabling or limiting the operation of wireless-enabled devices as they enter the predetermined boundaries of the wireless policy management environment. When the wireless-enabled devices exit the predetermined boundaries of the wireless policy management environment they are automatically restored to their prior operational state without user actions.

For purposes of this disclosure, an information handling system may include any instrumentality or aggregate of instrumentalities operable to compute, classify, process, transmit, receive, retrieve, originate, switch, store, display, manifest, detect, record, reproduce, handle, or utilize any form of information, intelligence, or data for business, scientific, control, or other purposes. For example, an information handling system may be a personal computer, a network storage device, or any other suitable

device and may vary in size, shape, performance, functionality, and price. The information handling system may include random access memory (RAM), one or more processing resources such as a central processing unit (CPU) or hardware or software control logic, ROM, and/or other types of nonvolatile memory. Additional components of the information handling system may include one or more disk drives, one or more network ports for communicating with external devices as well as various input and output (I/O) devices, such as a keyboard, a mouse, and a video display. The information handling system may also include one or more buses operable to transmit communications between the various hardware components.

Figure 1 is a generalized illustration of an information handling system 100 that can be used to implement the system and method of the present invention. The information handling system includes a processor (e.g., central processor unit or "CPU") 102, input/output (I/O) devices 104, such as a display, a keyboard, a mouse, and associated controllers, a hard drive or disk storage 106, various other subsystems 108, network port 110 operable to connect to a network 122, and system memory 112, all interconnected via one or more buses 114. Operating system 116 resides in system memory 112 and supports wireless communication application 118, which is utilized in an embodiment of the invention for implementation of wireless usage policy enforcement application 120.

Figure 2 depicts a wireless communications network 200 that can be used to implement the method and system of the invention. Wireless communications network 200 comprises wireless communications cells 202, 204, 206, 208, 210 and 212. In an embodiment of the invention, wireless communications cell 210 further

comprises smaller cells 214, 216, 218, 220, 222, 224 and 230, which may comprise, but are not limited to, small macrocells, microcells, picocells and/or nanocells as are familiar to those of skill in the art.

These smaller cells typically operate on different frequencies and handle the majority of the traffic within cell 210, with gaps in their coverage generally being accommodated by the overall wireless coverage provided by cell 210. Cell types are commonly classified by the location of their typical implementation and the wireless coverage they provide. For example, both large and small macrocells are generally implemented above rooftop location, but large macrocells typically provide 3 to 30 Km coverage while small macrocells provide 1 to 3 Km coverage. Microcells are generally implemented at or below rooftop level and typically provide coverage of 100 meters to 1 Km. Both picocells and nanocells are generally implemented below rooftop level and typically provide 10 meters to 1 Km and 1 meter to ten meters coverage respectively.

Smaller wireless cell 230 further comprises a wireless usage policy domain as described in greater detail hereinbelow. In this depiction of wireless communications network 200, a wireless-enabled device follows path 226 through wireless communications cells 202, 204, 206, 208, 212, and smaller wireless cells 216, 218 of wireless communications cell 210. As the wireless-enabled device traverses path 226, its communications connectivity is maintained from cell to cell by a process known to those of skill in the art as a handover, whereby the current cell relinquishes control of the communications session to the assuming cell.

In an embodiment of the invention, a wireless-enabled device follows path 228 through wireless communications cells 202, 206, and smaller wireless cell 214 of wireless communications cell 210 before entering smaller wireless cell 230, which further comprises a wireless usage policy domain as described in greater detail hereinbelow. As the wireless-enabled device enters the wireless usage policy domain comprising smaller wireless cell 230, control of its communications and associated capabilities are relinquished in a handover process described in greater detail hereinbelow. In this same and other embodiments of the invention, adherence to wireless usage policies is enforced for as long as the device is within the coverage area of the wireless usage policy domain 230. However, as the wireless-enabled device leaves the coverage area of the wireless usage policy domain 230 it is returned to its prior operational state and control of its communications and associated capabilities are once again relinquished in additional handover processes, first to small wireless cell 218 and then to wireless cell 212.

Figure 3 depicts a wireless usage policy enforcement system 300 as implemented in accordance with an embodiment of the invention. In this depiction, wireless communications network 306 is coupled to wireline communications network 308, and comprises one or more base transceiver systems (BTS) 304, which provide wireless communications connectivity to wireless devices 302 comprising usage policy enforcement application 120. Wireless usage policy domain 310 comprises wireless access point 312, which further comprises wireless usage policy manager 314 and wireless usage policies 316. In an embodiment of the invention, wireless usage policies 316 are stored locally in wireless access point 312. In another

embodiment of the invention, wireless usage policies 316 are stored on a remote host and accessed by wireless usage policy manager 314 through wireless connectivity through base transceiver systems (BTS) 304 and then through wireless communications network 306 or through wireline communications network 308. In yet another embodiment of the invention, wireless usage policies 316 and wireless usage policy manager 314 are both implemented on a remote host and accessed by wireless access point 312 through wireless connectivity through base transceiver systems (BTS) 304 and then through wireless communications network 306 or through wireline communications network 308.

As wireless devices 302, comprising usage policy enforcement application 120, enter wireless usage policy domain 310, their presence is detected using prior art methods familiar to those of skill in the art and control of their respective wireless communication connectivity is transferred as a handover from base transceiver system 304 to wireless access point 312. At the time of handover, wireless usage policy manager 314 communicates wireless usage policies 316 to wireless devices 302 through a series of exchanges that include extensions to information elements, described in greater detail hereinbelow. These information element extensions are implementable to enforce wireless usage policies 316 by controlling the required wireless communication and/or associated functionalities comprising wireless devices 302. In an embodiment of the invention, usage policy enforcement application 120 implements information element extensions to enforce wireless usage policies 316 by controlling the required wireless communication and/or associated functionalities referenced by the information element extensions. In another embodiment of the

invention, the operating system or other software code (e.g., operating system, communication application, etc.) comprising wireless devices 302 similarly implements information element extensions to enforce wireless usage policies 316.

In an embodiment of the invention, wireless connectivity, as allowed by
5 wireless usage policies 316, is maintained through a wireless link between wireless access point 312 and base transceiver system 304, which is coupled to wireless communications network 306, which in turn is coupled to wireline communications network 308. In another embodiment of the invention, wireless connectivity as allowed by wireless usage policies 316, is maintained through a wireline link between
10 wireless access point 312 and wireline communications network 308.

Figure 4 is generalized block diagram of a wireless usage policy negotiation system 400 as implemented in accordance with an embodiment of the invention to negotiate the enforcement of wireless usage policies 316 within wireless usage policy domain 310 as it relates to predetermined wireless devices 302. In this diagram,
15 wireless communication network 306 comprises gateway mobile switching center (GMSC) 'A' 402, mobile switching center (MSC) 'A' 404, base station controller (BSC) 'A' 406, and base transceiver system (BTS) 304. Mobile switching center (MSC) 'A' 404 further comprises home location register (HLR) 'A' 408, visitor location register (VLR) 'A' 410, and usage policy repository 'A' 412. In this same
20 diagram, wireless usage policy domain 310 comprises gateway mobile switching center (GMSC) 'B' 414, mobile switching center (MSC) 'B' 416, base station controller (BSC) 'B' 418, and wireless access point 312, further comprising wireless usage policy manager 314. Mobile switching center (MSC) 'B' 416 further comprises

home location register (HLR) 'B' 420, visitor location register (VLR) 'B' 422, and usage policy repository 'B' 424.

Gateway mobile switching center (GSMC) 'A' 402 communicates with GSMC 'B' 414 to determine whether wireless devices 302 are currently located within the coverage area of MSC 'A' 404 or MSC 'B' 416. Mobile switching center (MSC) 'A' 404 and MSC 'B' 416 provide circuit-switched calling and mobility management to wireless devices 302 roaming within their respective coverage areas. Home location register (HLR) 'A' 408 and HLR 'B' 420, respectively comprising MSC 'A' 404 and MSC 'B' 416, are persistent databases that contain details of each wireless device subscribed to their associated wireless networks and their current location. Conversely, visitor location register (VLR) 'A' 406 and VLR 'B' 422, also respectively comprising MSC 'A' 404 and MSC 'B' 416, are temporary databases that contain details of each wireless device that has roamed into their associated wireless network coverage area. Data stored in VLR 'A' 406 and VLR 'B' 422 is respectively obtained from HLR 'B' 420 or HLR 'A' 404, or it is collected from wireless devices 302. In an embodiment of the invention, the functionality of GSMC 'A' 402 is integrated with MSC 'A' 404 and the functionality of GSMC 'B' 420 is integrated with MSC 'B' 416. In another embodiment of the invention, the functionality of VLR 'A' 410 is likewise integrated with MSC 'A' 404 and the functionality of VLR 'B' 422 is likewise integrated with MSC 'B' 416. In yet another embodiment of the invention, the functionality of GSMC 'A' 402 and GSMC 'B' 420 and the functionality of VLR 'A' 410 and VLR 'B' 422 are respectively integrated with MSC 'A' 404 and MSC 'B' 416. HLR 'A' 408 and HLR 'B' 420 are generally

implemented on a remote host, and are typically queried by MSC 'B' 416 and MSC 'A' 404 at the time of handover to respectively populate their associated VLR databases 422, 410 with additional details regarding wireless devices 302 that are roaming in their coverage areas.

5 In an embodiment of the invention, usage policy repository 'A' 412 stores user profile information that is cross-referenced to data stored in HLR 'A' 408, which is associated with wireless devices 302 that are subscribed to wireless communications network 306. In the same embodiment of the invention, usage policy repository 'B' 316 stores wireless usage policy information associated with wireless usage policy
10 domain 310 as well as user profile information that is cross-referenced to data stored in HLR 'B' 422, which is likewise associated with wireless devices 302 that are subscribed to the wireless communications network comprising wireless usage policy domain 310. As wireless devices 302 enter wireless usage policy domain 310, identification information is collected by MSC 'B' 416 and compared to data stored in
15 HLR 'B' 420. If a match is not found, identification information collected from wireless devices 302 is added to VLR 'B' 422 and MSC 'B' 416 queries MSC 'A' 404 for additional information from HLR 'A' 408 and usage policy repository 'A' 412. Additional information retrieved from HLR 'A' 408 is then added to VLR 'B' 422 and information retrieved from usage policy repository 'A' 412 is compared to
20 wireless usage policy information residing in usage policy repository 'B' 316. Wireless usage policy information from usage policy repository 'B' 316 is then modified as appropriate and communicated by wireless usage policy manager 314 at time of handover, via information element extensions, to wireless usage policy

enforcement application 120 or other software code comprising wireless devices 302 for enforcement as described in greater detail hereinabove.

As an example, MSC 'B' 416 collects information from a wireless device 302 as it enters wireless usage domain 310 and queries MSC 'A' 404 to retrieve
5 information stored on HLR 'A' 408 and usage policy repository 'A' 412. The information retrieved from usage policy repository 'A' 412 indicates that the wireless device 302 is assigned to a law enforcement official, and due to security concerns, the wireless device should always be active, audible, and capable of receiving and transmitting voice calls. The default wireless usage policy stored in usage policy
10 repository 'B' 316 for wireless usage policy domain 310 allows inaudible notification of receipt of voicemails and interactive text messaging, but does not allow audible notification of incoming calls, nor does it allow receiving or transmitting of voice calls. In addition, use of digital camera functionality within a wireless device is likewise not allowed. In this example, since wireless device 302 is associated with
15 wireless usage policy overrides, the wireless usage policy retrieved from usage policy repository 'B' 316 is first modified to allow inaudible notification of receipt of voicemails, interactive text messaging, and receipt and transmission of voice calls. However, the use of digital camera functionality within wireless device 302 is not allowed as the policy overrides received from usage repository 'A' 412 is not
20 applicable. The resulting, modified wireless usage policies are then communicated by wireless usage policy manager 314 at time of handover, via information element extensions, to wireless usage policy enforcement application 120 or other software code comprising wireless devices 302 for enforcement.

Figure 5 is a generalized flowchart depicting a wireless usage policy enforcement system as implemented in accordance with an embodiment of the invention. In Step 502, a wireless device enters a wireless usage policy domain, as described in greater detail hereinabove, and related information details about the wireless device are collected in Step 504 by the mobile switching center (MSC) associated with the wireless network comprising the wireless usage policy domain. In an embodiment of the invention, the wireless usage policy domain is a smaller cell of the same wireless network and shares the same MSC, and while the wireless device may not be considered to be roaming by the MSC, it is still subject to wireless usage policies associated with the coverage of the smaller cell. In another embodiment of the invention, the wireless device is roaming from another wireless network and the MSC is different. In a different embodiment of the invention, MSC functionality is implemented in a wireless usage policy domain to create a virtual private wireless network and any wireless device within its area of coverage is treated as a roaming device.

Once additional details about the wireless device are collected in Step 504, the MSC associated with the wireless usage policy domain checks its associated home location register (HLR) in Step 506 to determine in Step 508 whether the wireless device is subscribed to its associated wireless network. If it is determined in Step 508 that the wireless device is subscribed to its associated network, the MSC retrieves additional detail information in Step 510 from its associated HLR and usage policy data from its associated wireless usage policy register as described in greater detail hereinabove. If it is determined in Step 508 that the wireless device is not subscribed

to its associated network, the MSC registers the wireless device in its visitor location register (VLR) in Step 512 and queries the wireless device's wireless network provider MSC in Step 514 to collect additional detail information from its associated HLR and usage policy data from its associated wireless usage policy register.

5 Retrieved detail information is then used in Step 516 by the MSC associated with the wireless usage policy domain to further populate its associated VLR as appropriate, and the retrieved usage policy data is conveyed to a wireless usage policy manager with the default wireless usage policies of the wireless usage policy domain for comparison.

10 If it is determined in Step 518 that the usage policy data retrieved in Step 510 or Step 514 requires overriding the default wireless usage policies of the wireless usage policy domain, then the wireless usage policy manager determines in Step 520 whether to allow the override to be implemented. If it is decided in Step 520 to override the default wireless usage policies of the wireless usage policy domain, then
15 the overrides are applied in Step 522 and communicated to the wireless device in Step 524 using information element extensions as described in greater detail hereinbelow. Otherwise, the default wireless usage policies of the wireless usage policy domain are communicated to the wireless device in Step 524 using information element extensions as described in greater detail hereinbelow. If the communicated
20 information element extensions are accepted by the wireless device and successfully implemented by a wireless usage policy enforcement application in Step 526, then it is determined in Step 534 whether the wireless device is leaving the coverage area of the wireless usage policy domain. If it is, appropriate information element extensions

are communicated to the wireless device by the wireless usage policy manager and are implemented in Step 538 by the wireless usage policy enforcement application to restore itself to its previous operational state and it is then handed over to the receiving MSC. Otherwise, the wireless usage policy manager communicates

5 appropriate information element extensions in Step 524 and the process continues. If the communicated information element extensions are accepted by the wireless device and but are not successfully implemented by a wireless usage policy enforcement application in Step 526, then it is determined in Step 528 whether they are successfully implemented by other software code comprising the wireless device.

10 If the information element extensions are successfully implemented in Step 528, then it is determined in Step 534 whether the wireless device is leaving the coverage area of the wireless usage policy domain. If it is, appropriate information element extensions are communicated to the wireless device by the wireless usage policy manager and are implemented in Step 538 by the other software code

15 comprising the wireless device to restore itself to its previous operational state and it is then handed over to the receiving MSC. Otherwise, the wireless usage policy manager communicates appropriate information element extensions in Step 524 and the process continues. If the communicated information element extensions are not accepted by the wireless device and are not successfully implemented in Step 526 or

20 Step 528, then the wireless usage policy manager uses information element extensions to transmit a notification of the wireless usage policies to the wireless device in Step 530 with acknowledgement of receipt of the message requested via user action in Step 532. If receipt of the notification is not acknowledged by the wireless device user in

Step 532, then the notification is retransmitted in Step 530 by the wireless usage policy manager at predetermined intervals until acknowledgement is received. In an embodiment of the invention, the wireless usage policy notification is sent as a text message to the wireless device. In another embodiment of the invention, the wireless
5 usage policy notification is sent as a prerecorded voice message to the wireless device. If it is then determined in Step 534 that the wireless device is leaving the coverage area of the wireless usage policy domain, the wireless device user is manually notified in Step 536 to restore the wireless device to its previous operational state and it is then handed over to the receiving MSC in Step 538.

10 Figure 6 is a generalized depiction of the flow of information element extensions as implemented in accordance with an embodiment of the invention. In this depiction, wireless-enabled device 302 receives handover trigger 602, such as but not limited to, quality of service (QoS) decreasing below a predetermined level, which results in the initiation of mode negotiations 604 with wireless access point 312.
15 Mode negotiation 604 with wireless access point 312 triggers a wireless usage policy request 604 from wireless usage policy manager 314 which downloads wireless usage policies 608 to wireless access point 312, which then checks device modes 610 of wireless-enabled device 302. Once wireless device modes have been checked by wireless access point 312, appropriate information elements 612 with extensions
20 containing wireless usage parameters and controls are communicated to wireless-enabled device 302 and are then applied 614. In an embodiment of the invention, IEEE 802.21 information elements for operator/user policies are extended and communicated to wireless-enabled device 302 for implementation by a wireless usage

policy enforcement application. In another embodiment of the invention, IEEE
802.21 information elements for operator/user policies are extended and
communicated to wireless-enabled device 302 for implementation by other software
code comprising wireless-enabled device 302. In other embodiments of the invention,
5 existing information elements comprising prior art wireless communication protocols
are either appended or extended for enforcement of predetermined wireless usage
policies and implemented in wireless-enabled device 302 using methods familiar to
those of skill in the art.

Once wireless usage parameters and controls are communicated to wireless-
10 enabled device 302 and are applied 614, acknowledgement of their successful
implementation 616 is conveyed to wireless access point 312, which then confirms
their implementation 618 such that a handover decision 620 can be made by wireless-
enabled device 302. Wireless-enabled device 302 then initiates a handover request
622 to wireless access point 312, which in turn initiates handover processes 624,
15 which are performed 626 in wireless access point 312. Once handover processes are
performed 626 on wireless-enabled device 302, confirmation 628 is conveyed to
wireless access point 312, which completes the handover 630. Once handover is
completed, wireless access point 312 maintains the wireless connection and monitors
wireless-enabled device 312 to ensure that wireless usage policies are enforced.
20 Skilled practitioners in the art will recognize that many other embodiments and
variations of the present invention are possible. In addition, each of the referenced
components in this embodiment of the invention may be comprised of a plurality of
components, each interacting with the other in a distributed environment.

Furthermore, other embodiments of the invention may expand on the referenced embodiment to extend the scale and reach of the system's implementation.

WHAT IS CLAIMED IS:

1. A system for controlling operation of wirelessly-enabled devices,
comprising:
 - 5 a wireless usage policy manager operable to generate commands for enforcing a plurality of wireless device usage policies;
at least one wirelessly-enabled device operable to execute a wireless policy enforcement application, thereby causing said wirelessly-enabled device to respond to said commands generated by said wireless usage policy manager,
 - 10 wherein said wireless usage policy manager is operable to override default wireless usage policies of a wireless usage policy domain based on information on the at least one wirelessly-enabled device.
2. The system of claim 1, wherein said wireless usage policy manager is at
15 a fixed location.
3. The system of claim 1, wherein said wireless usage policy manager is mobile.
- 20 4. The system of claim 1, wherein said wireless usage policy manager is implemented using a single wireless access point defining said wireless usage policy domain.
- 25 5. The system of claim 1, wherein said wireless usage policy manager is implemented using a plurality of wireless access points defining said wireless usage policy domain.
6. The system of claim 5, wherein individual wireless access points in said plurality of wireless access points are operable to enforce said wireless usage policies as
30 said wireless device moves within said wireless usage policy domain.

7. The system of claim 1, wherein wireless usage policy manager is operable to generate commands to automatically enforce said wireless usage policies when said wireless device enters said wireless usage policy domain.

5 8. The system of claim 1, wherein said wireless usage policy manager is operable to automatically terminate said wireless usage policies when said wireless device leaves said wireless usage policy domain.

9. The system of claim 1, wherein said wireless usage policy manager is
10 operable to execute a discovery application to detect wireless devices subject to predetermined usage policies within said wireless usage policy domain.

10. A method for controlling operation of wirelessly-enabled devices, comprising:
15 using a wireless usage policy manager to generate commands for enforcing a plurality of wireless device usage policies;
executing a wireless policy enforcement application on at least one wirelessly-enabled device, thereby causing said wirelessly-enabled device to respond to said commands generated by said wireless usage policy manager,
20 wherein said wireless usage policy manager is operable to override default wireless usage policies of a wireless usage policy domain based on information on the at least one wirelessly-enabled device.

11. The method of claim 10, wherein said wireless usage policy manager is
25 at a fixed location.

12. The method of claim 10, wherein said wireless usage policy manager is mobile.

30 13. The method of claim 10, wherein said wireless usage policy manager is implemented using a single wireless access point defining said wireless usage policy domain.

14. The method of claim 10, wherein said wireless usage policy manager is implemented using a plurality of wireless access points defining said wireless usage policy domain.

5 15. The method of claim 14, wherein individual wireless access points in said plurality of wireless access points are operable to enforce said wireless usage policies as said wireless device moves within said wireless usage policy domain.

10 16. The method of claim 10, wherein said wireless usage policy manager is operable to generate commands to automatically enforce said wireless usage policies when said wireless device enters said wireless usage policy domain.

15 17. The method of claim 10, wherein said wireless usage policy manager is operable to automatically terminate said wireless usage policies when said wireless device leaves said wireless usage policy domain.

18. The method of claim 10, wherein said wireless usage policy manager is operable to execute a discovery application to detect wireless devices subject to predetermined usage policies within said wireless usage policy domain.

20