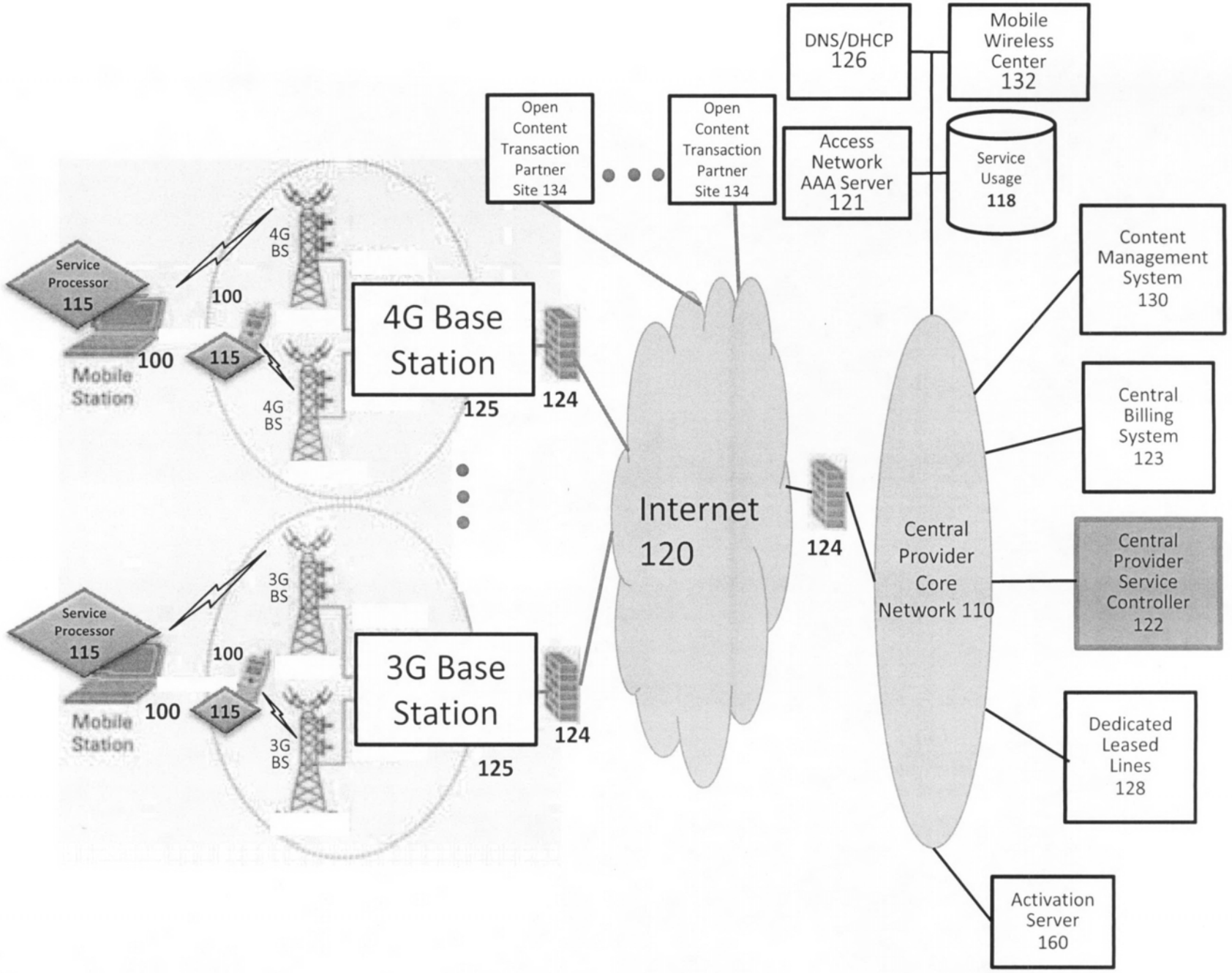

DNS/DHCP
126
Mobile
Wireless
Center
132
Open
Content
Transaction
Partner
Site 134
Open
Content
Transaction
Partner
Site 134
Access
Network
AAA Server
121
Service
Usage
118
Content
Management
System
130
Service
Processor
115
4G
BS
100
100
115
Mobile
Station
4G
BS
4G Base
Station
125
124
Central
Billing
System
123
Internet
120
124
Central
Provider
Core
Network 110
Central
Provider
Service
Controller
122
Service
Processor
115
3G
BS
100
100
115
Mobile
Station
3G
BS
3G Base
Station
125
124
Dedicated
Leased
Lines
128
Activation
Server
160

Figure 1

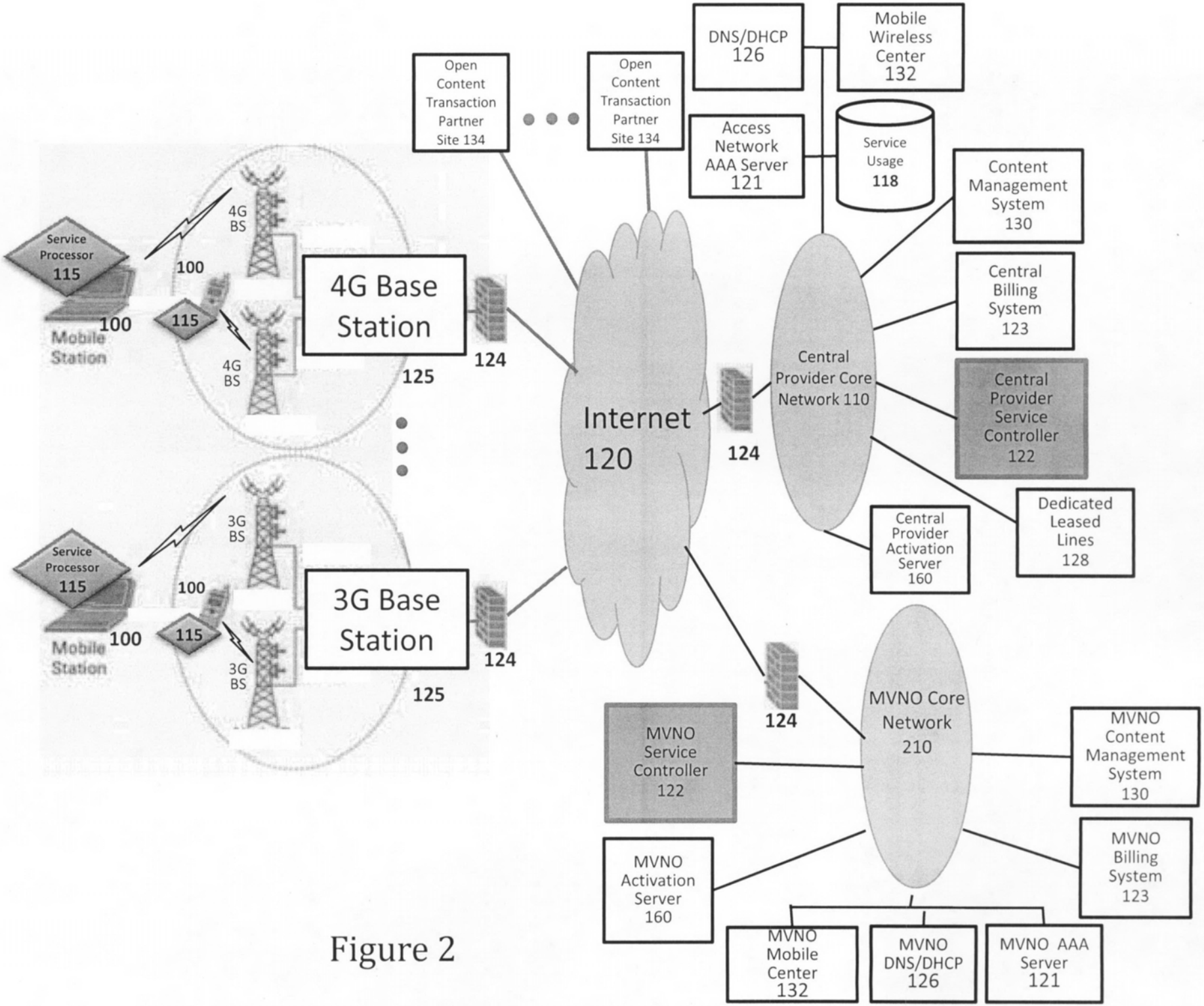

Open Content Transaction Partner Site 134
Open Content Transaction Partner Site 134
DNS/DHCP 126
Mobile Wireless Center 132
Access Network AAA Server 121
Service Usage 118
Content Management System 130
Central Billing System 123
Central Provider Service Controller 122
Dedicated Leased Lines 128
Central Provider Activation Server 160
Central Provider Core Network 110
Internet 120
124
125
4G Base Station
3G Base Station
4G BS
3G BS
Service Processor 115
Mobile Station
100
115
MVNO Core Network 210
MVNO Service Controller 122
MVNO Content Management System 130
MVNO Billing System 123
MVNO Activation Server 160
MVNO Mobile Center 132
MVNO DNS/DHCP 126
MVNO AAA Server 121

Figure 2

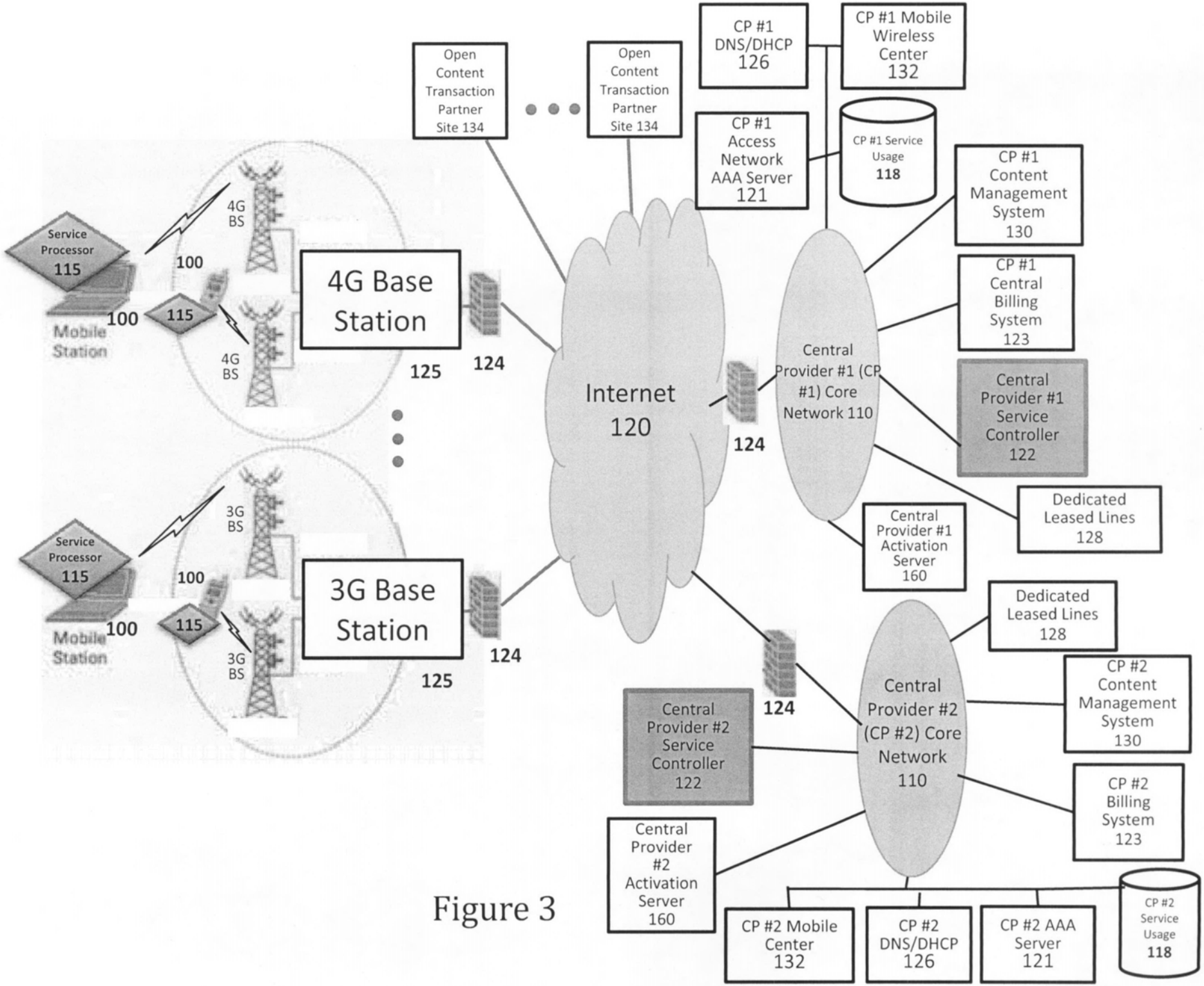

Open Content Transaction Partner Site 134
Open Content Transaction Partner Site 134
CP #1 DNS/DHCP 126
CP #1 Mobile Wireless Center 132
CP #1 Access Network AAA Server 121
CP #1 Service Usage 118
CP #1 Content Management System 130
CP #1 Central Billing System 123
Central Provider #1 Service Controller 122
Dedicated Leased Lines 128
Central Provider #1 Activation Server 160
Central Provider #1 (CP #1) Core Network 110
Internet 120
4G Base Station
125
124
4G BS
Service Processor 115
100
Mobile Station
3G Base Station
3G BS
Central Provider #2 Service Controller 122
Central Provider #2 (CP #2) Core Network 110
CP #2 Content Management System 130
CP #2 Billing System 123
Central Provider #2 Activation Server 160
CP #2 Mobile Center 132
CP #2 DNS/DHCP 126
CP #2 AAA Server 121
CP #2 Service Usage 118

Figure 3

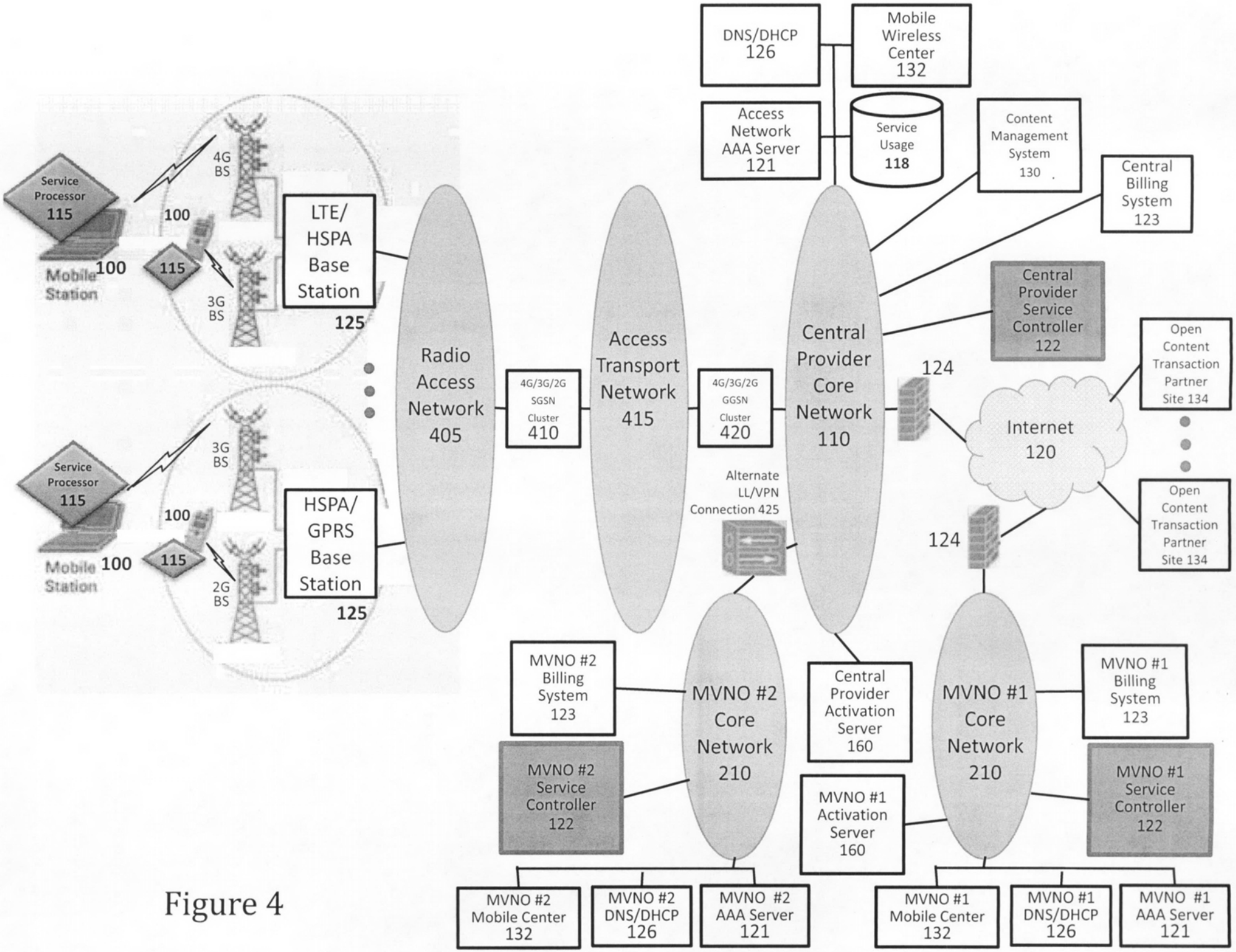

DNS/DHCP 126
Mobile Wireless Center 132
Access Network AAA Server 121
Service Usage 118
Content Management System 130
Central Billing System 123
Central Provider Service Controller 122
Service Processor 115
100
4G BS
LTE/ HSPA Base Station 125
Mobile Station 100
115
3G BS
Radio Access Network 405
4G/3G/2G SGSN Cluster 410
Access Transport Network 415
4G/3G/2G GGSN Cluster 420
Central Provider Core Network 110
124
Internet 120
Open Content Transaction Partner Site 134
Service Processor 115
100
3G BS
HSPA/ GPRS Base Station 125
Mobile Station 100
115
2G BS
Alternate LL/VPN Connection 425
124
MVNO #2 Billing System 123
MVNO #2 Core Network 210
Central Provider Activation Server 160
MVNO #1 Core Network 210
MVNO #1 Billing System 123
MVNO #2 Service Controller 122
MVNO #1 Activation Server 160
MVNO #1 Service Controller 122
MVNO #2 Mobile Center 132
MVNO #2 DNS/DHCP 126
MVNO #2 AAA Server 121
MVNO #1 Mobile Center 132
MVNO #1 DNS/DHCP 126
MVNO #1 AAA Server 121

Figure 4

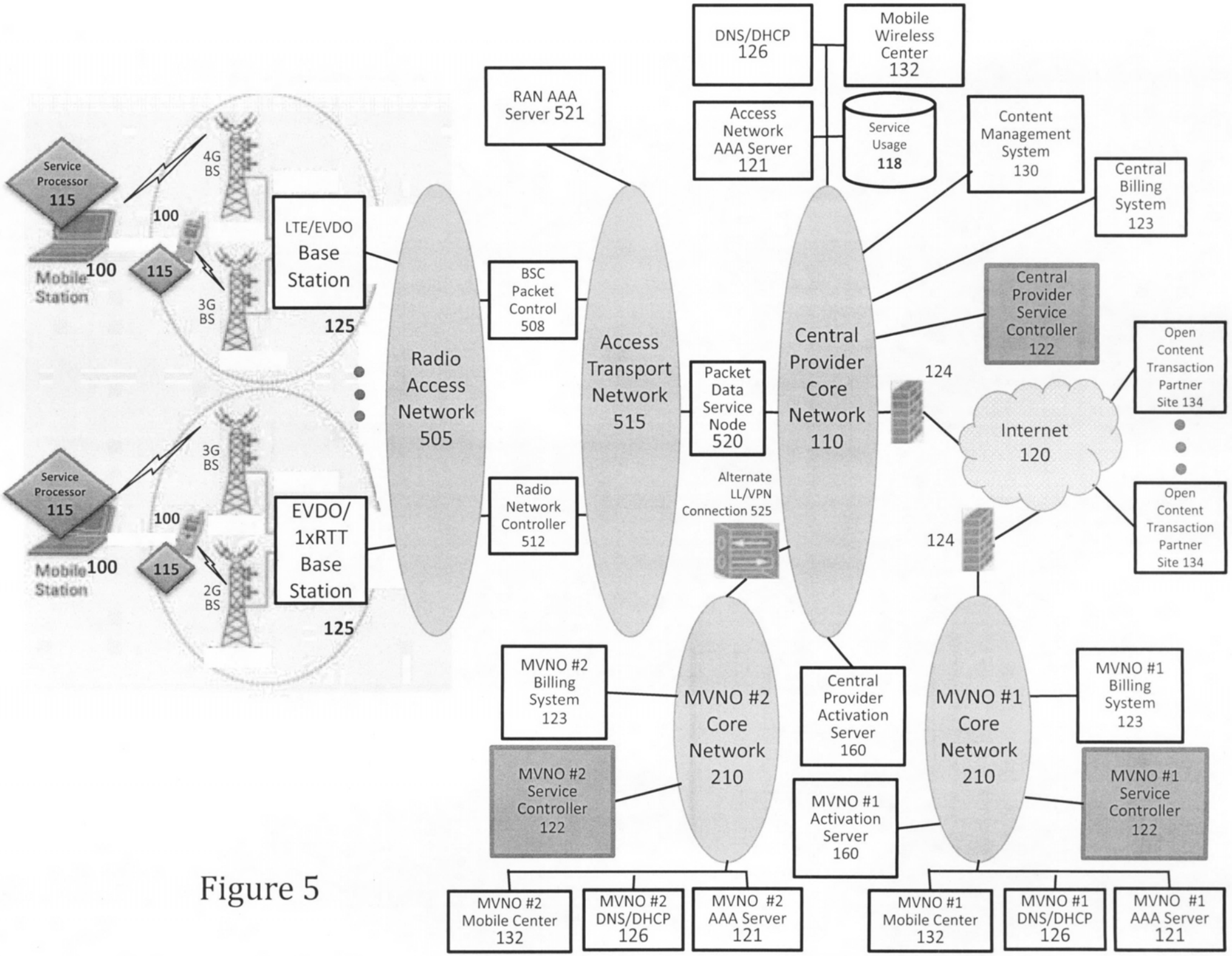

Service Processor 115
4G BS
100
Mobile Station 100
115
3G BS
LTE/EVDO Base Station 125
Service Processor 115
3G BS
100
Mobile Station 100
115
2G BS
EVDO/ 1xRTT Base Station 125
Radio Access Network 505
RAN AAA Server 521
BSC Packet Control 508
Radio Network Controller 512
Access Transport Network 515
Packet Data Service Node 520
Alternate LL/VPN Connection 525
Central Provider Core Network 110
DNS/DHCP 126
Mobile Wireless Center 132
Access Network AAA Server 121
Service Usage 118
Content Management System 130
Central Billing System 123
Central Provider Service Controller 122
124
Internet 120
Open Content Transaction Partner Site 134
Open Content Transaction Partner Site 134
124
MVNO #2 Billing System 123
MVNO #2 Service Controller 122
MVNO #2 Core Network 210
Central Provider Activation Server 160
MVNO #1 Activation Server 160
MVNO #1 Core Network 210
MVNO #1 Billing System 123
MVNO #1 Service Controller 122
MVNO #2 Mobile Center 132
MVNO #2 DNS/DHCP 126
MVNO #2 AAA Server 121
MVNO #1 Mobile Center 132
MVNO #1 DNS/DHCP 126
MVNO #1 AAA Server 121

Figure 5

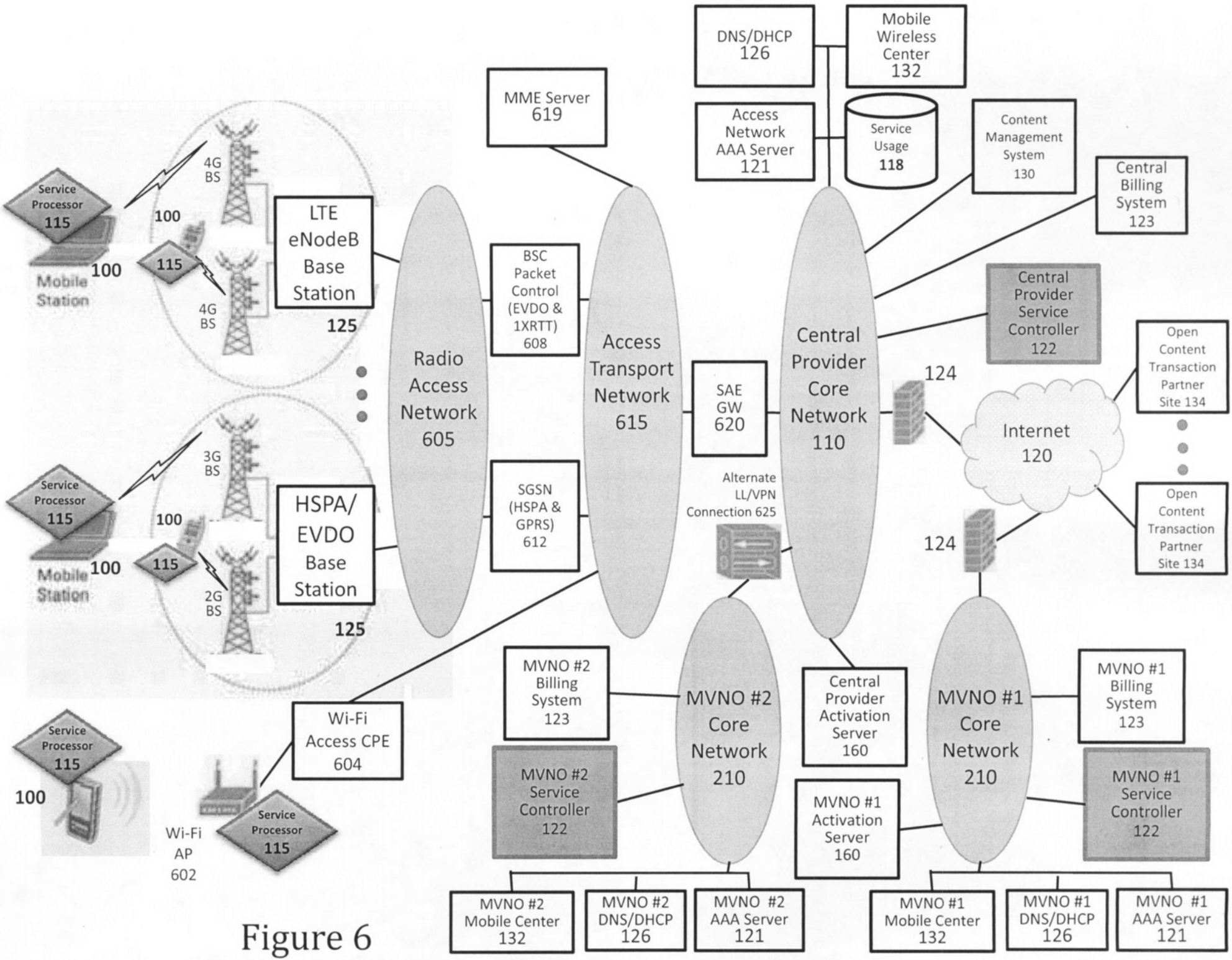

DNS/DHCP 126
Mobile Wireless Center 132
MME Server 619
Access Network AAA Server 121
Service Usage 118
Content Management System 130
Central Billing System 123
Service Processor 115
100
4G BS
LTE eNodeB Base Station 125
BSC Packet Control (EVDO & 1XRTT) 608
Radio Access Network 605
Access Transport Network 615
SAE GW 620
Central Provider Core Network 110
Central Provider Service Controller 122
Mobile Station
3G BS
HSPA/ EVDO Base Station 125
SGSN (HSPA & GPRS) 612
2G BS
Alternate LL/VPN Connection 625
124
Internet 120
Open Content Transaction Partner Site 134
Wi-Fi Access CPE 604
Wi-Fi AP 602
MVNO #2 Billing System 123
MVNO #2 Core Network 210
Central Provider Activation Server 160
MVNO #1 Core Network 210
MVNO #1 Billing System 123
MVNO #2 Service Controller 122
MVNO #1 Activation Server 160
MVNO #1 Service Controller 122
MVNO #2 Mobile Center 132
MVNO #2 DNS/DHCP 126
MVNO #2 AAA Server 121
MVNO #1 Mobile Center 132
MVNO #1 DNS/DHCP 126
MVNO #1 AAA Server 121

Figure 6

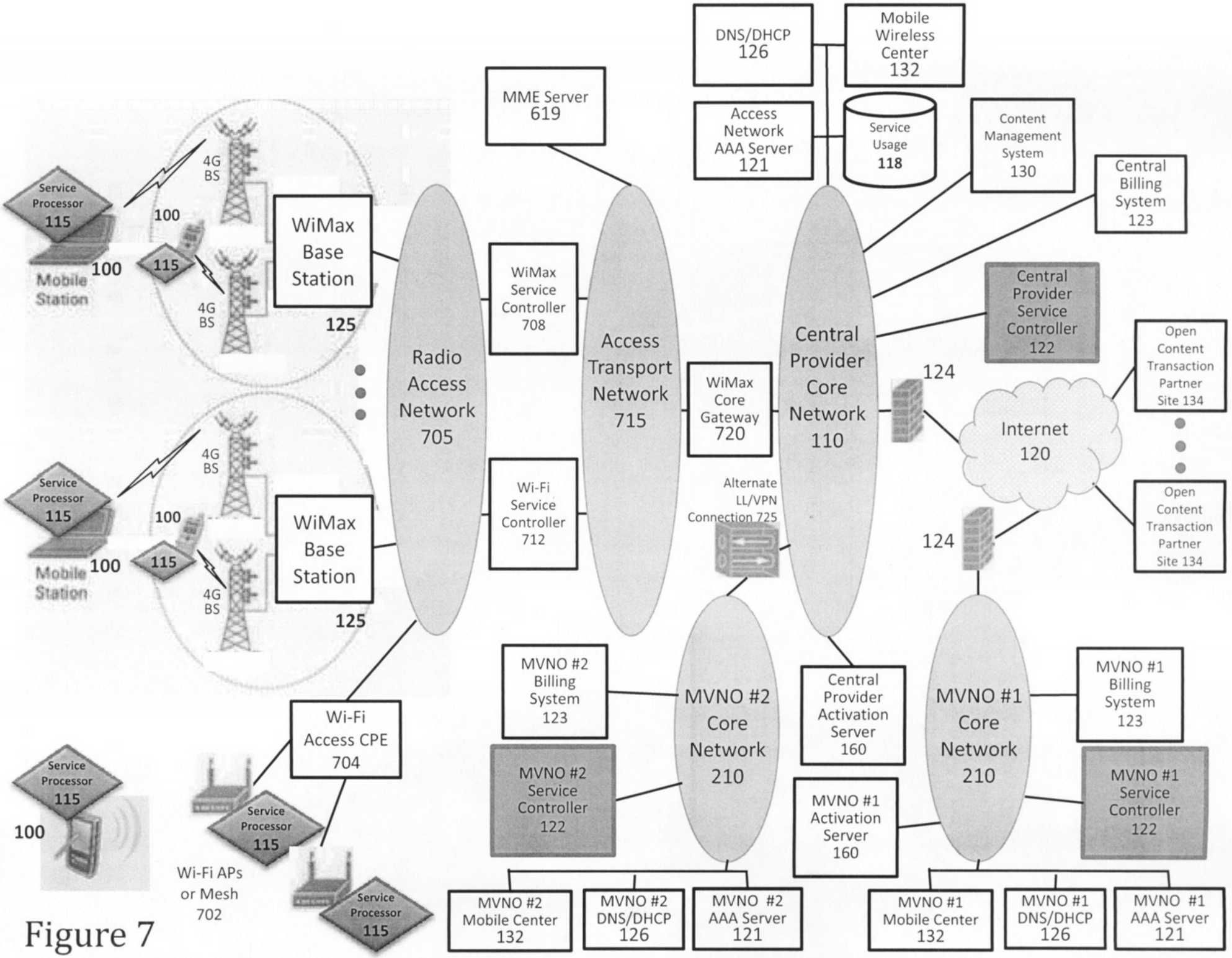

DNS/DHCP 126
Mobile Wireless Center 132
MME Server 619
Access Network AAA Server 121
Service Usage 118
Content Management System 130
Central Billing System 123
Service Processor 115
100
4G BS
WiMax Base Station 125
Mobile Station
WiMax Service Controller 708
Radio Access Network 705
Access Transport Network 715
WiMax Core Gateway 720
Central Provider Core Network 110
Central Provider Service Controller 122
124
Internet 120
Open Content Transaction Partner Site 134
Wi-Fi Service Controller 712
Alternate LL/VPN Connection 725
Wi-Fi Access CPE 704
Wi-Fi APs or Mesh 702
MVNO #2 Billing System 123
MVNO #2 Service Controller 122
MVNO #2 Core Network 210
Central Provider Activation Server 160
MVNO #1 Core Network 210
MVNO #1 Billing System 123
MVNO #1 Service Controller 122
MVNO #1 Activation Server 160
MVNO #2 Mobile Center 132
MVNO #2 DNS/DHCP 126
MVNO #2 AAA Server 121
MVNO #1 Mobile Center 132
MVNO #1 DNS/DHCP 126
MVNO #1 AAA Server 121

Figure 7

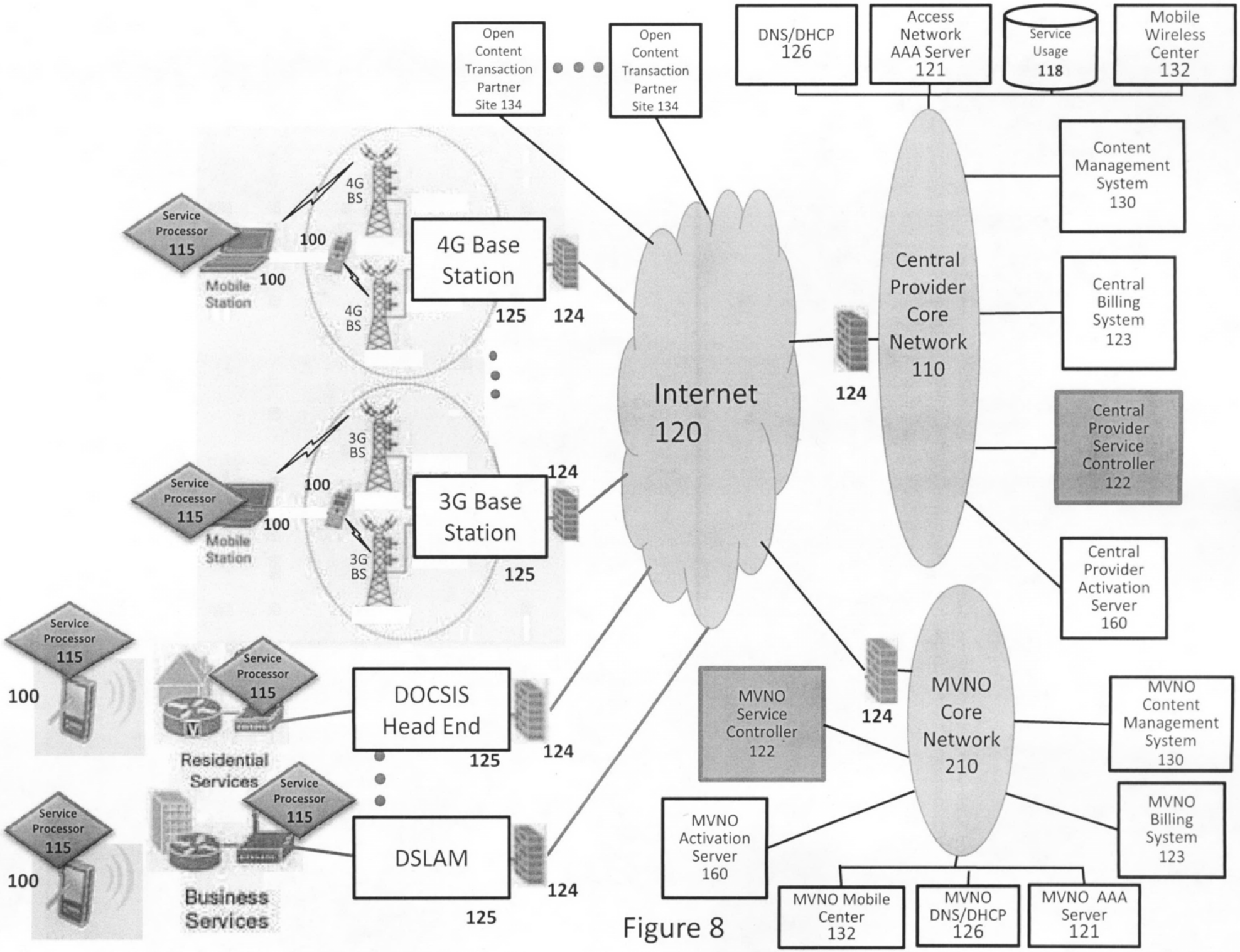

Open Content Transaction Partner Site 134
Open Content Transaction Partner Site 134
DNS/DHCP 126
Access Network AAA Server 121
Service Usage 118
Mobile Wireless Center 132
Content Management System 130
Central Billing System 123
Central Provider Service Controller 122
Central Provider Activation Server 160
Central Provider Core Network 110
Internet 120
4G BS
4G BS
Service Processor 115
100
Mobile Station
4G Base Station
125
124
3G BS
3G BS
3G Base Station
DOCSIS Head End
DSLAM
Residential Services
Business Services
MVNO Service Controller 122
MVNO Core Network 210
MVNO Content Management System 130
MVNO Billing System 123
MVNO Activation Server 160
MVNO Mobile Center 132
MVNO DNS/DHCP 126
MVNO AAA Server 121

Figure 8

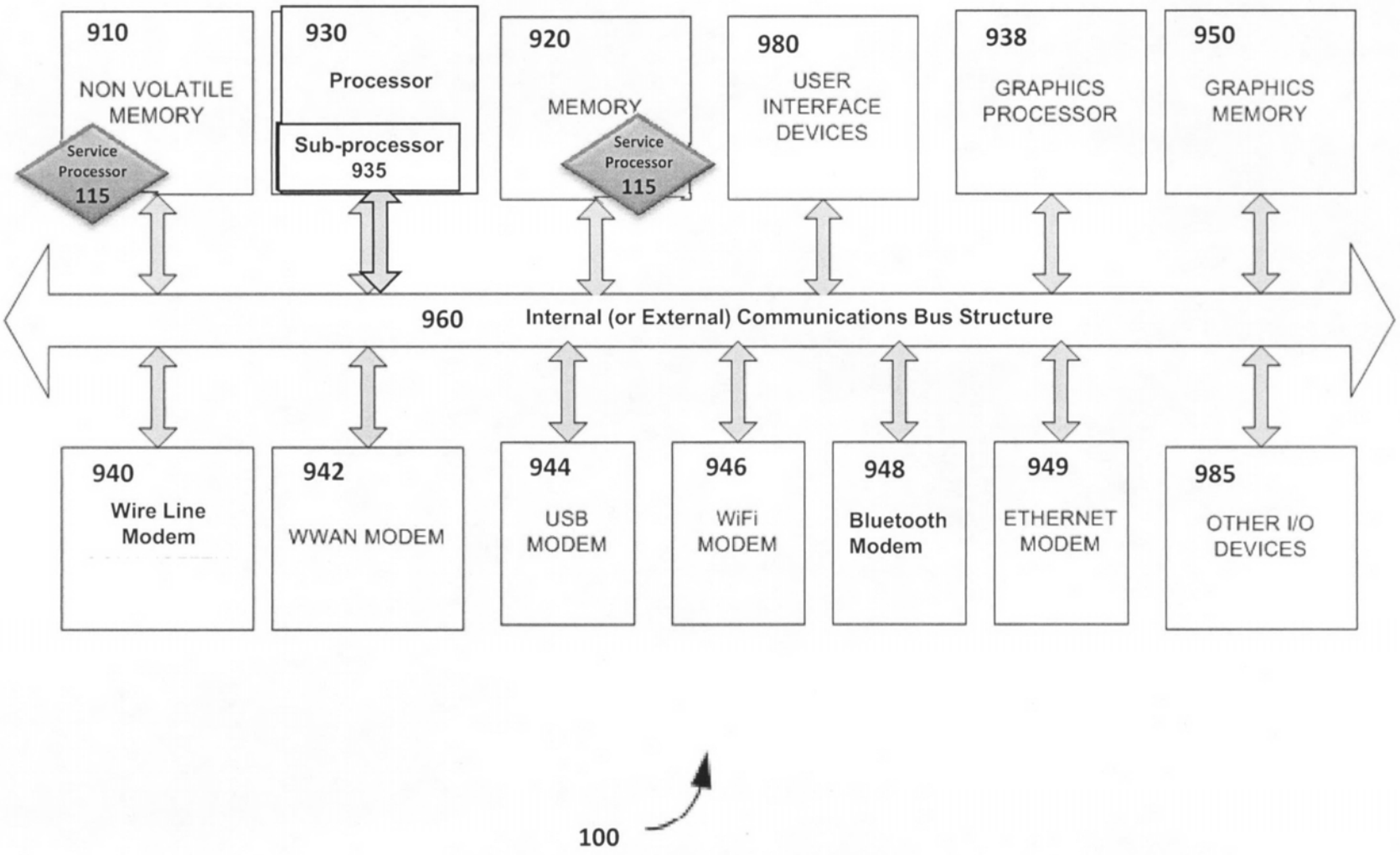

910
NON VOLATILE MEMORY
Service Processor 115
930
Processor
Sub-processor 935
920
MEMORY
Service Processor 115
980
USER INTERFACE DEVICES
938
GRAPHICS PROCESSOR
950
GRAPHICS MEMORY
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN MODEM
944
USB MODEM
946
WiFi MODEM
948
Bluetooth Modem
949
ETHERNET MODEM
985
OTHER I/O DEVICES
100

Figure 9

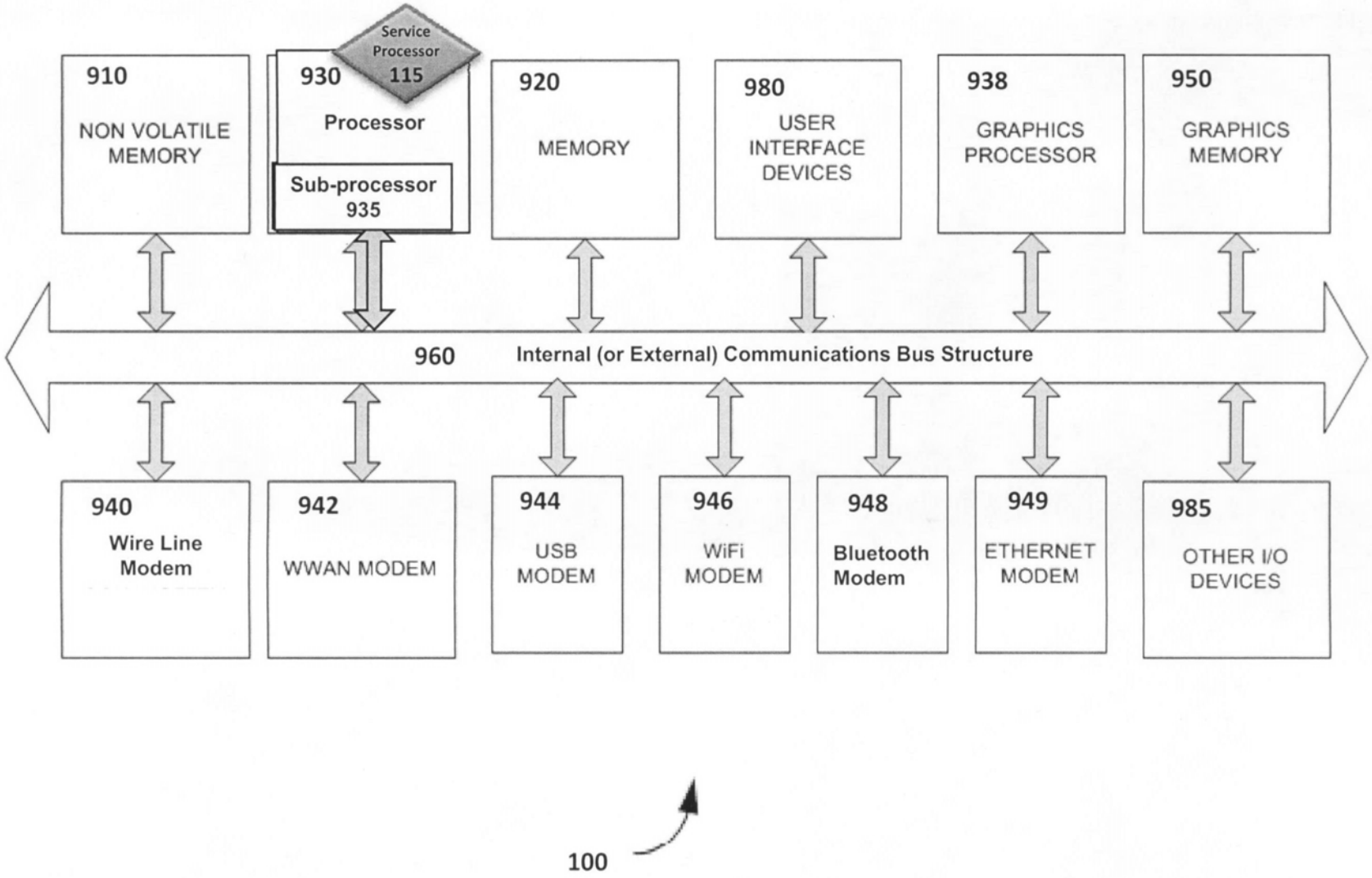

910
NON VOLATILE MEMORY
930
Service Processor 115
Processor
Sub-processor 935
920
MEMORY
980
USER INTERFACE DEVICES
938
GRAPHICS PROCESSOR
950
GRAPHICS MEMORY
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN MODEM
944
USB MODEM
946
WiFi MODEM
948
Bluetooth Modem
949
ETHERNET MODEM
985
OTHER I/O DEVICES
100

Figure 10

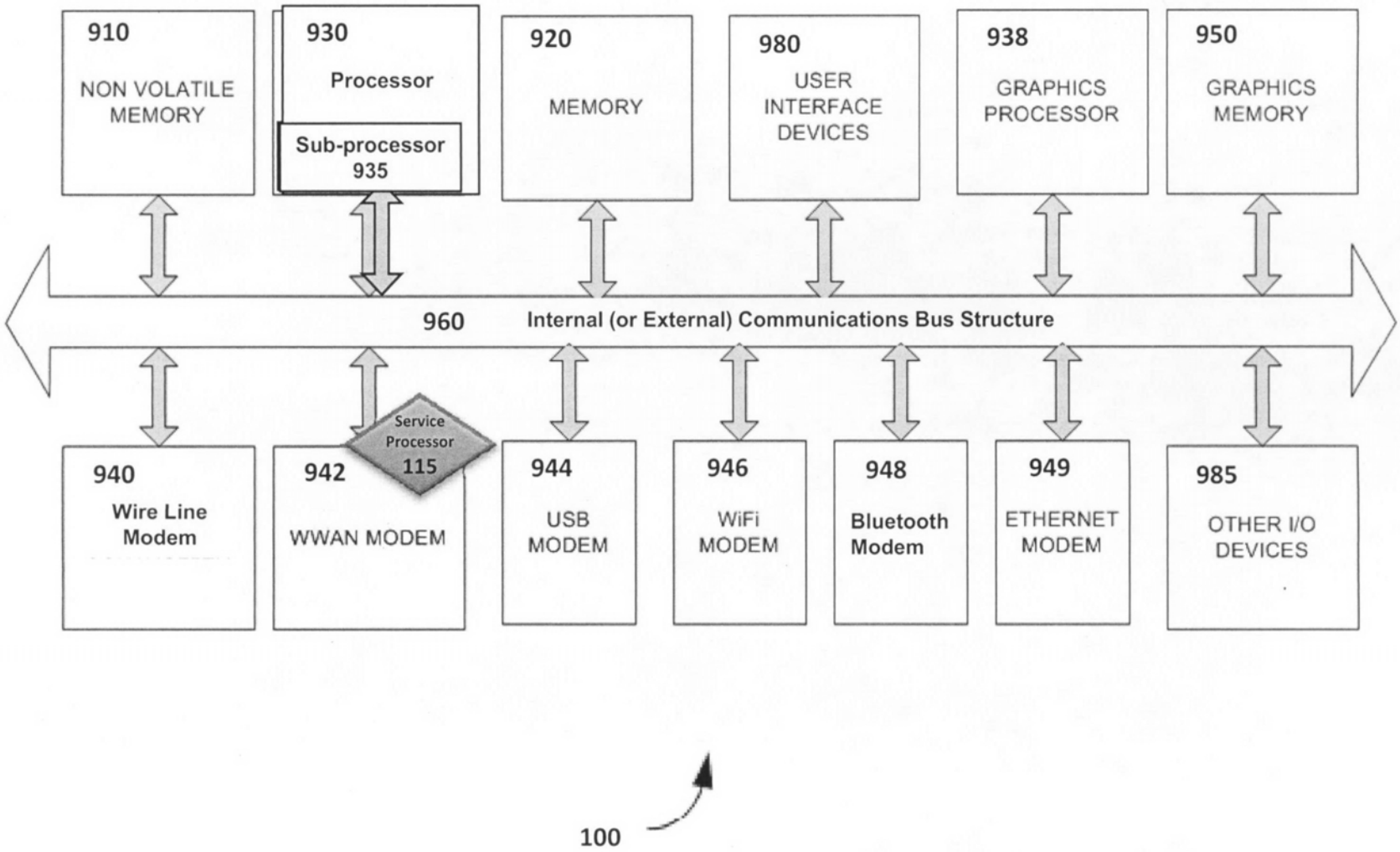

910
NON VOLATILE MEMORY
930
Processor
Sub-processor 935
920
MEMORY
980
USER INTERFACE DEVICES
938
GRAPHICS PROCESSOR
950
GRAPHICS MEMORY
960
Internal (or External) Communications Bus Structure
Service Processor 115
940
Wire Line Modem
942
WWAN MODEM
944
USB MODEM
946
WiFi MODEM
948
Bluetooth Modem
949
ETHERNET MODEM
985
OTHER I/O DEVICES
100

Figure 11

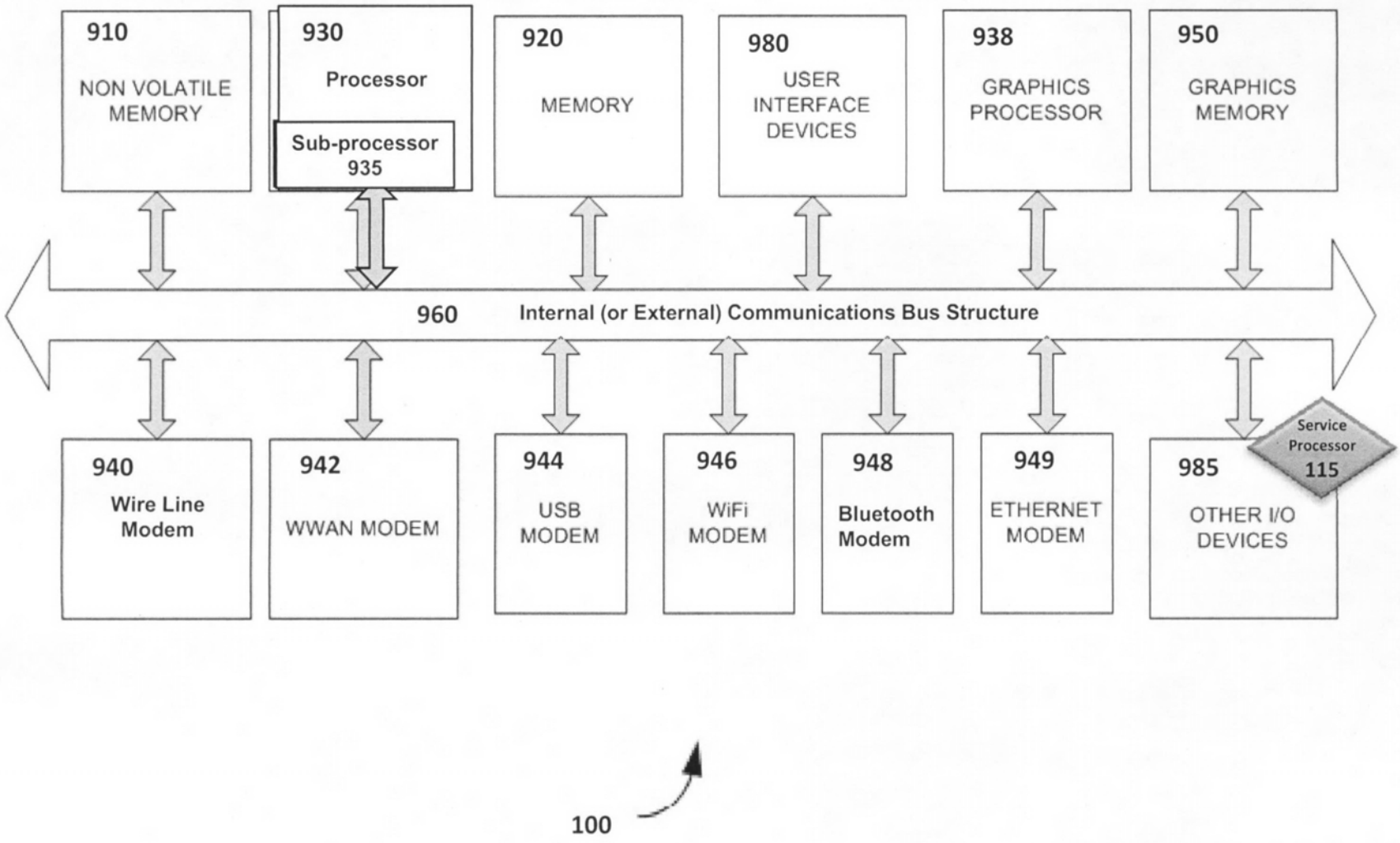

910
NON VOLATILE MEMORY
930
Processor
Sub-processor 935
920
MEMORY
980
USER INTERFACE DEVICES
938
GRAPHICS PROCESSOR
950
GRAPHICS MEMORY
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN MODEM
944
USB MODEM
946
WiFi MODEM
948
Bluetooth Modem
949
ETHERNET MODEM
985
OTHER I/O DEVICES
Service Processor 115
100

Figure 12

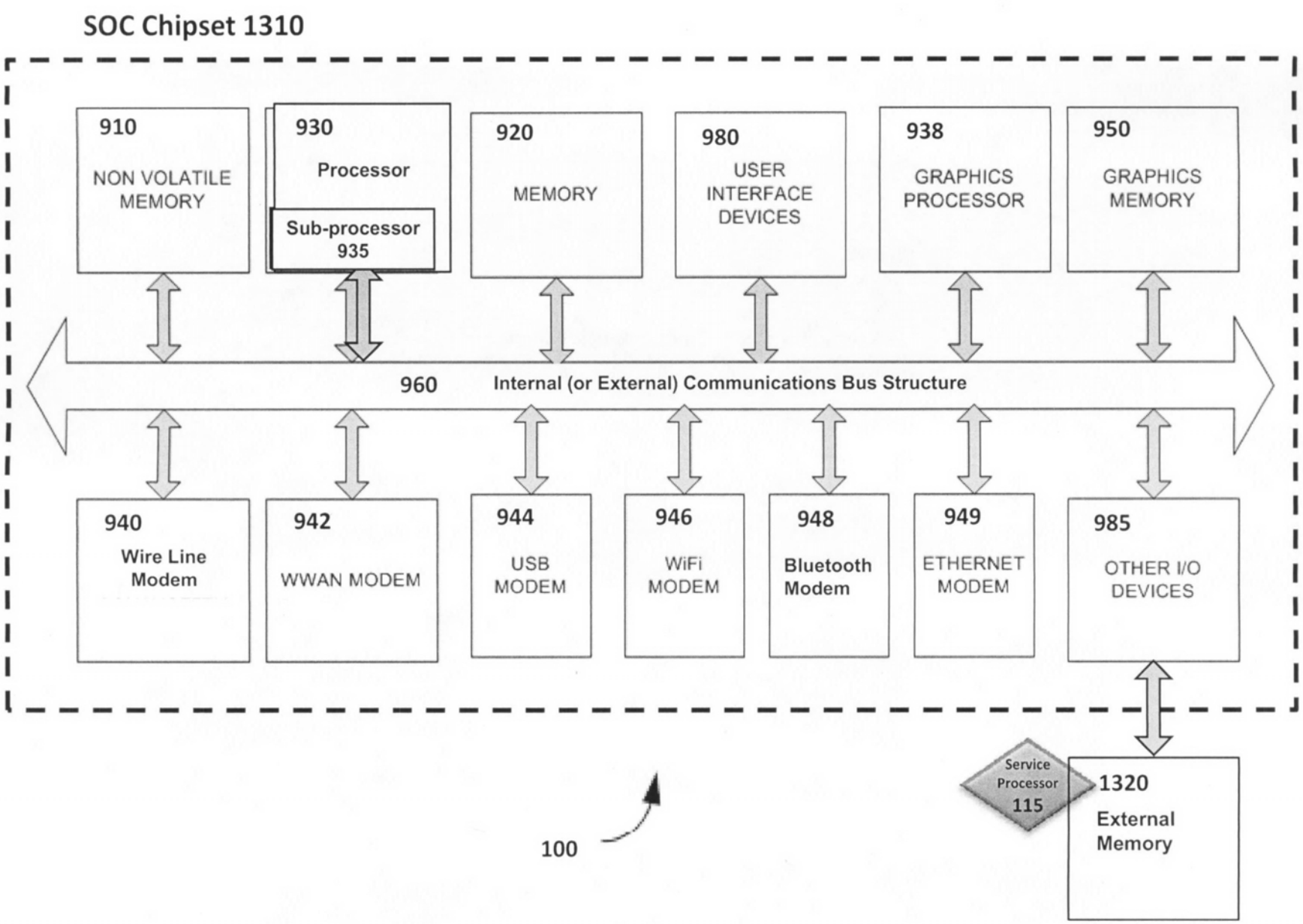

SOC Chipset 1310
910
NON VOLATILE MEMORY
930
Processor
Sub-processor 935
920
MEMORY
980
USER INTERFACE DEVICES
938
GRAPHICS PROCESSOR
950
GRAPHICS MEMORY
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN MODEM
944
USB MODEM
946
WiFi MODEM
948
Bluetooth Modem
949
ETHERNET MODEM
985
OTHER I/O DEVICES
Service Processor 115
1320
External Memory
100

Figure 13

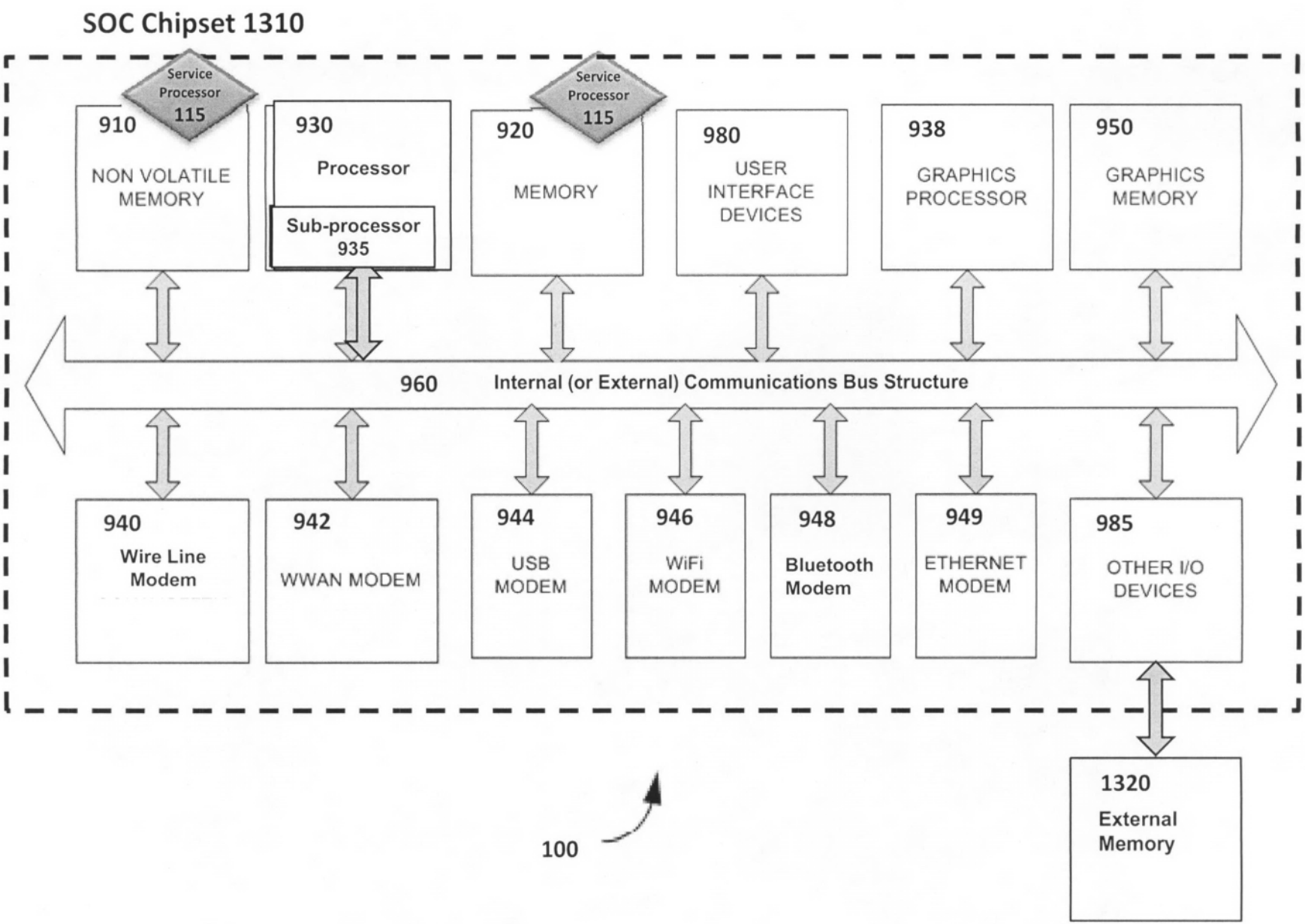

SOC Chipset 1310
Service Processor 115
910
NON VOLATILE MEMORY
930
Processor
Sub-processor 935
Service Processor 115
920
MEMORY
980
USER INTERFACE DEVICES
938
GRAPHICS PROCESSOR
950
GRAPHICS MEMORY
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN MODEM
944
USB MODEM
946
WiFi MODEM
948
Bluetooth Modem
949
ETHERNET MODEM
985
OTHER I/O DEVICES
1320
External Memory
100

Figure 14

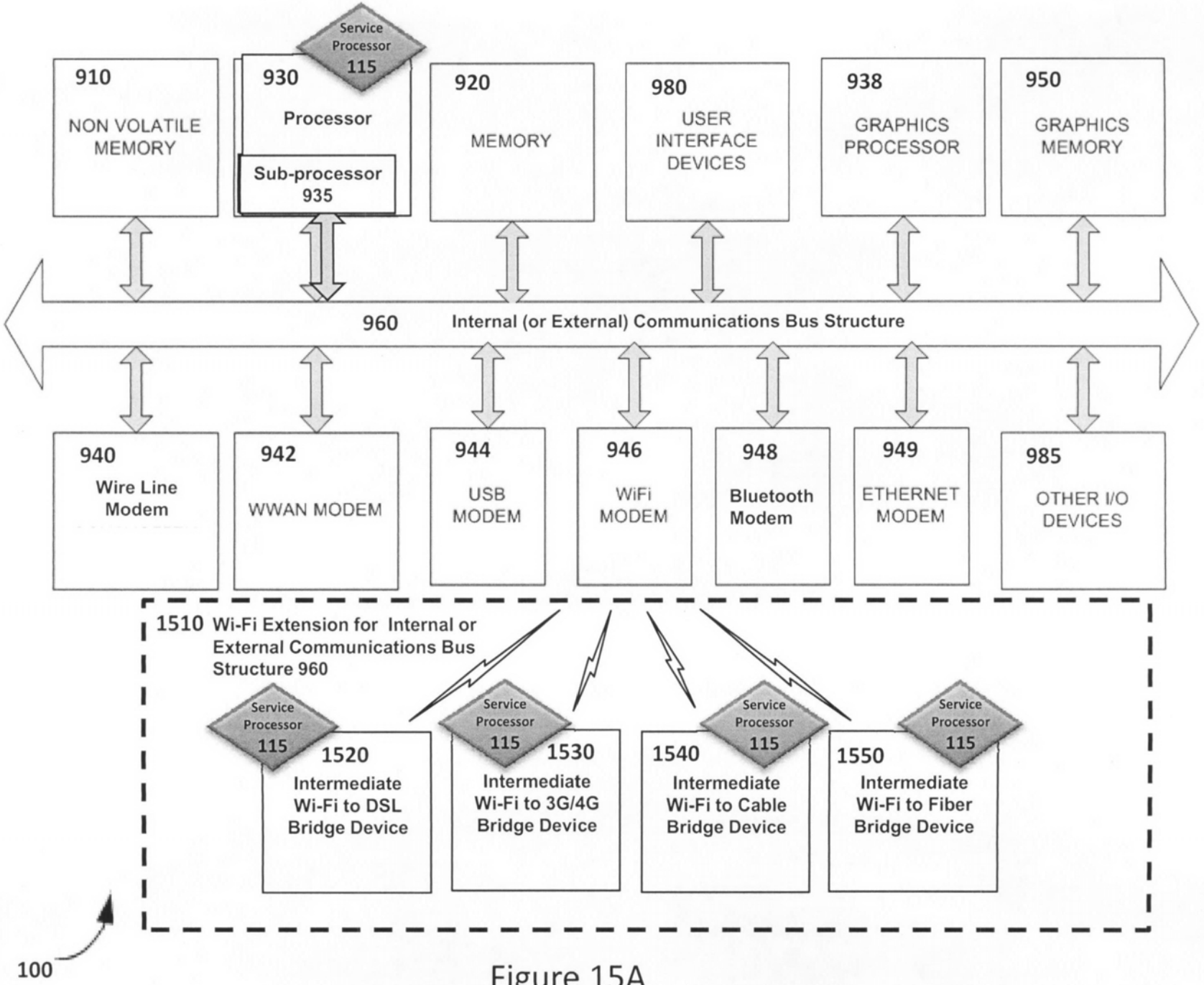

Service Processor 115
910
NON VOLATILE MEMORY
930
Processor
Sub-processor 935
920
MEMORY
980
USER INTERFACE DEVICES
938
GRAPHICS PROCESSOR
950
GRAPHICS MEMORY
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN MODEM
944
USB MODEM
946
WiFi MODEM
948
Bluetooth Modem
949
ETHERNET MODEM
985
OTHER I/O DEVICES
1510 Wi-Fi Extension for Internal or External Communications Bus Structure 960
Service Processor 115
1520
Intermediate Wi-Fi to DSL Bridge Device
Service Processor 115
1530
Intermediate Wi-Fi to 3G/4G Bridge Device
Service Processor 115
1540
Intermediate Wi-Fi to Cable Bridge Device
Service Processor 115
1550
Intermediate Wi-Fi to Fiber Bridge Device
100

Figure 15A

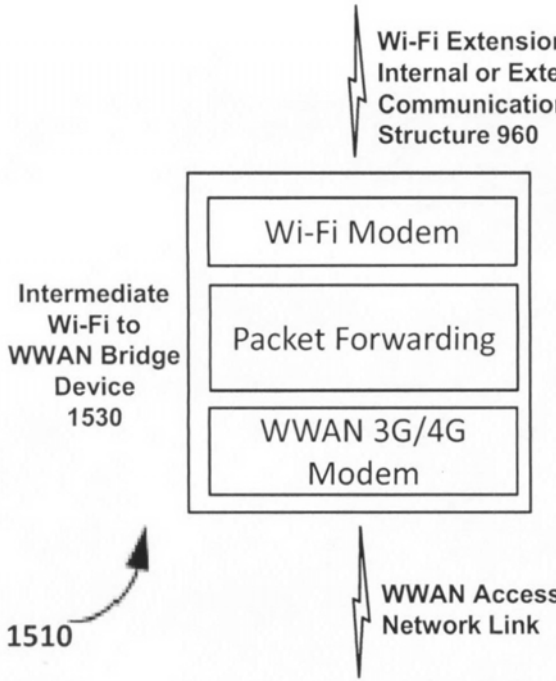


Figure 15B (1)

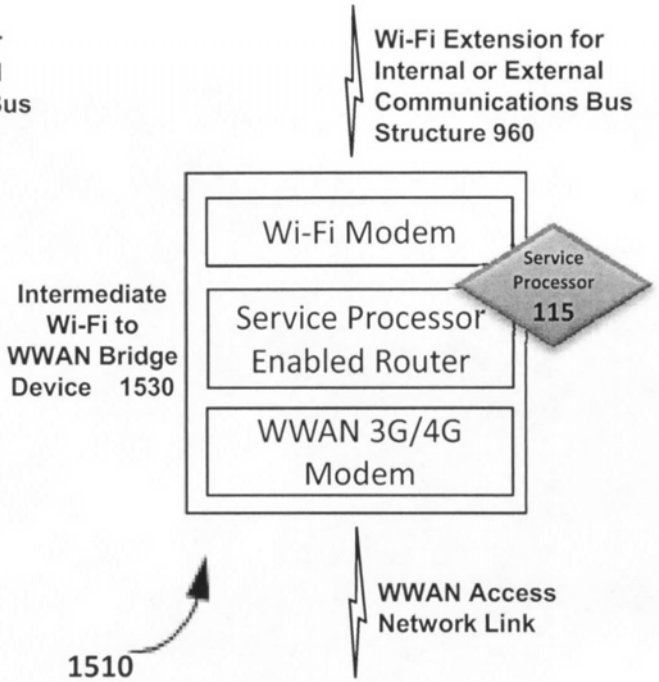


Figure 15B (2)

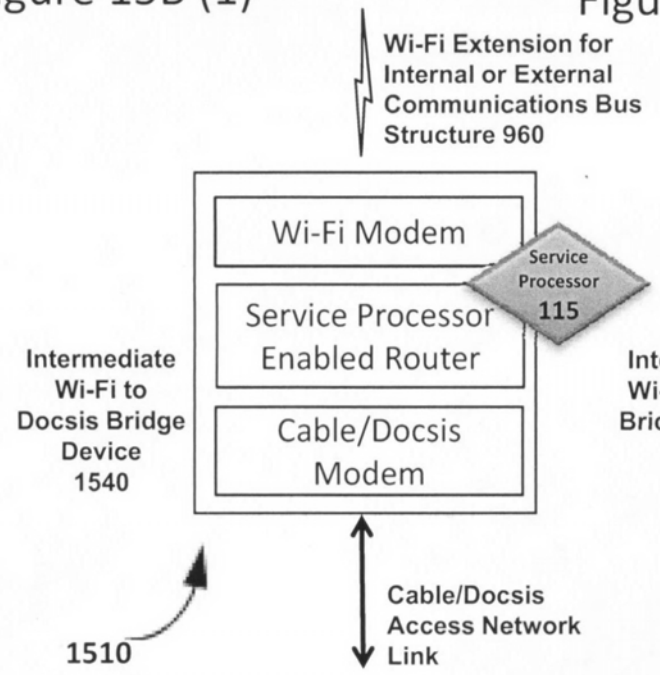


Figure 15B (3)

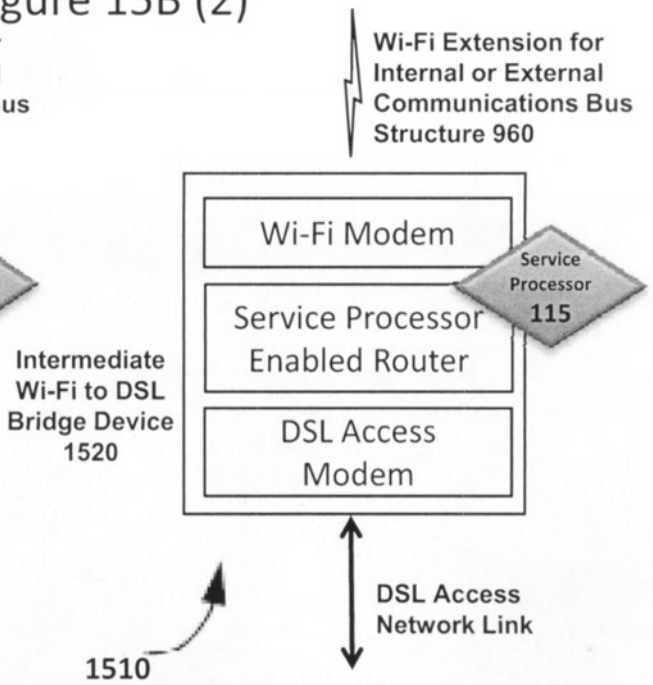


Figure 15B (4)

Figure 15B

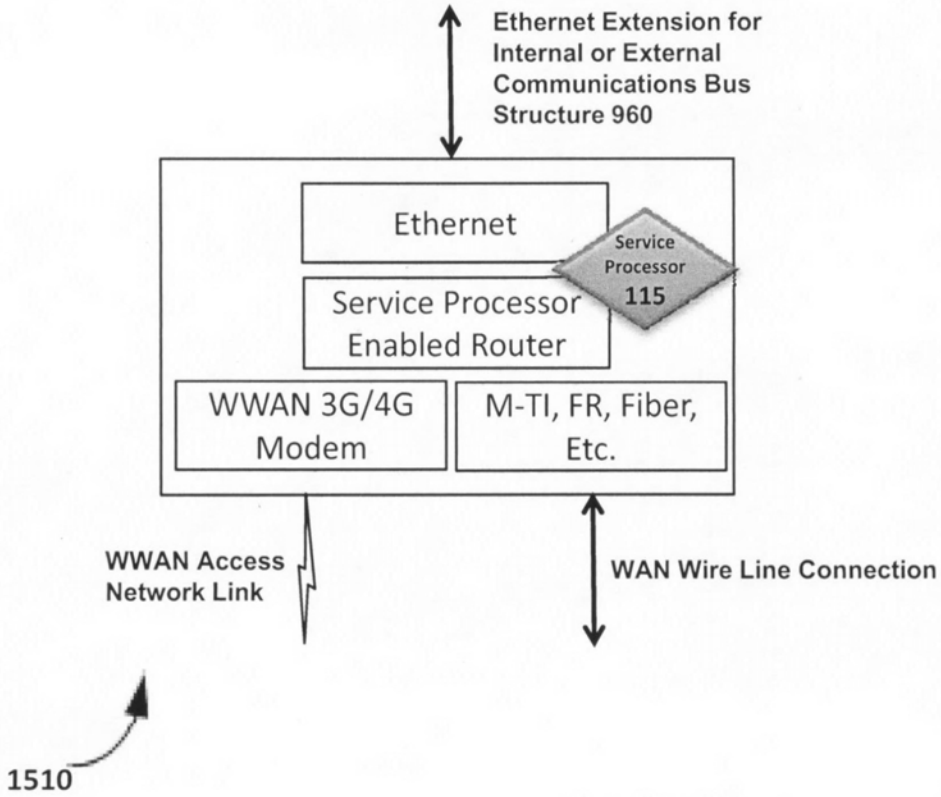

Ethernet Extension for Internal or External Communications Bus Structure 960
Ethernet
Service Processor 115
Service Processor Enabled Router
WWAN 3G/4G Modem
M-TI, FR, Fiber, Etc.
WWAN Access Network Link
WAN Wire Line Connection
1510

Figure 15C

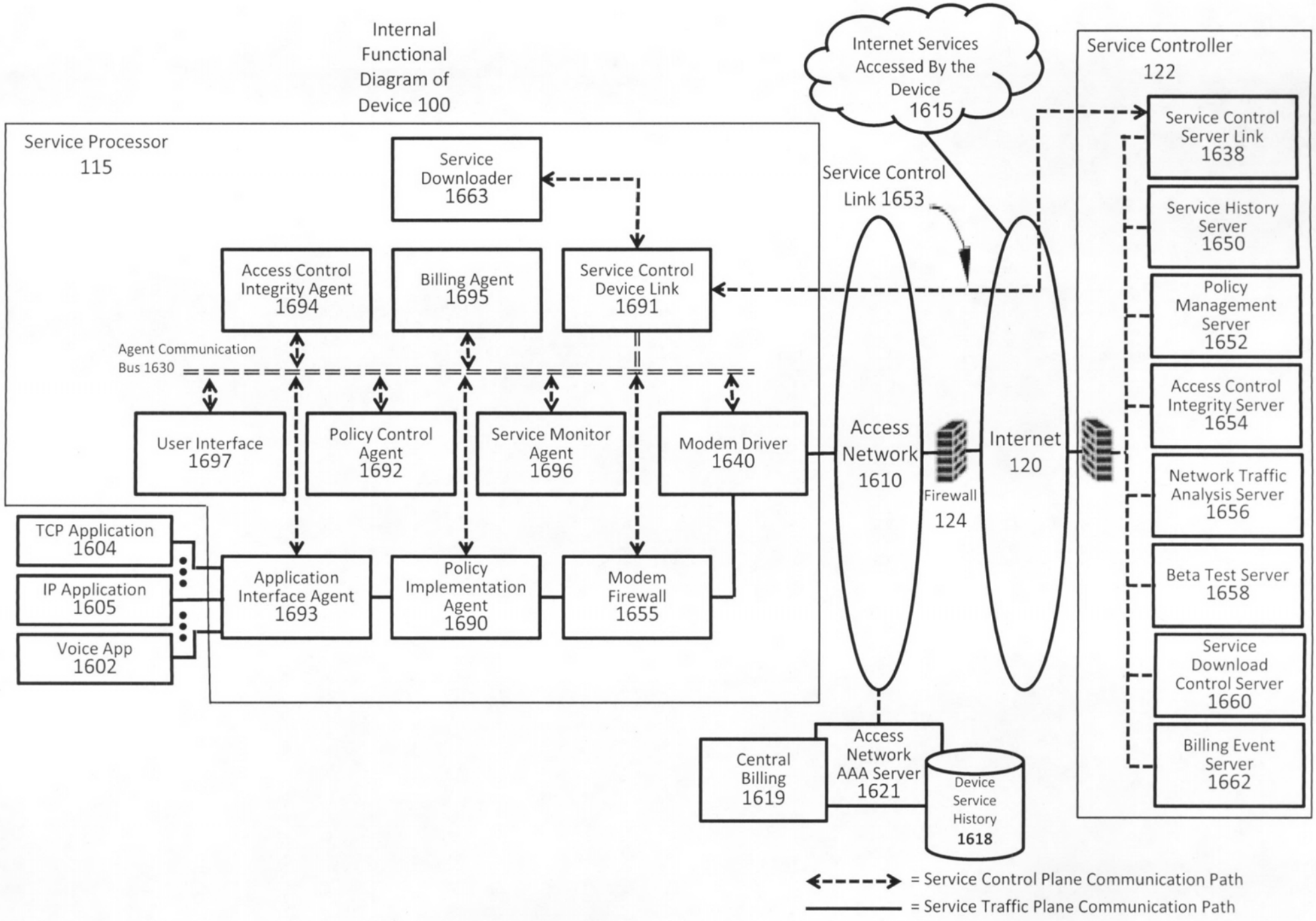

Internal Functional Diagram of Device 100
Service Processor 115
Service Downloader 1663
Access Control Integrity Agent 1694
Billing Agent 1695
Service Control Device Link 1691
Agent Communication Bus 1630
User Interface 1697
Policy Control Agent 1692
Service Monitor Agent 1696
Modem Driver 1640
TCP Application 1604
IP Application 1605
Voice App 1602
Application Interface Agent 1693
Policy Implementation Agent 1690
Modem Firewall 1655
Internet Services Accessed By the Device 1615
Service Control Link 1653
Access Network 1610
Firewall 124
Internet 120
Service Controller 122
Service Control Server Link 1638
Service History Server 1650
Policy Management Server 1652
Access Control Integrity Server 1654
Network Traffic Analysis Server 1656
Beta Test Server 1658
Service Download Control Server 1660
Billing Event Server 1662
Central Billing 1619
Access Network AAA Server 1621
Device Service History 1618
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

Figure 16

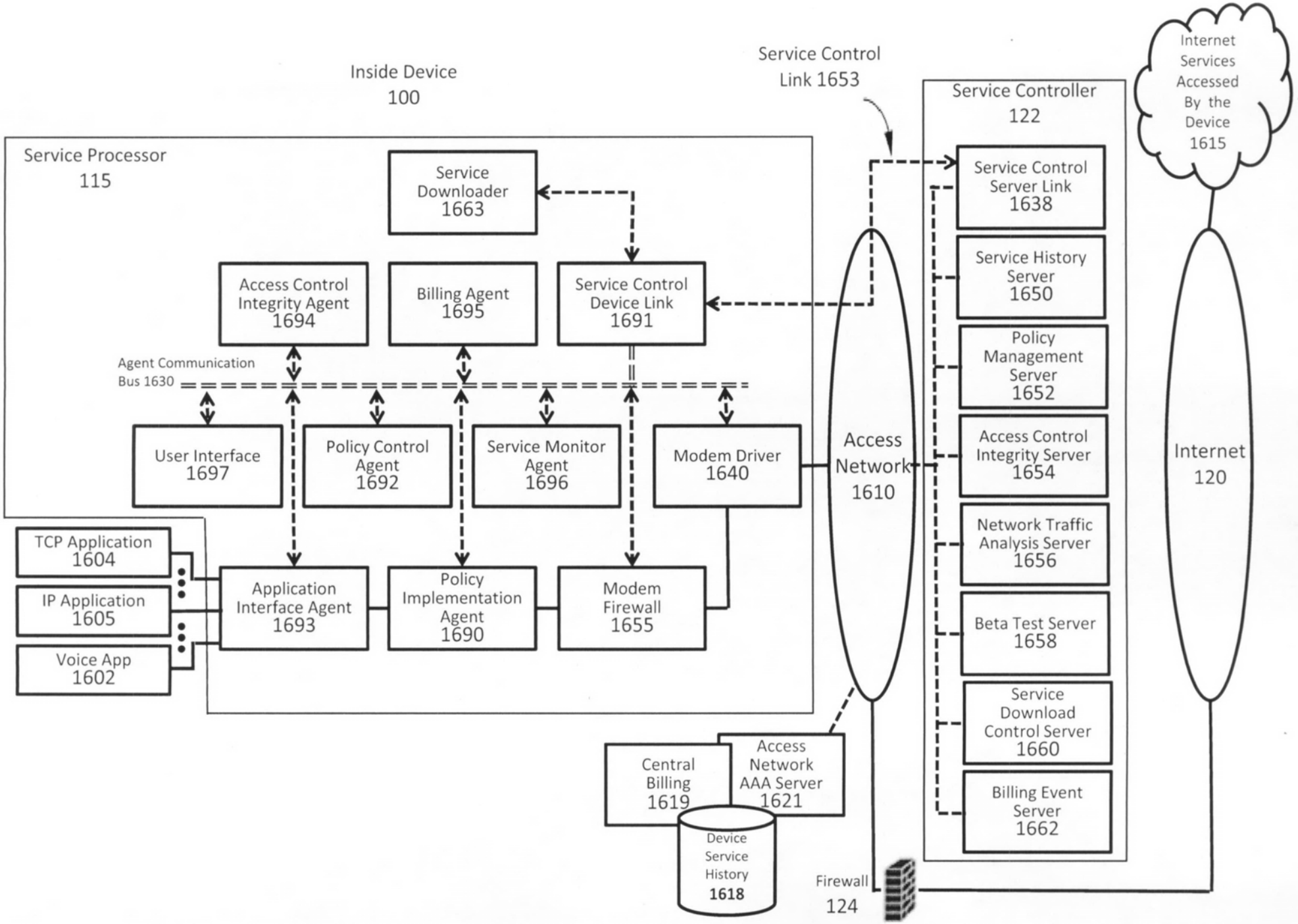

Inside Device
100
Service Control
Link 1653
Service Controller
122
Internet
Services
Accessed
By the
Device
1615
Service Processor
115
Service
Downloader
1663
Service Control
Server Link
1638
Service History
Server
1650
Access Control
Integrity Agent
1694
Billing Agent
1695
Service Control
Device Link
1691
Policy
Management
Server
1652
Agent Communication
Bus 1630
User Interface
1697
Policy Control
Agent
1692
Service Monitor
Agent
1696
Modem Driver
1640
Access
Network
1610
Access Control
Integrity Server
1654
Internet
120
Network Traffic
Analysis Server
1656
TCP Application
1604
IP Application
1605
Voice App
1602
Application
Interface Agent
1693
Policy
Implementation
Agent
1690
Modem
Firewall
1655
Beta Test Server
1658
Service
Download
Control Server
1660
Central
Billing
1619
Access
Network
AAA Server
1621
Billing Event
Server
1662
Device
Service
History
1618
Firewall
124
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

Figure 17

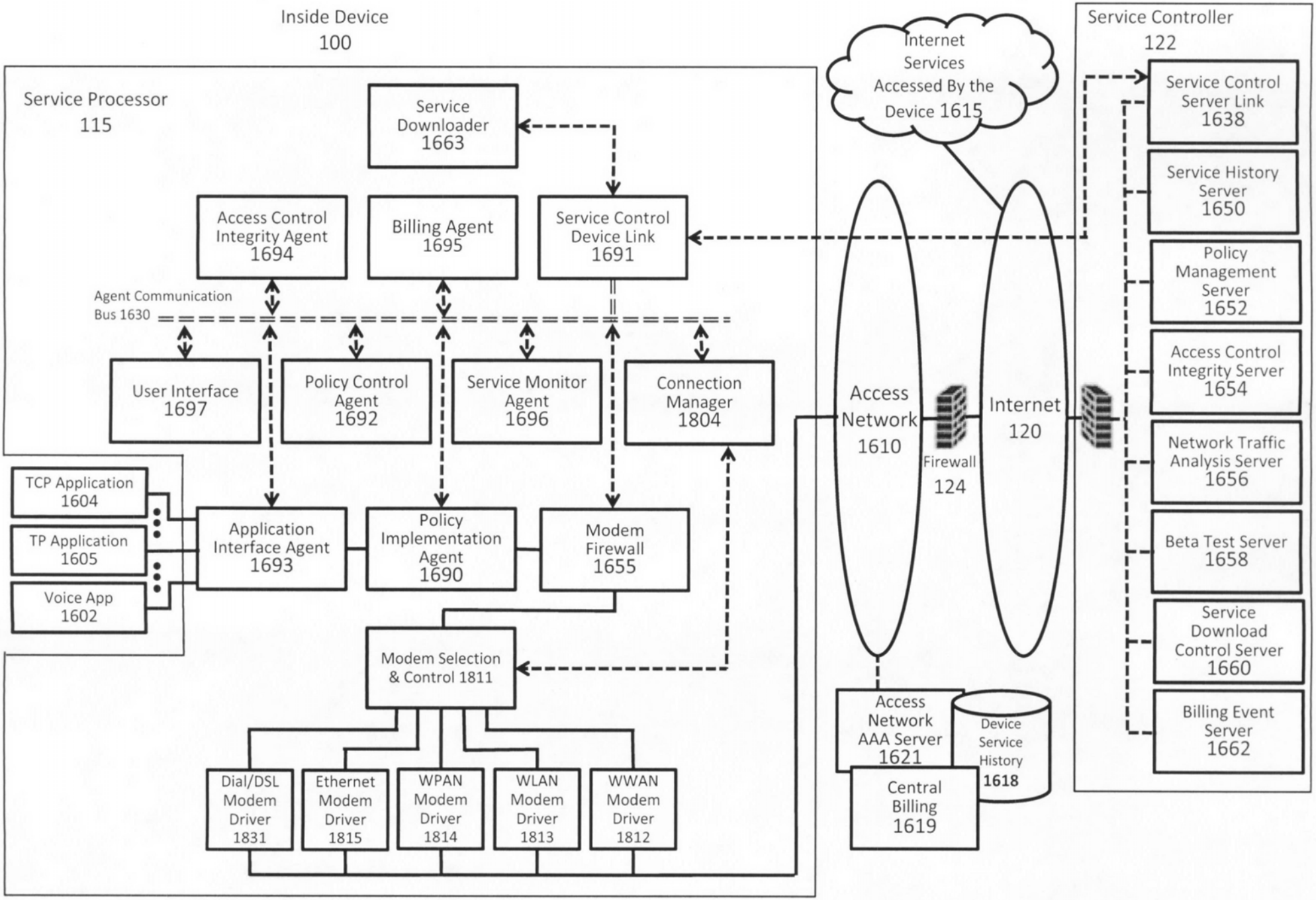

Inside Device
100
Service Processor
115
Service Downloader
1663
Access Control Integrity Agent
1694
Billing Agent
1695
Service Control Device Link
1691
Agent Communication Bus 1630
User Interface
1697
Policy Control Agent
1692
Service Monitor Agent
1696
Connection Manager
1804
TCP Application
1604
TP Application
1605
Voice App
1602
Application Interface Agent
1693
Policy Implementation Agent
1690
Modem Firewall
1655
Modem Selection & Control 1811
Dial/DSL Modem Driver
1831
Ethernet Modem Driver
1815
WPAN Modem Driver
1814
WLAN Modem Driver
1813
WWAN Modem Driver
1812
Internet Services Accessed By the Device 1615
Access Network
1610
Firewall
124
Internet
120
Access Network AAA Server
1621
Device Service History
1618
Central Billing
1619
Service Controller
122
Service Control Server Link
1638
Service History Server
1650
Policy Management Server
1652
Access Control Integrity Server
1654
Network Traffic Analysis Server
1656
Beta Test Server
1658
Service Download Control Server
1660
Billing Event Server
1662
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

Figure 18

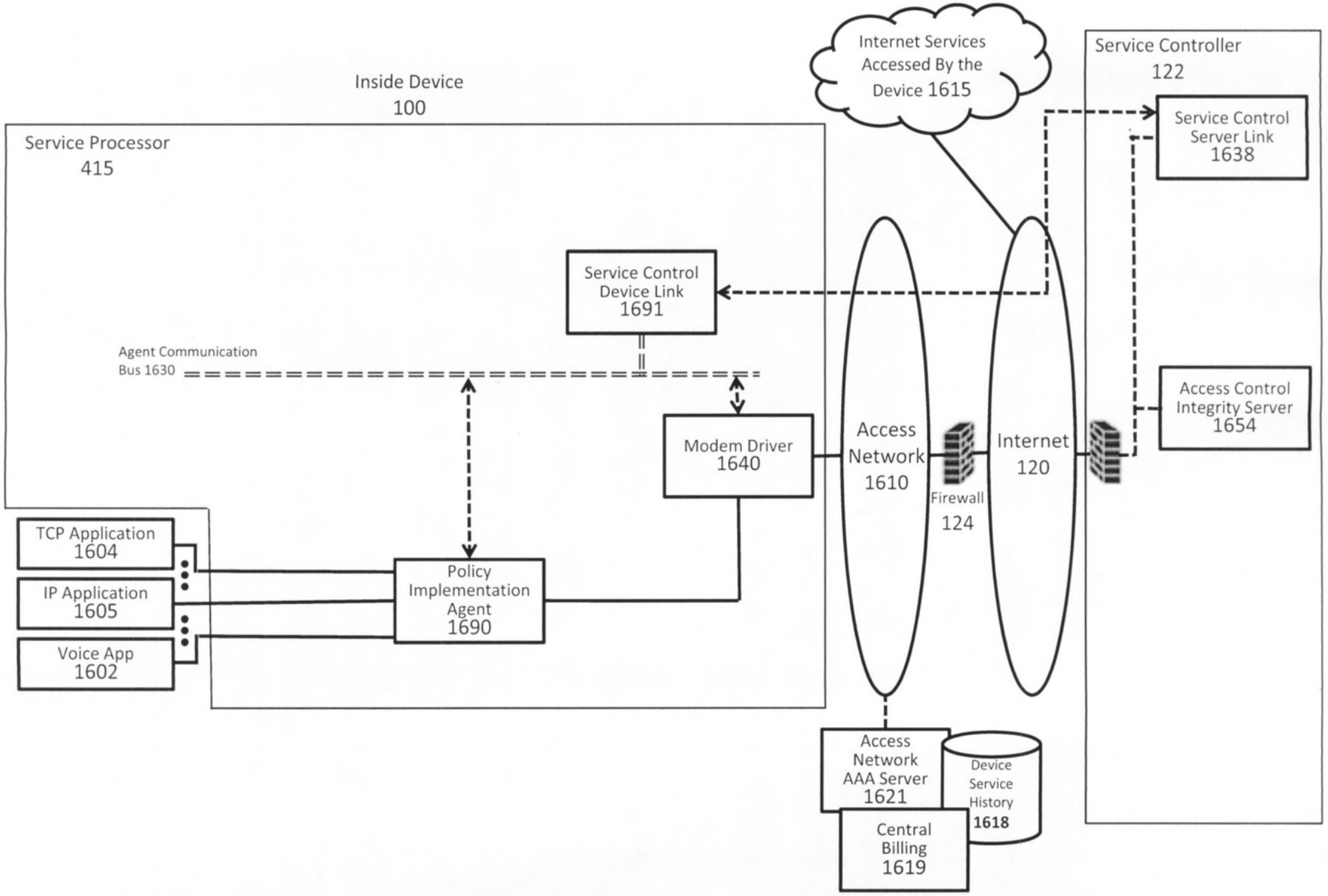

Inside Device
100
Service Processor
415
Internet Services Accessed By the Device 1615
Service Controller
122
Service Control Server Link
1638
Service Control Device Link
1691
Agent Communication Bus 1630
Access Control Integrity Server
1654
Modem Driver
1640
Access Network
1610
Firewall
124
Internet
120
TCP Application
1604
IP Application
1605
Voice App
1602
Policy Implementation Agent
1690
Access Network AAA Server
1621
Device Service History
1618
Central Billing
1619
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

Figure 19

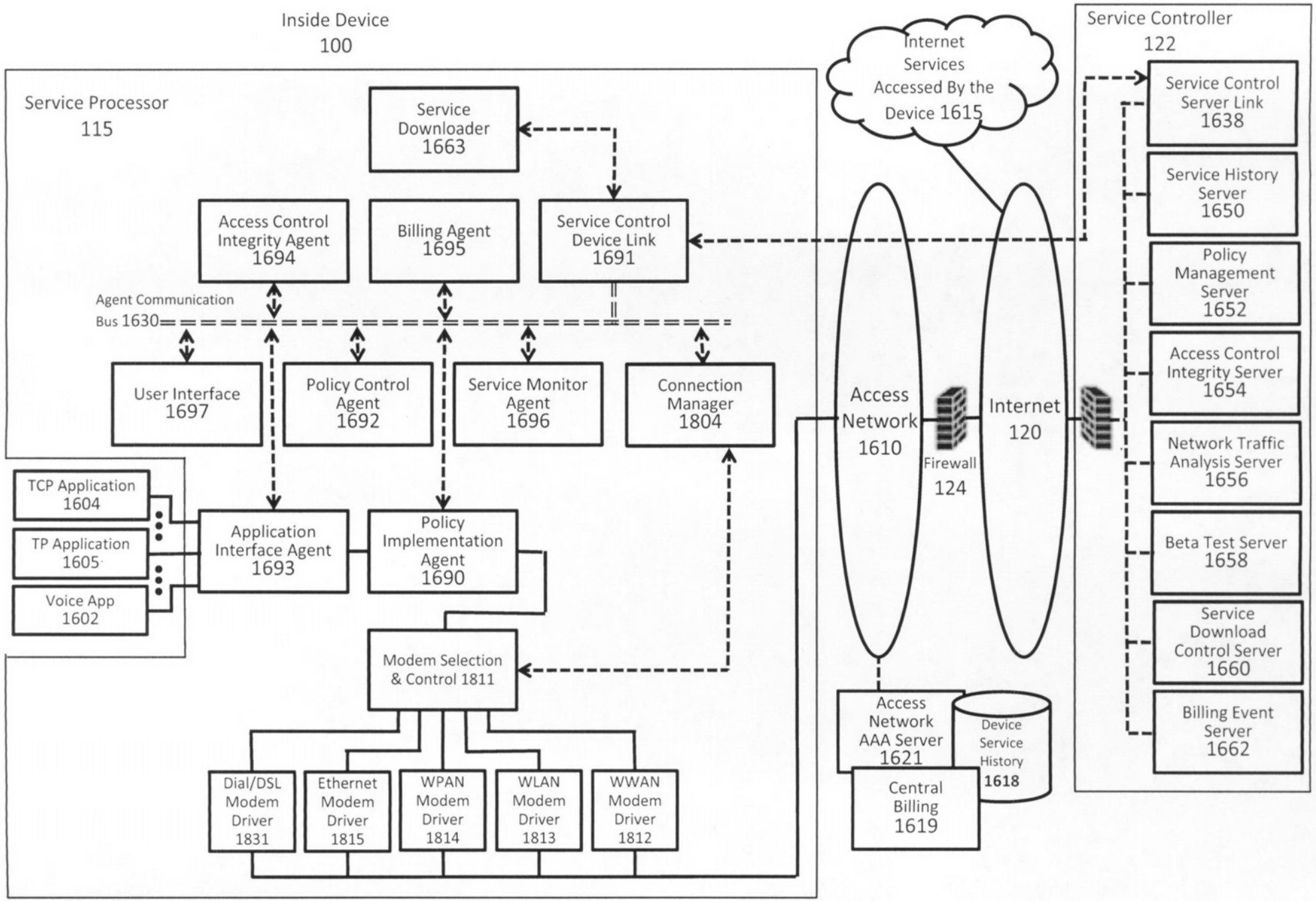

Inside Device
100
Service Processor
115
Service Downloader
1663
Access Control Integrity Agent
1694
Billing Agent
1695
Service Control Device Link
1691
Agent Communication Bus 1630
User Interface
1697
Policy Control Agent
1692
Service Monitor Agent
1696
Connection Manager
1804
TCP Application
1604
TP Application
1605
Voice App
1602
Application Interface Agent
1693
Policy Implementation Agent
1690
Modem Selection & Control 1811
Dial/DSL Modem Driver
1831
Ethernet Modem Driver
1815
WPAN Modem Driver
1814
WLAN Modem Driver
1813
WWAN Modem Driver
1812
Internet Services Accessed By the Device 1615
Access Network
1610
Firewall
124
Internet
120
Access Network AAA Server
1621
Device Service History
1618
Central Billing
1619
Service Controller
122
Service Control Server Link
1638
Service History Server
1650
Policy Management Server
1652
Access Control Integrity Server
1654
Network Traffic Analysis Server
1656
Beta Test Server
1658
Service Download Control Server
1660
Billing Event Server
1662
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

Figure 20

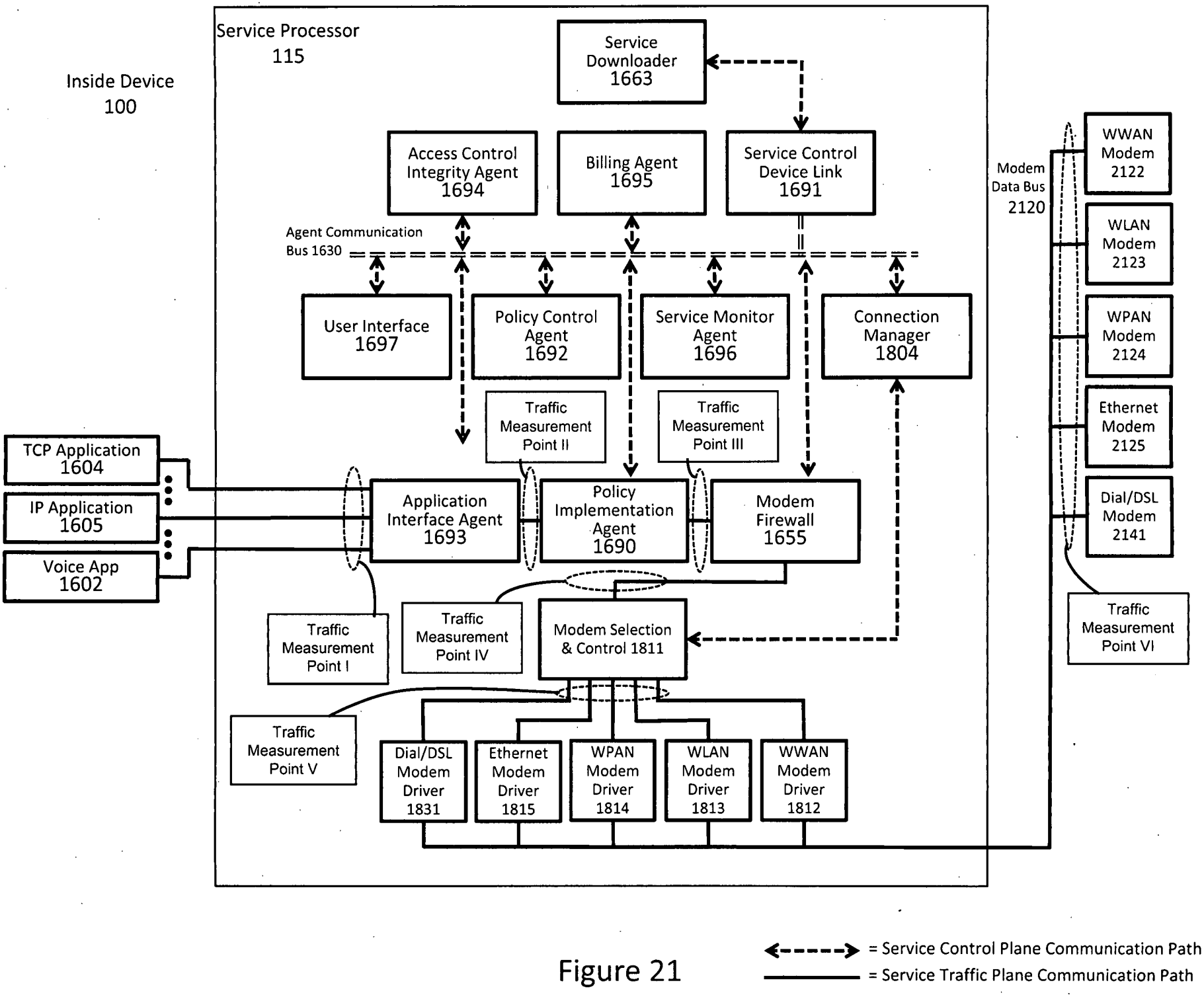

Inside Device
100
Service Processor
115
Service Downloader
1663
Access Control Integrity Agent
1694
Billing Agent
1695
Service Control Device Link
1691
Agent Communication Bus 1630
User Interface
1697
Policy Control Agent
1692
Service Monitor Agent
1696
Connection Manager
1804
Traffic Measurement Point II
Traffic Measurement Point III
TCP Application
1604
IP Application
1605
Voice App
1602
Application Interface Agent
1693
Policy Implementation Agent
1690
Modem Firewall
1655
Traffic Measurement Point I
Traffic Measurement Point IV
Modem Selection & Control 1811
Traffic Measurement Point V
Dial/DSL Modem Driver
1831
Ethernet Modem Driver
1815
WPAN Modem Driver
1814
WLAN Modem Driver
1813
WWAN Modem Driver
1812
Modem Data Bus
2120
WWAN Modem
2122
WLAN Modem
2123
WPAN Modem
2124
Ethernet Modem
2125
Dial/DSL Modem
2141
Traffic Measurement Point VI
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

Figure 21

Service Processor 115 Embodiment	Partial Summary of Embodiment Functions
Service Control Device Link 1691	Device side control plane link for connecting Service Processor 415 to Service Controller. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Agent 1694	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, verifies configuration of other agents or performs challenge-response sequence testing. In some embodiments, monitors software loading activity, protected memory access or communication with Service Processor agents to detect unauthorized changes to Service Processor software or configuration.
Policy Control Agent 1692	Takes policy instructions from the network and sets instantaneous device service policy. In some embodiments, performs a policy control function to adapt instantaneous service policies to achieve a service usage objective.
Policy Implementation Agent 1690	Implements traffic control and QOS policy rules for device. In some embodiments provides the functions of access control and/or firewall function or perform traffic inspection and characterization. In some embodiments packet inspection is aided by literal or virtual application layer tagging while in other embodiments packet inspection is performed completely in the Policy Implementation Agent 490.
Service Monitor Agent 1696	Records and reports device service usage. In some embodiments, assists in communicating application tagging of traffic flows through the networking stack policy implementation. In some embodiments, maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection.
Application Interface Agent 1693	Rich feature interface for device application programs. In some embodiments, identifies application level traffic, reports service usage or tags traffic for service QOS control. In some embodiments, interacts with applications or programs applications to arrange application settings such as email file transfer options or browser headers. In some embodiments, intercepts certain application traffic to modify traffic application layer parameters such as email file transfer options or browser headers. In some embodiments implements certain aspects of traffic control or other service policies. In some embodiments, provides the functions of traffic control, access control and/or firewall.
Modem Firewall 1655	Blocks or passes traffic based on service policies and traffic attributes. In some embodiments, assists in traffic flow tagging. In some embodiments provides the functions of traffic control and/or access control.
Billing Agent 1695	Detects and reports billing events. In some embodiments interacts with the User Interface Agent 497 to provide the user with service plan options, accept service plan selections, provide notification on service usage levels, provide options on service usage control policy, accept choices on service usage policy, provide transaction options or accept transaction choices. In some embodiments, interacts with Transaction Servers 134 to conduct ecommerce transactions with central billing.
User Interface Agent 1697	Provide service interface to users.
Service Downloader 1663	Provides a download function to install or update service software elements on the device.
Connection Manager 1804	Provides a control and supervision function for one or more modem drivers or modems that connect to an access network.
Modem Selection and Control 1811	Selects the access network connection.
Modem Drivers 1831, 1815, 1814, 1813, 1812	Converts data traffic into modem bus traffic for one or more modems.
Modems 2141, 2125, 2124, 2123, 2122	Connects the device to one or more networks.

Figure 22

Service Controller 122 Element	Partial Summary of Embodiment Functions
Service Control Server Link 1638	Network side control plane link for connecting Service Controller 422 Service Processor 415 device agents. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Server 1654	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected.
Policy Management Server 1652	Transmits policies to the Service Processor 415.
Access Network AAA Server 1621	Provides access control and authorization functions for the device access layer. Records and reports device network service usage.
Service History Server 1650	Collects and records service usage reports from the Access Network AAA Server 421 and the Service Monitor Agent 496. In some embodiments, maintains a history of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection. In some embodiments, this activity summary is further analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.
Central Provider Billing System 1619	Provides mediation function for central provider billing events. Accepts service plan changes. In some embodiments, provides updates on device service usage, service plan limits or service policies.
Billing Event Server 1662	In some embodiments, collects billing events, provides service plan information to the Service Processor 415, provides service usage updates to the Service Processor 415, serves as interface between device and central Provider Billing System 123, or provides trusted third party function for certain ecommerce billing transactions.
Network Traffic Analysis Server 1656	Collects service usage history for devices or groups of devices and analyses the service usage. In some embodiments, presents service usage statistics in various formats to identify improvements in network service quality or service profitability. In other embodiments, estimates the service quality or service usage for the network under variable settings on potential service policy. In other embodiments, identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost.
Beta Test Server 1658	Publishes candidate service plan policy setting to one or more devices. In some embodiments, provides summary reports of network service usage or user feedback information for one or more candidate service plan policy setting. In some embodiments, provides a means to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further setting optimization.
Service Download Control Server 1660	Provides a download function to install or update service software elements on the device.
Transaction Server 134	Provides an electronic commerce offering and transaction platform to the device.

Figure 23

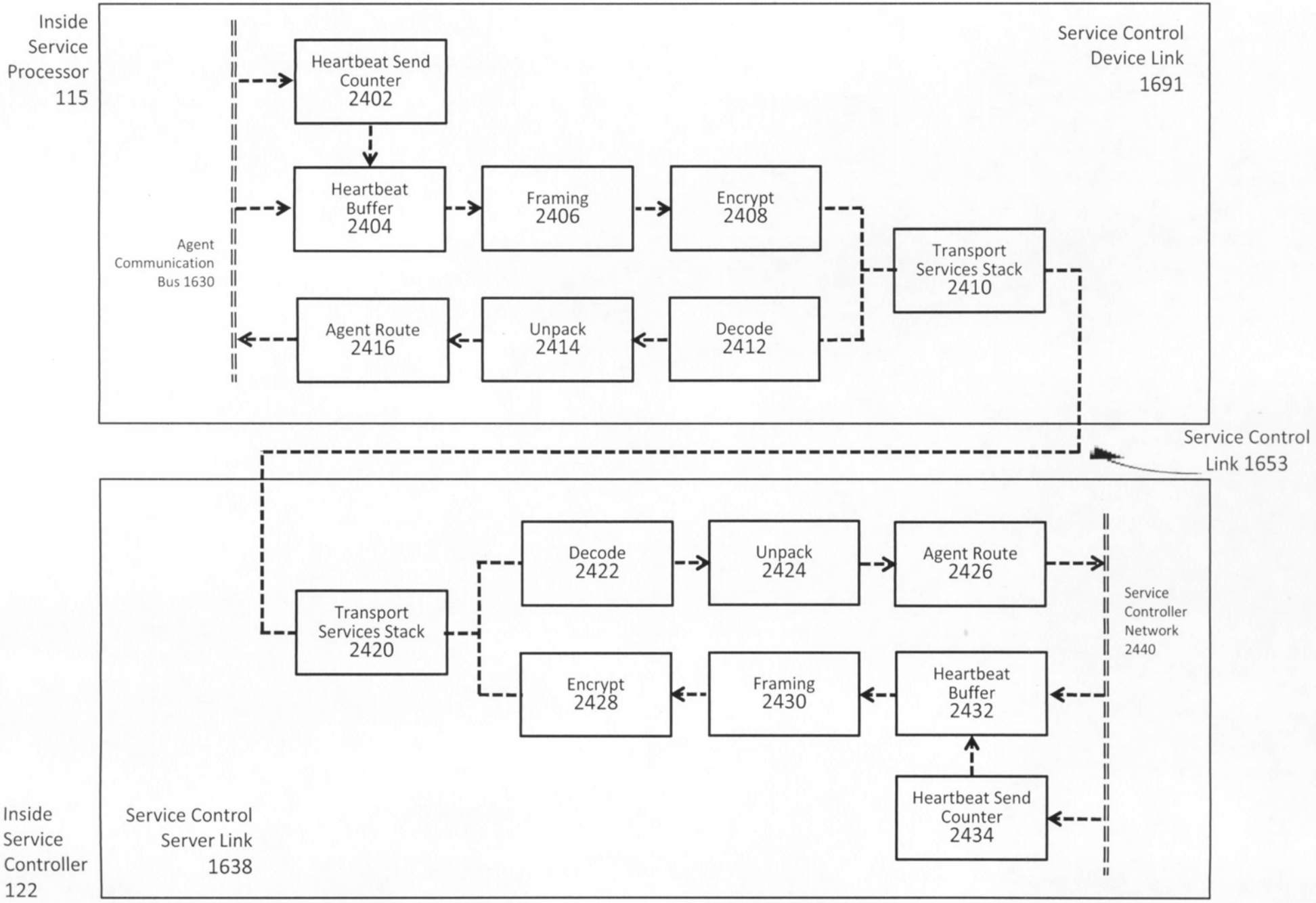
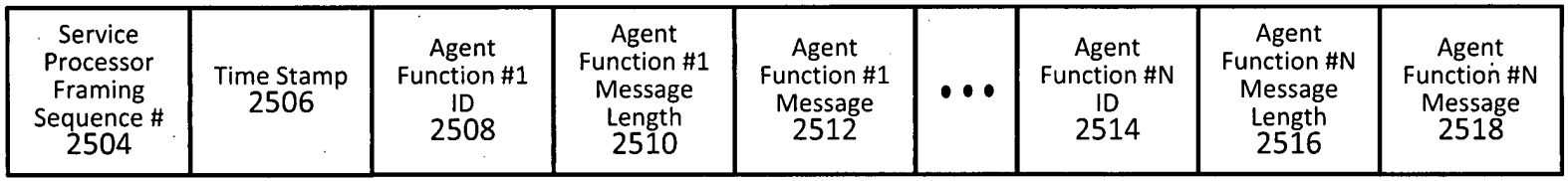
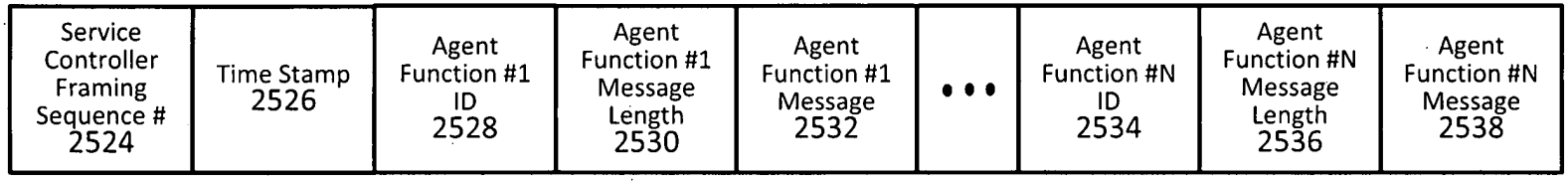

Inside Service Processor 115
Service Control Device Link 1691
Heartbeat Send Counter 2402
Heartbeat Buffer 2404
Framing 2406
Encrypt 2408
Transport Services Stack 2410
Agent Communication Bus 1630
Agent Route 2416
Unpack 2414
Decode 2412
Service Control Link 1653
Decode 2422
Unpack 2424
Agent Route 2426
Transport Services Stack 2420
Service Controller Network 2440
Encrypt 2428
Framing 2430
Heartbeat Buffer 2432
Heartbeat Send Counter 2434
Inside Service Controller 122
Service Control Server Link 1638

Figure 24



Service Processor Communication Frame 2502



Service Controller Communication Frame 2522

Figure 25

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Access control integrity report	Contains the latest results of the Access Control Integrity agents Service Processor system checks and reports any error events.	Not necessary to report in every heartbeat if there are no errors. Can report only on error, set a minimum frequency or respond to Service Controller polling.
Service monitor report	Reports filtered summary of Service Monitor Agent measurements. Summary reduces control traffic and filters out unauthorized private information.	Every heartbeat. Some embodiments link this to amount of data usage in the data path to keep overhead low. Report immediately upon polling from Service Controller.
Billing event report	Reports any billing activity since the last heartbeat. Billing events may include service usage events, transaction events, bill by account records, bill by account offset reports, or any other event that results in a billing event report.	Send upon billing event. Report immediately upon polling from Service Controller.
Service Processor settings report	Reports service policy settings for all Service Processor agents.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Customer resource management report	Reports filtered summary of Service Monitor Agent measurements or filtered summary of other device or user activity such as service preferences, advertisement behavior and location. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Responses to Service Processor agent queries	Sends agent responses to challenge-response queries from the Service Controller.	Report immediately upon polling from Service Controller.
Location tracking service update	Reports filtered summary of location tracking information. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments call for a minimum time based transmission frequency.
Service usage based transmission frequency	Lowers overhead by buffering and reserving heartbeat communications from agents and servers until a certain amount of data has been transmitted or received in the network, or a certain amount of service has been consumed. When the parameters are chosen properly, this can result in the network control plane traffic overhead being a small percentage of data path traffic or result in the control plane traffic cost being a small percentage of the service usage cost.	Ranges depending on settings. For example, if there are 5 agents messages that typically need to be communicated, and each message is less than 100 bytes, and Service Processor heartbeat framing plus network overhead would result in a packet size of less than 1,000 bytes, and the heartbeat packet is transmitted when 10,000,000 bytes have been communicated over the data path, then the overhead loss due to one heartbeat packet in each direction is less than 0.02%.
Constant frequency transmissions	Since the device may be off line for long periods of time where the Service Control Processor needs to verify service control integrity, in some embodiments it can be advantageous to transmit heartbeat packets at a minimum rate regardless of data traffic activity. This is accomplished by setting a timer that sends queued heartbeat packets on a regular schedule.	Ranges depending on settings and applications.
Service Controller polled transmissions	In some embodiments, the Service Controller may poll the Service Processor for a heartbeat transmission at which time the Service Processor will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Controller.
Service Processor polled transmissions	In some embodiments, the Service Processor polls the Service Controller for a heartbeat transmission at which time the Service Controller will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Processor.

Figure 26A

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Agent self-check reports	Agent reports results of various agent self-diagnosis procedures to ensure that the agent is properly configured, operating properly, properly implementing service control policy or has not been tampered with. [provide examples which are extensions of typical software security self diagnosis reporting]	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Environment reports	One or more agents scan the storage or execution environment for one or more of the agents to identify potential threats to the integrity of the service implementation or agent integrity and makes a report. In one example embodiment, a scan is done to determine if unauthorized software or hardware is executing in a secure agent environment. In another embodiment, a scan is done to determine the software that has been loaded into a portion of the device operating environment, memory or storage, and the software list is referenced against a known threat list. In another example embodiment, the list of entities that accessed one or more agents is scanned to determine if an unauthorized access to an agent has occurred. In another embodiment a scan is performed to determine if unauthorized access to secure execution environment, memory or storage has occurred. In another example embodiment, the network access pattern for the device is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity. In another example embodiment, the internal device software, memory or peripheral access pattern is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
User notification response reports	Billing agent, UI agent or another agent logs user notification events and the response of the user to the notification event. In some embodiments these events may be cross-referenced to the notification policy that should be in force on the device and the device service usage to ensure that the proper notification sequences are being adhered to. In other embodiments, the user notification responses are logged and used to document user choices to notification events, billing event decisions, service control decisions or service cost control decisions. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly. In some embodiments, the user may be asked to acknowledge a service overage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service overage acknowledgement.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a user notification sequence action with the user. In some embodiments, the report is generated when there is a verification error of some kind that is identified.

Figure 26B

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
User warning response reports	Billing agent, UI agent or another agent logs user warning events and the response of the user to warning event. In some embodiments the user response is used to determine if the user is in positive control of the device. In some embodiments the response is used to confirm that the user acknowledges a billing overage or other service cost event. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a warning sequence action with the user. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Agent communication log reports	Reports entities that established or attempted to establish communication with the agents. In one embodiment, reports a list of entities and the number of times the entity communicated or attempted to communicate with the agent. In another embodiments, reports an error flag when unauthorized entities attempt to establish communication with an agent.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Service usage synchronization data	IPDR or other data that is used to synchronize the device service usage counters. In some embodiments the data is time stamped so that the service usage at a point in time may be reconciled between the local device usage count and the network based usage count, and then the local device usage count since the point in time may be used to estimate the present real-time usage count. In some embodiments, the service usage data from the device is used by the network as the actual service usage or billing data base for the device. In other embodiments, a bill by account function is included in the service usage synchronization data so that the service usage may be billed to different accounts other than a single or main user account.	Service usage synchronization is continuous with each heartbeat in some embodiments. In other embodiments service usage synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.
Service cost synchronization data	Information to reconcile a service cost estimate on the local device with a service cost count from a network based function. Similar to the service usage count, in some embodiments the service cost information is time stamped so that service cost at a point in time may be reconciled between the device and the network based function, and then a local measure of service cost may be used to estimate the present real-time service cost. In some embodiments the local service cost is determined by taking recorded billing events and looking up the cumulative cost of one or more billing events using a service usage to cost look up data base stored locally on the device or available from a network function. In some embodiments, service cost estimation is done entirely in the network and the result is pushed out to the device UI. In other embodiments service cost estimation is done in the device based on local usage estimates and a local usage to cost lookup table.	Service cost synchronization is continuous with each heartbeat in some embodiments. In other embodiments service cost synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.

Figure 26C

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Available network information and roaming information	Device receives available network or available roaming service provider information from a network function. The available network or roaming service information may include the potential network service or roaming service a device or user may choose to select, or the network service or roaming service the user has already selected. In some embodiments this information includes service cost information to aid the device or the user in determining the potential or actual costs of service usage while using the available network or roaming network. In some embodiments the service cost information is used to help the user in selecting the available network provider or roaming service provider. In some embodiments the available network cost information or roaming cost information is combined with a measure of expected or possible service usage to estimate how much a typical usage scenario may cost. In some embodiments, the available network information or roaming information is used to help the user estimate the present available network or roaming service charges for services used to date. In some embodiments service usage is recorded and sent to a network function that estimates the current service cost. In other embodiments the service cost is estimated locally on the device based on a service usage estimate and a service usage to cost look up function. In other embodiments, the service cost is derived by querying the available network or roaming network billing system.	In some embodiments available network information or roaming information is requested by the device. In other embodiments, the information is periodically updated by the Service Controller or other network function that contains the information.
System messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display a system messages or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include, ... etc.	System messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some system messages are generated in response to user input or requests. In other embodiments, system messages are generated on a regular time table or in accordance with a certain amount of service usage.
UI screen messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display user interface message or screen that is generated by a network function or serve to the end user and possibly report user inputs to the UI message or screen. Examples include service usage UI, service choice UI, upgrade UI, transaction UI, marketing UI, billing UI, user identify confirmation UI, user service warning UI, user potential service tamper response request UI, etc.	UI screen messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some user UI messages are generated in response to user input or requests. In other embodiments, UI messages are generated on a regular time table or in accordance with a certain amount of service usage.
Local agent check-in history	Logs and reports agent check-ins or self-reports that are made to a local agent integrity verification function.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.

Figure 26D

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Software install report	Logs and reports one or more aspects of software installs that have occurred on the device.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified. In some embodiments, the report is generated when new SW is installed.
Test billing event	In some embodiments the Service Controller or other network function may send or cause a test billing event wherein the device triggers a local billing sequence for the purpose of verifying that the billing sequence is properly logged, conducted and reported. The billing sequence can be related to a service usage event or sequence, a transaction event or sequence, or any other event or sequence that should result in a billing event.	In some embodiments, the test billing event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.
Test service event	In some embodiments the service Controller or other network function may send or cause a service usage event wherein the device triggers a local service usage event or sequence for the purpose of verifying that the service usage event or sequence is properly logged and reported.	In some embodiments, the test service usage event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.

Figure 26E

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify service usage measure in network is consistent with expected service behavior	Network service usage measure is in conflict with expected service usage. Examples: traffic usage outside limits, address access outside limits, data rate outside limits, traffic shaping rules not being followed.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify service usage measure at device is consistent with expected service behavior	Device service usage measure is in conflict with expected service usage. Examples: traffic usage too high, address access outside limits, email accessed against policy.	Same as above.
Verify service usage measure in network is consistent with service usage measure at device	Device service usage measure varies significantly from network service usage measure	Same as above.
Verify service usage measure at one point in device is consistent with service usage measure at a second point in device	Service usage measure at one point in device stack that is inconsistent with another point indicates error or potential parasitic usage	Same as above. In some embodiments, the differences in service measures on the device may be used to evaluate the nature of the service usage policy implementation problem.
Verify that service policies in effect are as intended	Service policy setting queries result in settings that are different than intended	In some embodiments, reset service policies and see if error persist. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 27A

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify presence of Service Processor agents	Agent does not respond to agent communication or query-response	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify configuration of Service Processor agents	Agent configuration audit or configuration self-check fails.	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify billing events are reported or are reported properly	Billing Agent query reveals logged billing events that have not been reported.	In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 27B

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify network reported service usage measure are consistent with reported device billing data.	Billing agent is not properly reporting billing events for service usage, transactions, bill by account, or other billing event functions.	In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify device reported service usage measure are consistent with reported device billing data.	Billing agent reports are inconsistent with service usage reports.	In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 27C

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Send test billing event through device and verify it is reported.	Test billing event is nor properly reported by the device.	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify device reports billing events reported from transaction servers.	Transaction server receipts do not correspond with billing events from device.	In some embodiments, perform checks to determine of transaction server receipts are valid. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform on or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify activation tracking system presence, configuration or operation	Activation tracking service is not present, is not providing scheduled network activity reporting, or is exhibiting erroneous reports.	In some embodiments the response is to place the device ID. on a list of devices suspected of having activation tracking functions that have been tampered with for the purpose of central provider billing reconciliation. In some embodiments, install a new copy of the activation tracking service agent software either from a locally stored device copy or a network download. In some embodiments where authorization exists to manage device software and some aspects of service tracking, run further checks on device service integrity such as agent query-response. In some embodiments where authorization exists to manage a device access service connection, send error message to device UI, suspend device or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Verify device standing or service plan standing	No service plan on record or device not authorized	In some embodiments, if device is not yet activated with a service plan, provide UI with activation sequence. In some embodiments, if device is not authorized for service on one of the networks controlled by the Service Controller, send the UI en error message instructing the user how to proceed. In some embodiments, configure the Service Processor for the ambient service intended for that device. In some embodiments, download the appropriate Service Processor agent software that is appropriate for that device.

Figure 27D

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify proper operation of Service Processor agents	Check input to output relationship on Policy Implementation agent, Firewall agent. Check billing event reports to verify events are being recorded. Check application and traffic inspection tagging system correctly tagging traffic. Verify Service Processor heartbeat reports proper agent integrity self-checks, cross-checks and query/response sequences with Service Controller.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Service Processor heartbeat response reports	One or more of the heartbeat reports indicate an error in operation, configuration, or tamper and error prevention system. Heartbeat function not functioning properly but device is still indicating service usage on the network.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Test service event	Service usage reporting system does not properly report test service usage event	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing test event to determine if the device is properly reporting billing events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 27E

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Load a fresh version of Service Processor software and perform integrity reports	After fresh load of Access Control Integrity Agent, agent discovers one or more of the other agents are corrupted.	Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify Service Processor code configuration with agent self diagnosis checks	One or more of the agents indicates an error after running a self-check.	Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform on or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify that device uses service only after being authorized	Device gains access to the network and does not check in with the Access Control Integrity Server and service measures indicate device is on the network.	In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 27F

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify user standing	User does not respond with proper response to UI query such as request for ID., password or biometric input. This process may be part of handling a suspected error.	In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis. In some embodiments, the user may be asked to acknowledge a service overage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service overage acknowledgement.
Agent communications log	Unauthorized communications with one or more agents is detected	In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

Figure 27G

Service Policy Implementation Tamper or Error Protection Technique	Example Error Trigger Criteria	Example Error Responses
Detect or block device networking activity that is potentially harmful for the operation of Service Processor.	Network activity is observed in service monitor reports that fit known patterns that indicated harmful software may be present on device.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized Service Processor software from being loaded.	Access Control Integrity Agent discovers software that is on a known malicious list.	Same as above.
Detect or block unauthorized access of protected Service Processor software or hardware memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized communication with Service Processor software or hardware.	Unauthorized communication is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure loader with signed SW installed into protected memory	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor agents.	Secure communication link is in error or unauthorized access is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh agents with communication links that are in error or entire Service Processor. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor and Service Controller.	Service Processor communication is lost.	Send error message to device UI (if possible), suspend device, place on SPAN, place on watch list, place on further action list or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Execution of Service Processor software within secure memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

Figure 28A

Service Policy Implementation Tamper or Error Protection Technique	Example Error Trigger Criteria	Example Error Responses
Storage of service processor software in secure memory	Secure memory violation or Service Processor stored in non-secure memory	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detection or removal of software thought to be harmful to Service Processor operation.	Unauthorized software is detected.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Recording and reporting of software loading signatures, software activity signatures or network activity signatures for later identification of threat sequences.	Unauthorized software or malicious network activity is detected	Same as above.
Implement critical Service Processor software as a self-refreshing program that resists corruption by running self-audit and reinstall processes such as placing audit function in inaccessible memory or OS functions or bios.	Re-installation function alerts that re-installation has been required. Continued re-installations or failure to re-install alert increases severity of warnings.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Encrypted agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code encryption	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Obfuscated agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code obfuscation	Same as above.
Unique agent identification numbers and signatures	Agent is discovered to have an incorrect ID. or fails signature	Same as above.
Secure agent communication bus	Agent communication bus monitoring discovers unauthorized communication or other unauthorized access to one or more agents is discovered	Same as above.
Agent level message encryption	Agent is found to be communicating without the required level of agent communication encryption	Same as above.

Figure 28B

Service Policy Implementation Tamper or Error Protection Technique	Example Error Trigger Criteria	Example Error Responses
Service control link message level encryption	Unauthorized communication traffic is discovered on service control link	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Service control link transport layer encryption	Unauthorized communication traffic is discovered on service control link	Same as above.
Agent communication access permissions	Unauthorized communication is discovered with one or more agents	Same as above.
Agent communication log	Unauthorized communication is discovered with one or more agents	Same as above.
Encrypted agent code for downloads	Agent download is found to have incorrect or absent encryption or signature	Same as above.
Secure downloader memory	Unauthorized access to or storage in secure downloader memory is discovered	Same as above.

Figure 28C

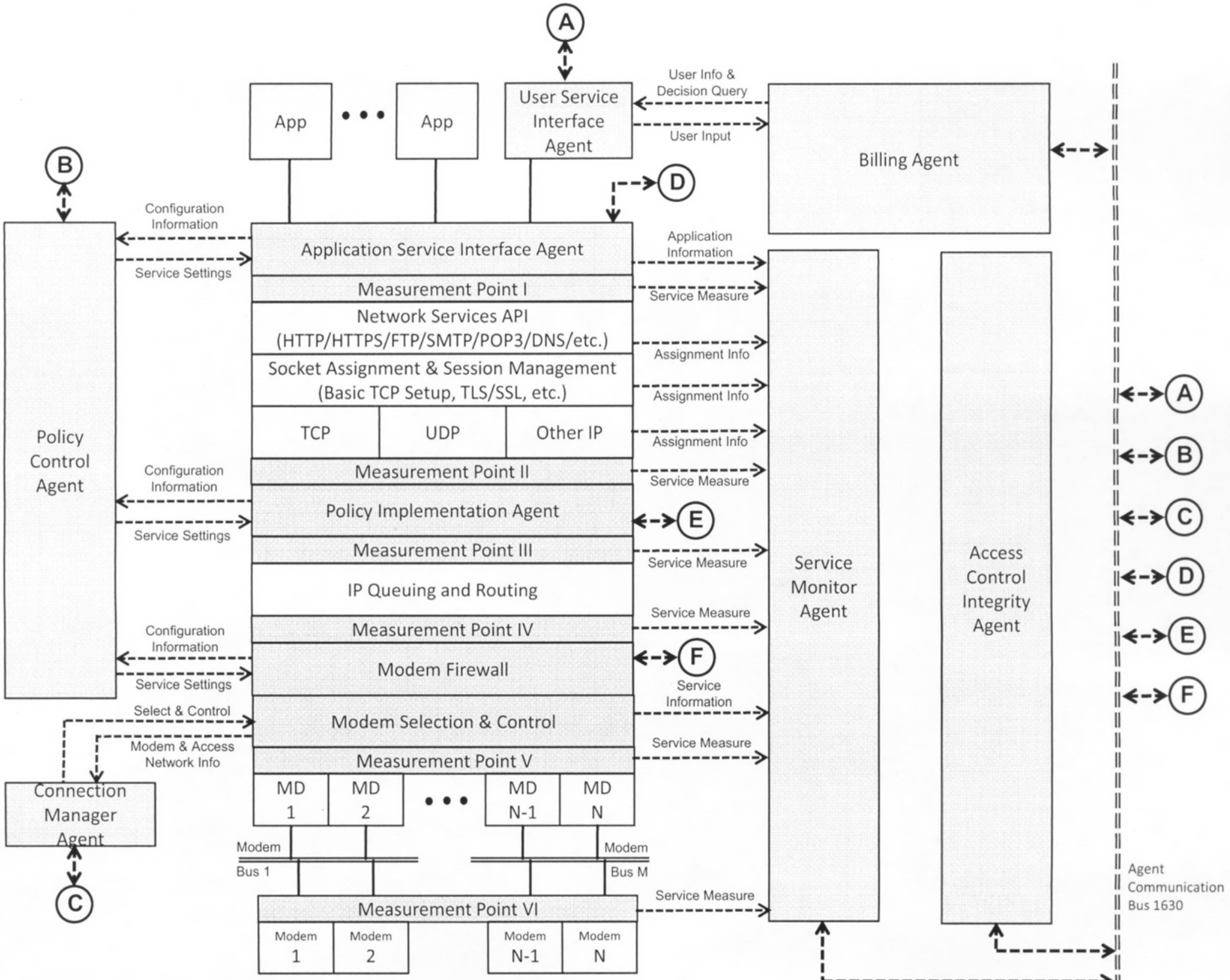

A
App
App
User Service Interface Agent
User Info & Decision Query
User Input
Billing Agent
B
D
Configuration Information
Service Settings
Application Service Interface Agent
Application Information
Measurement Point I
Service Measure
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Assignment Info
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
Assignment Info
TCP
UDP
Other IP
Assignment Info
Policy Control Agent
Configuration Information
Measurement Point II
Service Measure
Service Settings
Policy Implementation Agent
E
Measurement Point III
Service Measure
IP Queuing and Routing
Service Measure
Measurement Point IV
Configuration Information
Modem Firewall
F
Service Information
Service Settings
Select & Control
Modem Selection & Control
Service Measure
Modem & Access Network Info
Measurement Point V
Service Monitor Agent
Access Control Integrity Agent
MD 1
MD 2
MD N-1
MD N
Connection Manager Agent
Modem Bus 1
Modem Bus M
C
Service Measure
Measurement Point VI
Modem 1
Modem 2
Modem N-1
Modem N
A
B
C
D
E
F
Agent Communication Bus 1630

Figure 29

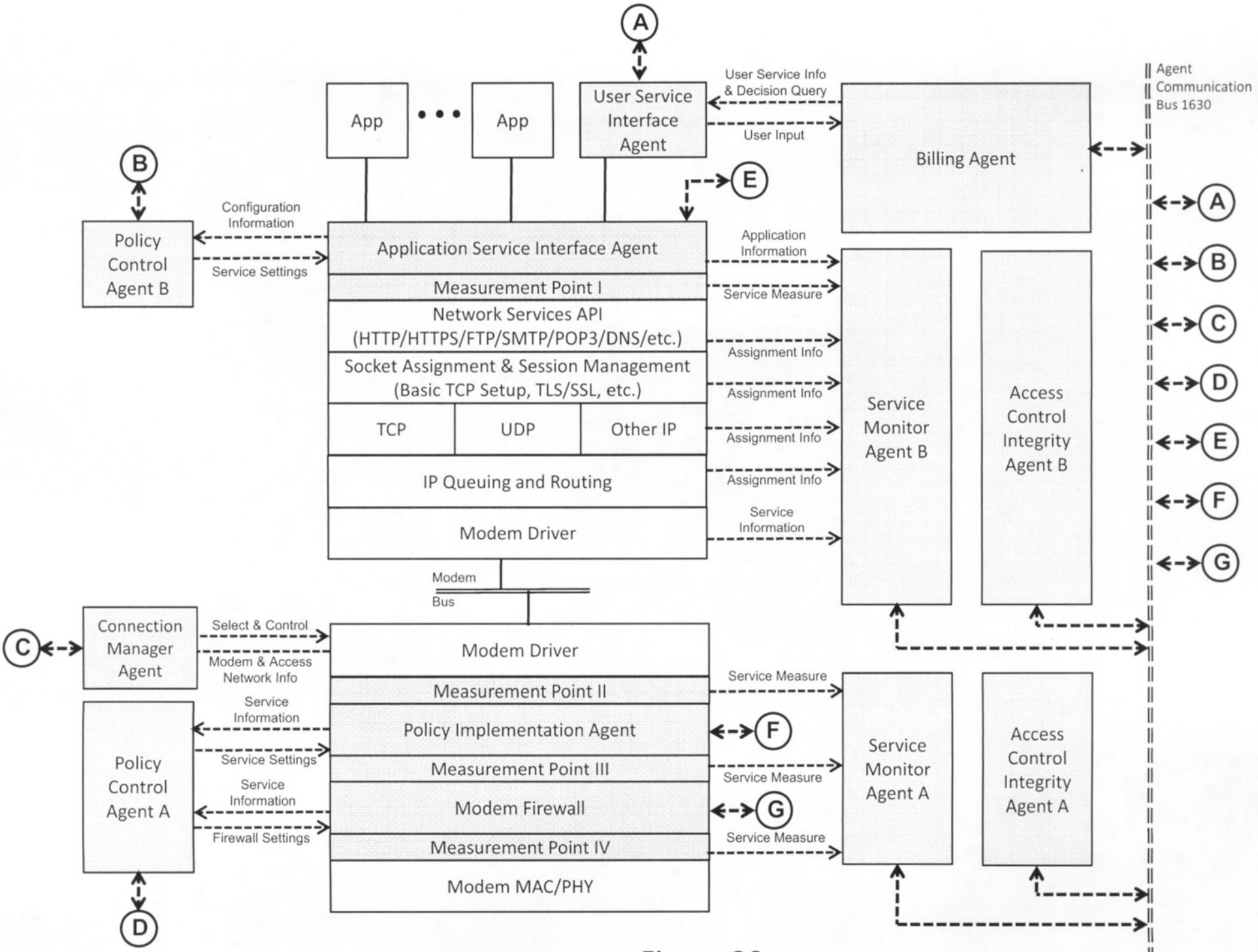

A
App
App
User Service Interface Agent
User Service Info & Decision Query
User Input
Billing Agent
Agent Communication Bus 1630
B
E
Configuration Information
Policy Control Agent B
Service Settings
Application Service Interface Agent
Application Information
Measurement Point I
Service Measure
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Assignment Info
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
Assignment Info
TCP
UDP
Other IP
Assignment Info
IP Queuing and Routing
Assignment Info
Modem Driver
Service Information
Service Monitor Agent B
Access Control Integrity Agent B
Modem Bus
C
Connection Manager Agent
Select & Control
Modem & Access Network Info
Modem Driver
Measurement Point II
Service Measure
Service Information
Policy Implementation Agent
F
Service Settings
Measurement Point III
Service Measure
Policy Control Agent A
Service Information
Modem Firewall
G
Firewall Settings
Measurement Point IV
Service Measure
Modem MAC/PHY
Service Monitor Agent A
Access Control Integrity Agent A
D

Figure 30

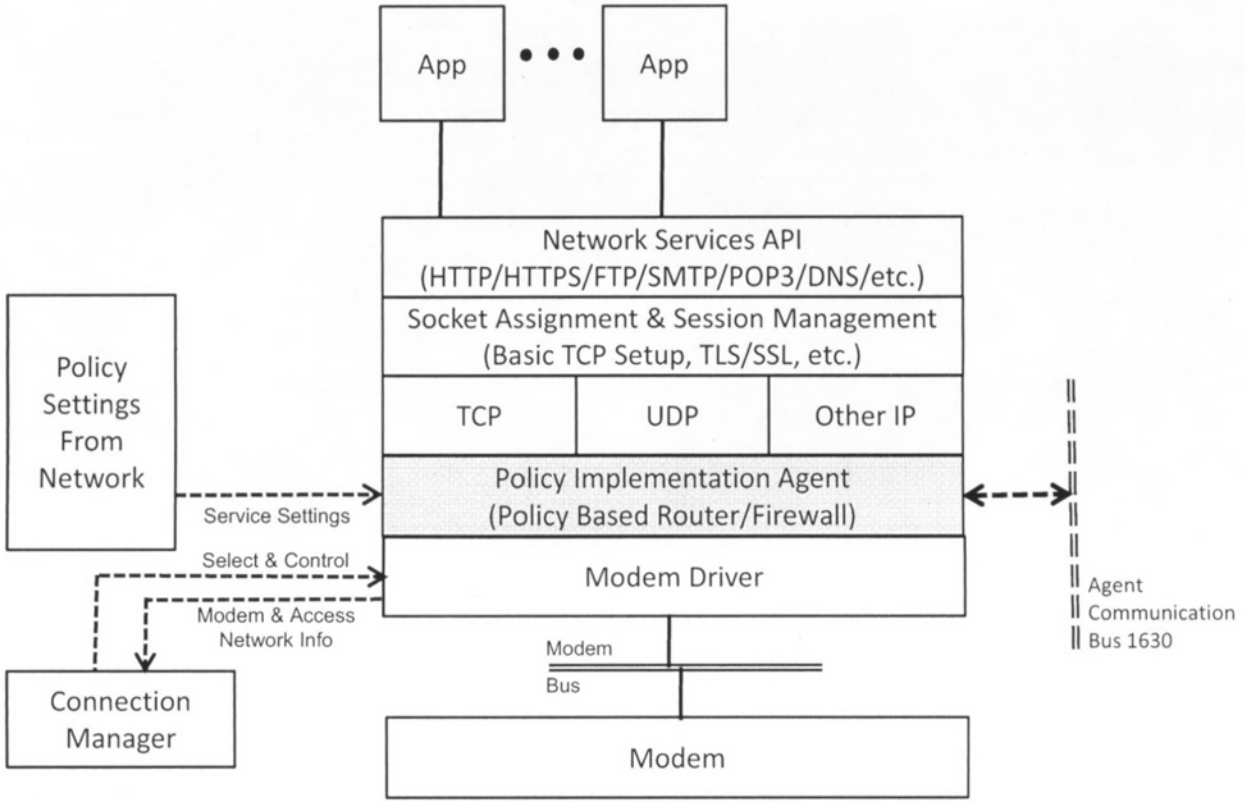

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Policy Implementation Agent
(Policy Based Router/Firewall)
Modem Driver
Modem
Bus
Modem
Policy
Settings
From
Network
Service Settings
Select & Control
Modem & Access
Network Info
Connection
Manager
Agent
Communication
Bus 1630

Figure 31

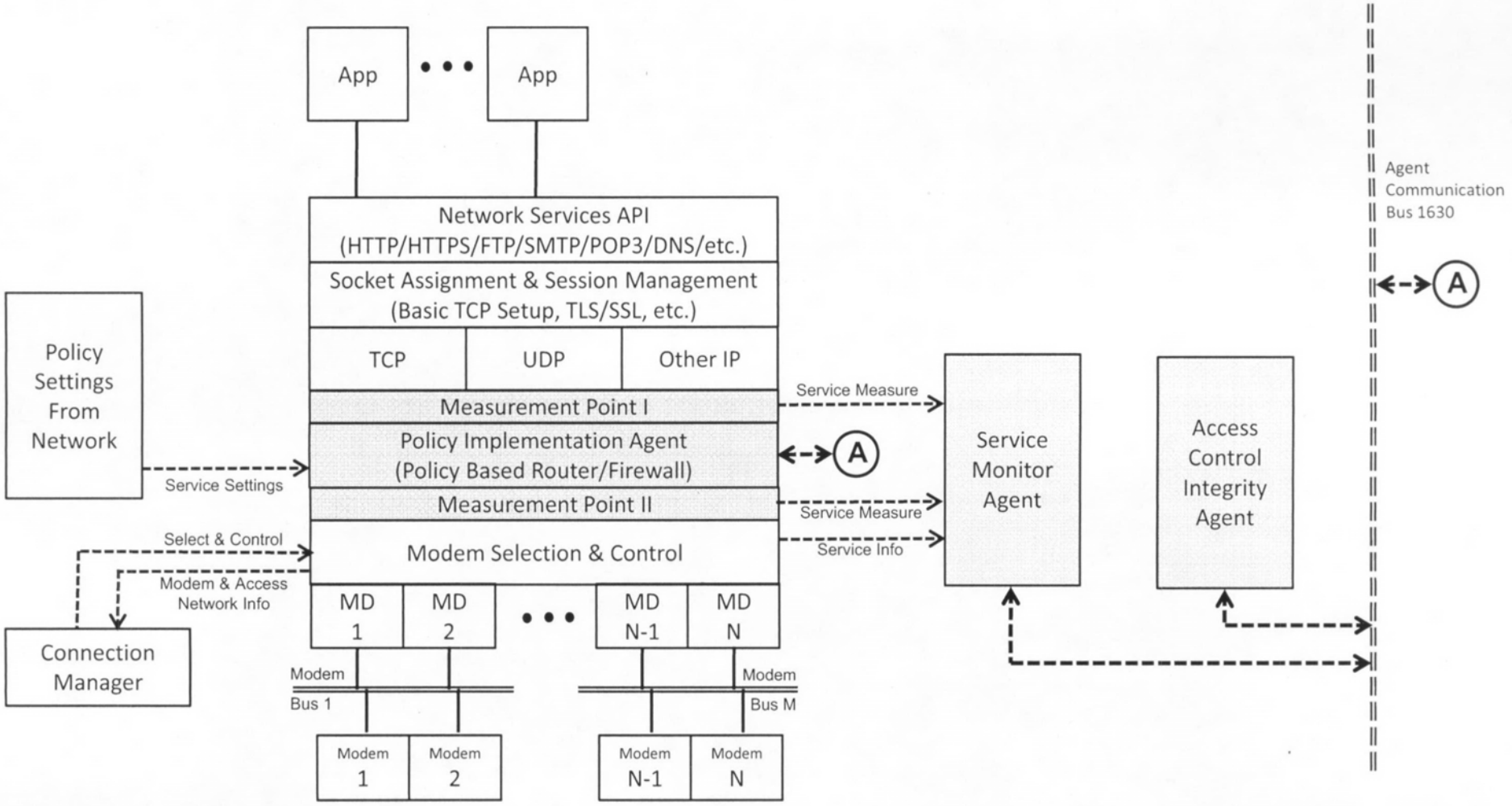

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Measurement Point I
Policy Implementation Agent
(Policy Based Router/Firewall)
Measurement Point II
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem Bus 1
Modem Bus M
Modem 1
Modem 2
Modem N-1
Modem N
Policy Settings From Network
Service Settings
Select & Control
Modem & Access Network Info
Connection Manager
Service Measure
Service Measure
Service Info
Service Monitor Agent
Access Control Integrity Agent
Agent Communication Bus 1630
A
A

Figure 32

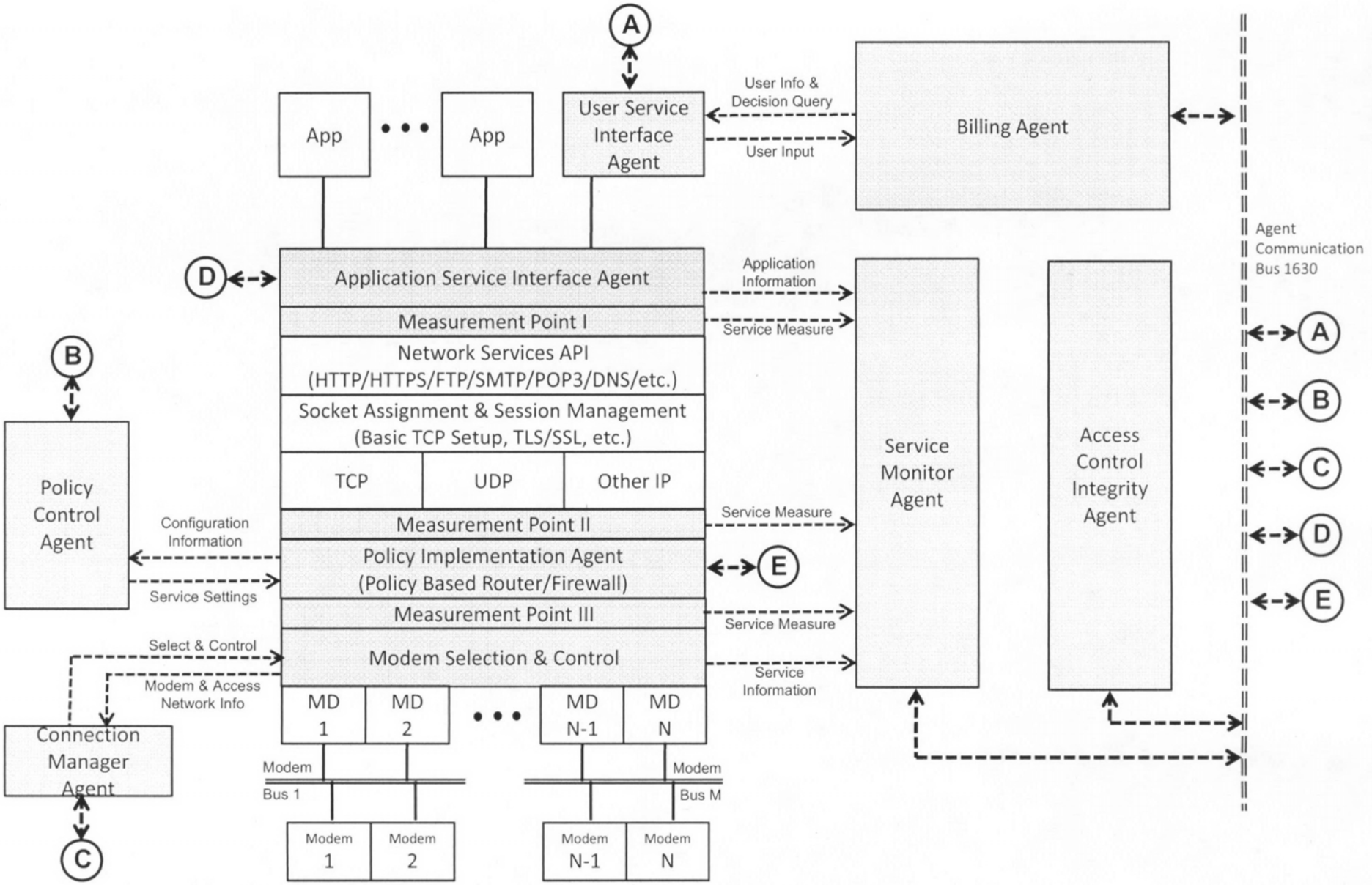

A
App
App
User Service Interface Agent
User Info & Decision Query
User Input
Billing Agent
Agent Communication Bus 1630
D
Application Service Interface Agent
Application Information
Measurement Point I
Service Measure
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
B
Policy Control Agent
Configuration Information
Measurement Point II
Service Measure
Policy Implementation Agent (Policy Based Router/Firewall)
E
Service Settings
Measurement Point III
Service Measure
Select & Control
Modem Selection & Control
Service Information
Modem & Access Network Info
MD 1
MD 2
MD N-1
MD N
Connection Manager Agent
Modem Bus 1
Modem Bus M
Modem 1
Modem 2
Modem N-1
Modem N
C
Service Monitor Agent
Access Control Integrity Agent

Figure 33

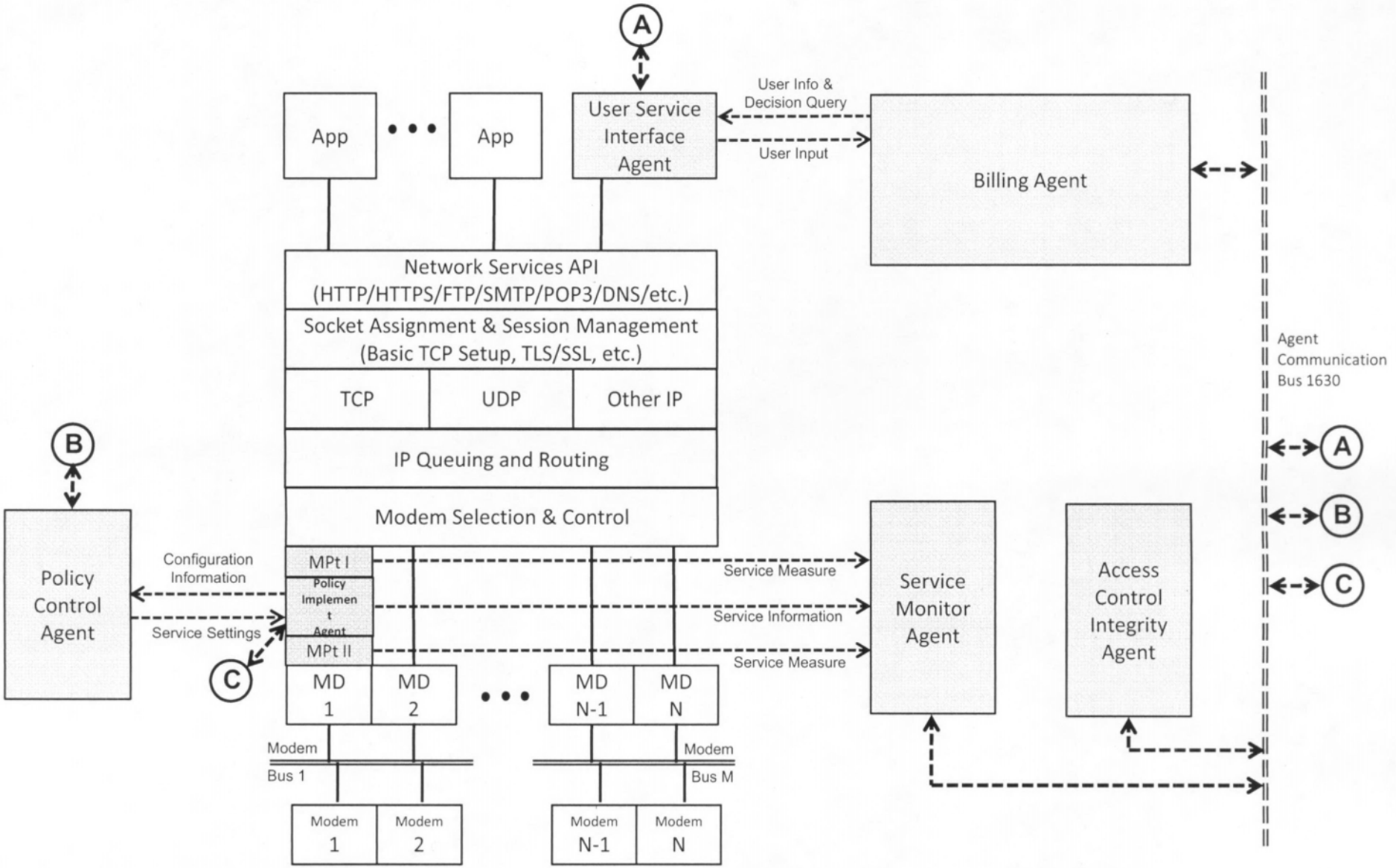

A
App
App
User Service Interface Agent
User Info & Decision Query
User Input
Billing Agent
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
Agent Communication Bus 1630
B
Policy Control Agent
Configuration Information
Service Settings
MPt I
Policy Implement Agent
MPt II
C
Service Measure
Service Information
Service Measure
Service Monitor Agent
Access Control Integrity Agent
MD 1
MD 2
MD N-1
MD N
Modem Bus 1
Modem Bus M
Modem 1
Modem 2
Modem N-1
Modem N

Figure 34

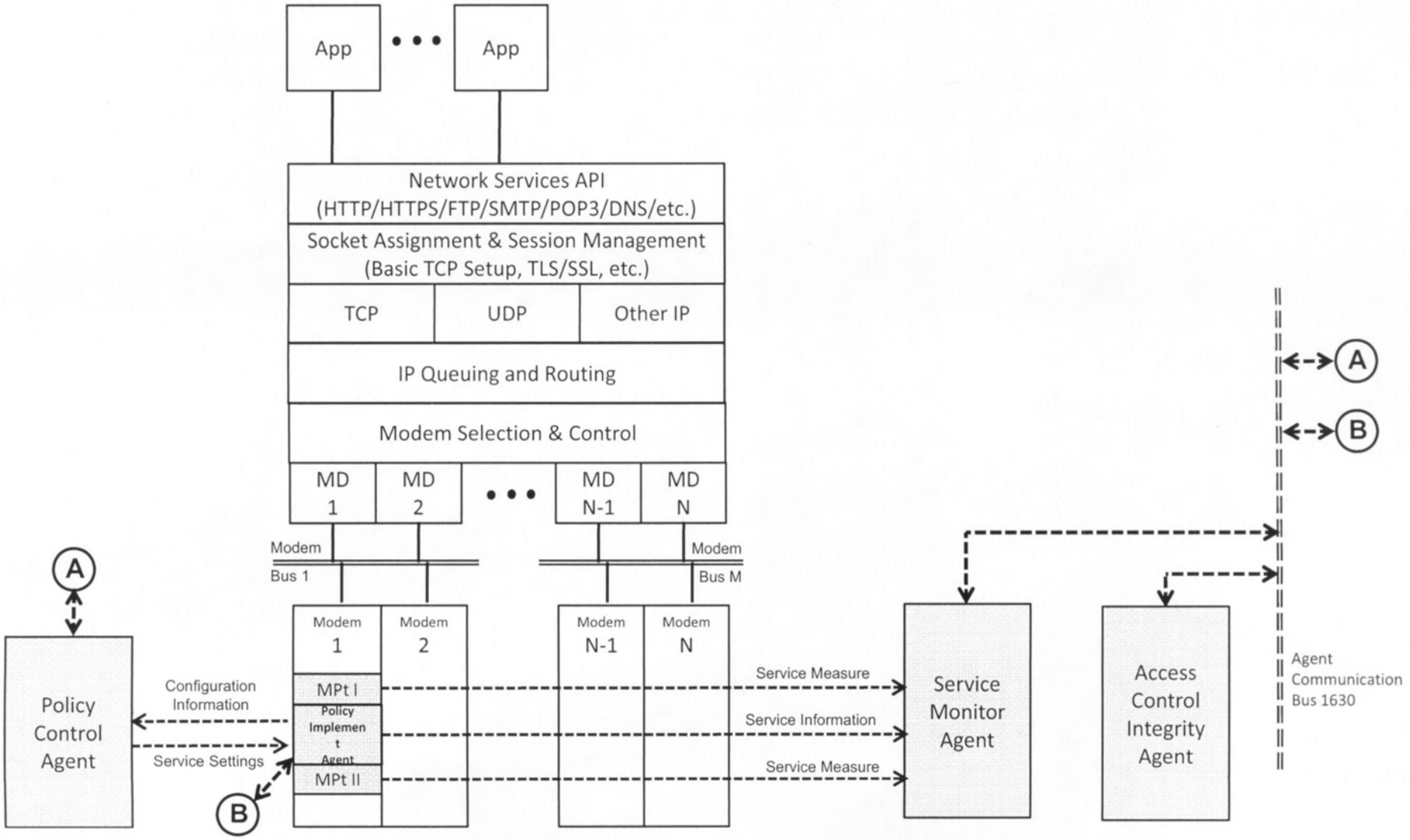

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem Bus 1
Modem Bus M
Modem 1
Modem 2
Modem N-1
Modem N
MPt I
Policy Implement Agent
MPt II
A
B
Policy Control Agent
Configuration Information
Service Settings
Service Measure
Service Information
Service Measure
Service Monitor Agent
Access Control Integrity Agent
Agent Communication Bus 1630

Figure 35

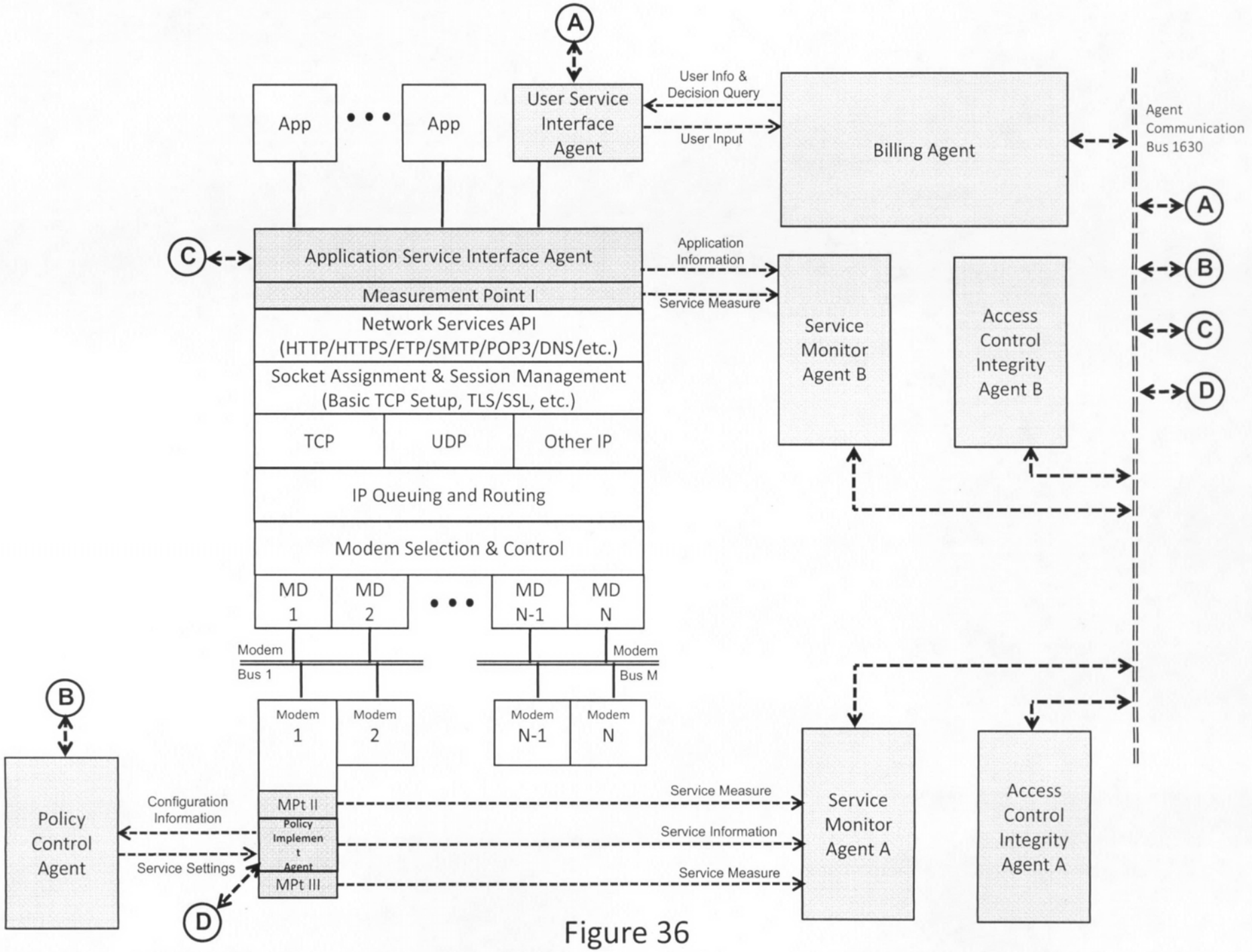

A
App
App
User Service Interface Agent
User Info & Decision Query
User Input
Billing Agent
Agent Communication Bus 1630
C
Application Service Interface Agent
Application Information
Measurement Point I
Service Measure
Service Monitor Agent B
Access Control Integrity Agent B
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem Bus 1
Modem Bus M
Modem 1
Modem 2
Modem N-1
Modem N
B
Policy Control Agent
Configuration Information
Service Settings
MPt II
Policy Implement Agent
MPt III
Service Measure
Service Information
Service Measure
Service Monitor Agent A
Access Control Integrity Agent A
D

Figure 36

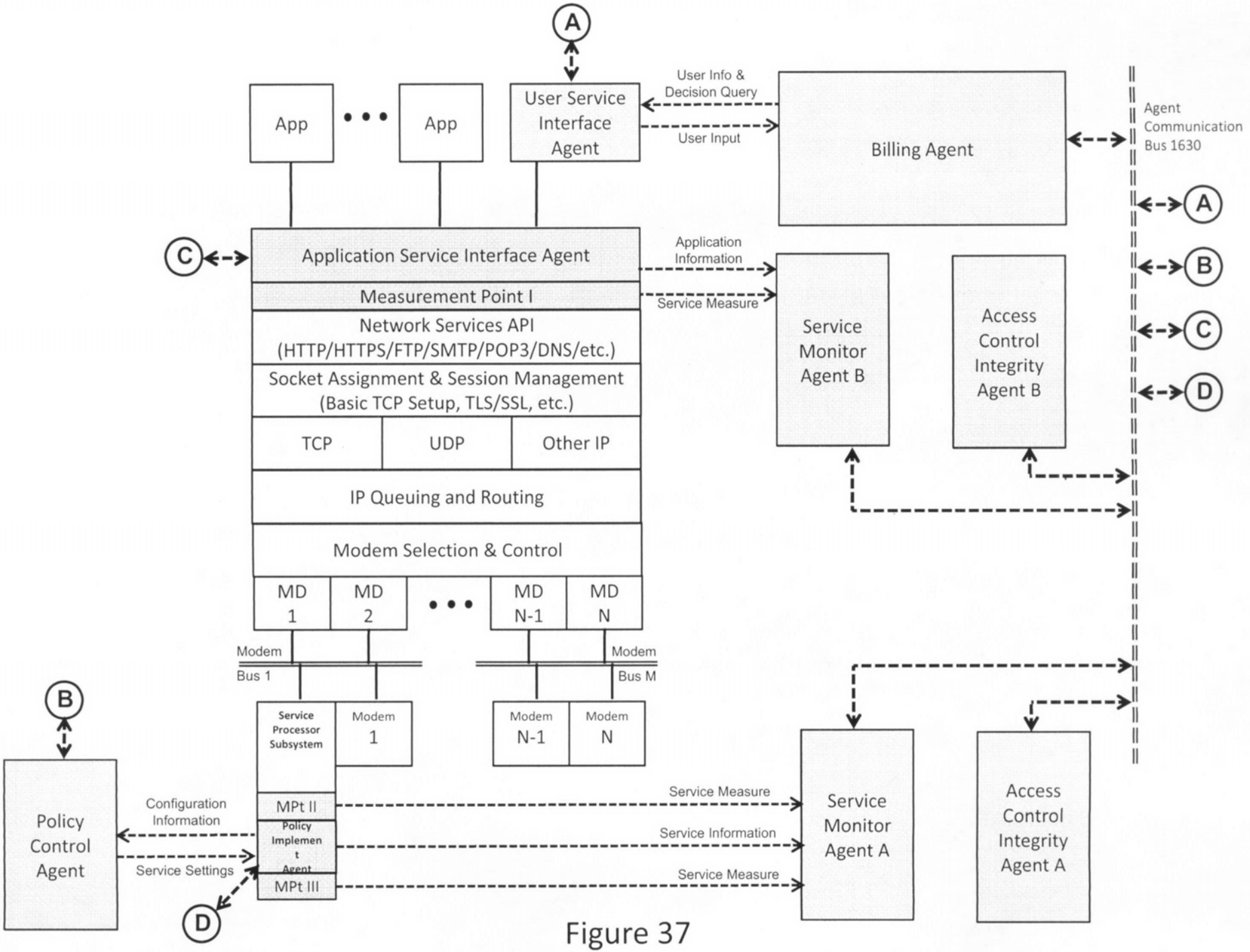
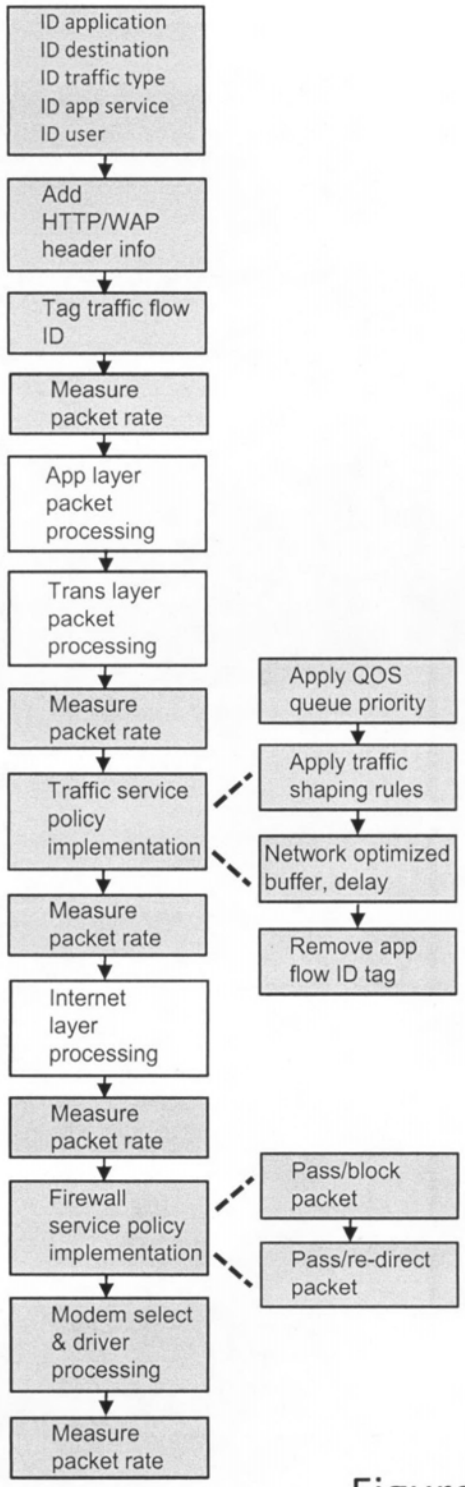

A
App
App
User Service Interface Agent
User Info & Decision Query
User Input
Billing Agent
Agent Communication Bus 1630
A
B
C
D
C
Application Service Interface Agent
Application Information
Measurement Point I
Service Measure
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Service Monitor Agent B
Access Control Integrity Agent B
Modem Bus 1
Modem Bus M
B
Service Processor Subsystem
Modem 1
Modem N-1
Modem N
Policy Control Agent
Configuration Information
Service Settings
MPt II
Policy Implement Agent
MPt III
D
Service Measure
Service Information
Service Measure
Service Monitor Agent A
Access Control Integrity Agent A

Figure 37


ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy implementation
Apply QOS queue priority
Apply traffic shaping rules
Network optimized buffer, delay
Remove app flow ID tag
Measure packet rate
Internet layer processing
Measure packet rate
Firewall service policy implementation
Pass/block packet
Pass/re-direct packet
Modem select & driver processing
Measure packet rate
Upstream Flow (device to network)

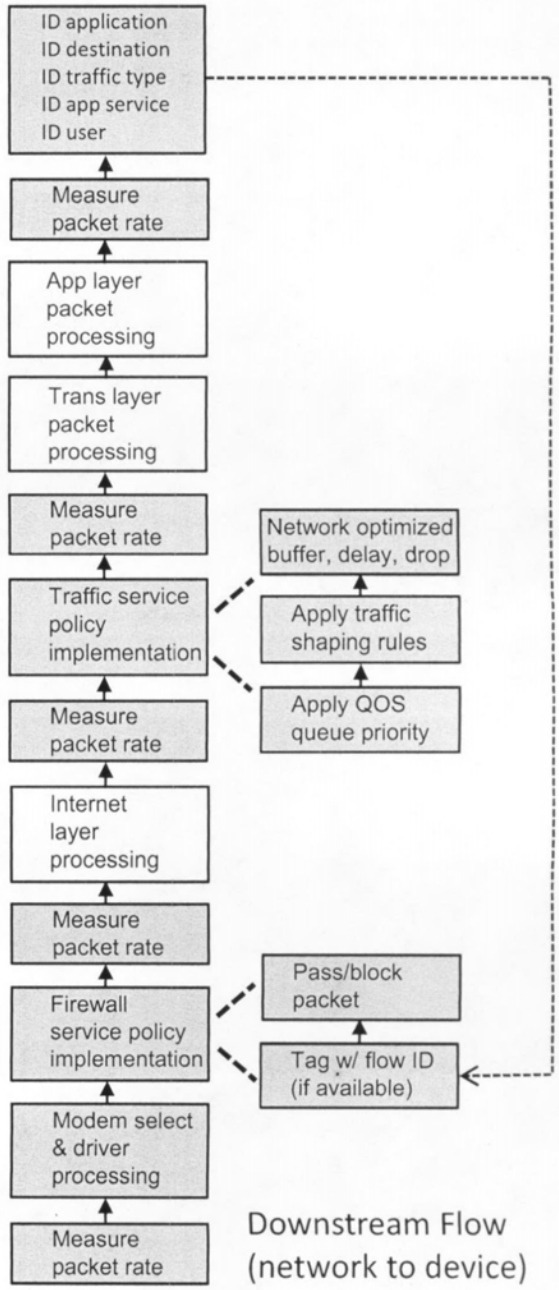

ID application
ID destination
ID traffic type
ID app service
ID user
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy implementation
Network optimized buffer, delay, drop
Apply traffic shaping rules
Apply QOS queue priority
Measure packet rate
Internet layer processing
Measure packet rate
Firewall service policy implementation
Pass/block packet
Tag w/ flow ID (if available)
Modem select & driver processing
Measure packet rate
Downstream Flow (network to device)

Figure 38

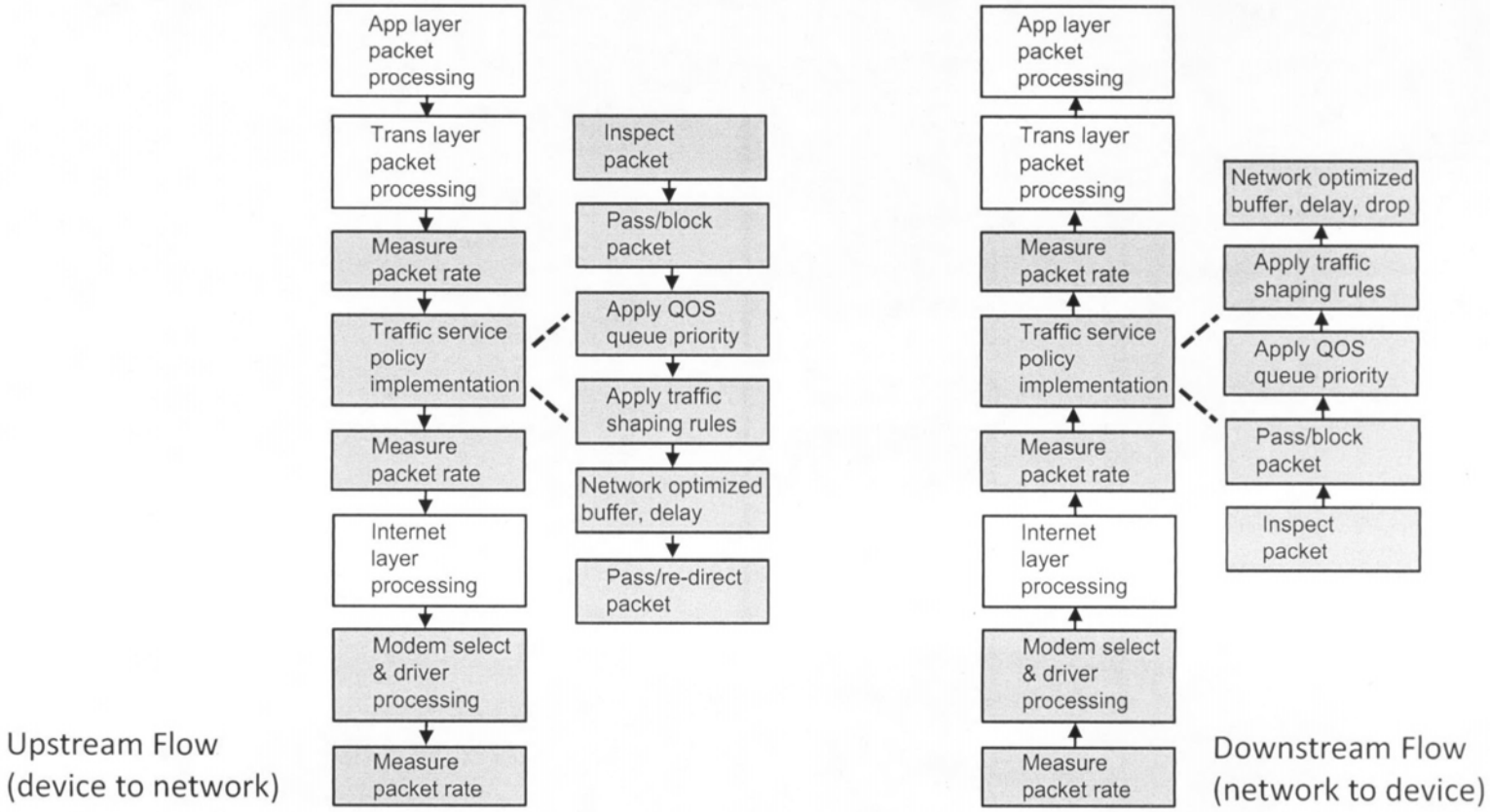

App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy implementation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Inspect packet
Pass/block packet
Apply QOS queue priority
Apply traffic shaping rules
Network optimized buffer, delay
Pass/re-direct packet
Upstream Flow (device to network)
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy implementation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Network optimized buffer, delay, drop
Apply traffic shaping rules
Apply QOS queue priority
Pass/block packet
Inspect packet
Downstream Flow (network to device)

Figure 39

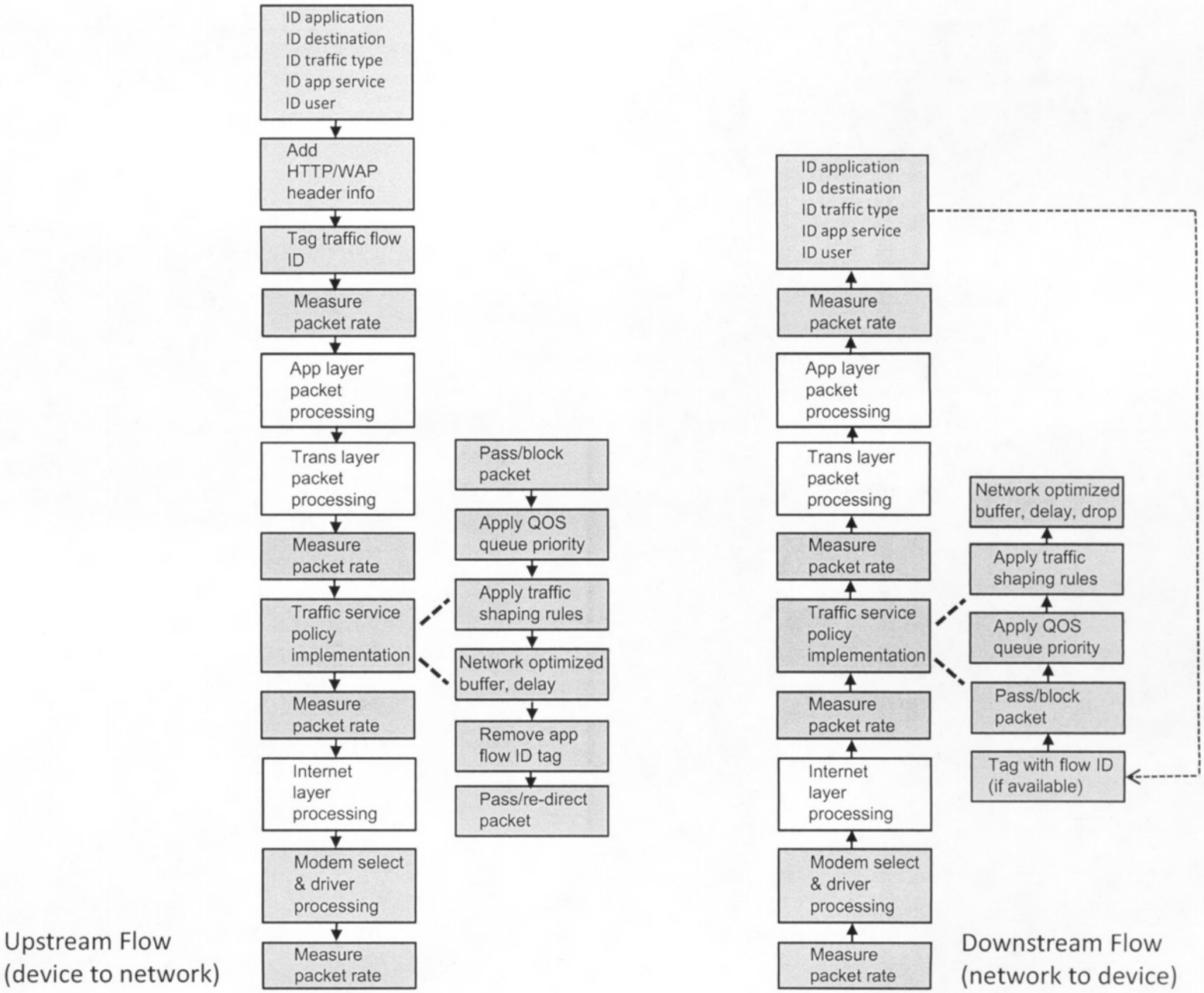

ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy implementation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Pass/block packet
Apply QOS queue priority
Apply traffic shaping rules
Network optimized buffer, delay
Remove app flow ID tag
Pass/re-direct packet
Upstream Flow
(device to network)
ID application
ID destination
ID traffic type
ID app service
ID user
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy implementation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Network optimized buffer, delay, drop
Apply traffic shaping rules
Apply QOS queue priority
Pass/block packet
Tag with flow ID (if available)
Downstream Flow
(network to device)

Figure 40

Example Device CRM Data Collection and Reporting Classification	Partial Description	Example Sensitivity Level Classification	Example Authorization Level to Include in Report
Basic non-specific service usage parameters	User sensitive information is filtered from this report which is used for purposes such as service control, service control integrity monitoring or network traffic analysis.	Low	None
Service billing events or service plan selection events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with basic service agreement or enterprise agreement
Transaction billing events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with central billing agreement or enterprise agreement
Device location – customer location based service assist	Reports customer location for the purpose of assisting with location based services such as directions, yellow pages, shopping and social networking.	High	Customer authorization with basic service agreement or enterprise agreement
Device location – device or people tracking	Reports customer location for the purpose of providing tracking services for the device or the user.	High	Customer authorization with separate device tracking service agreement or enterprise agreement
Transaction associated information	Reports customer information such as networking activity, location, advertising usage, shopping behavior that is associated with a commerce transaction or happens around the same time as the transaction.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
URL history	Reports customer web surfing history.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
Served and visited advertisement history	Reports the advertisements served to the user or which advertisements the user responded to. This information may be used to determine customer preferences or for a revenue sharing relationship with the advertisers.	Medium	Customer authorization – potential service discount, perk or upgrade or enterprise agreement
911 Service usage and location trace log	This log contains all information pertinent to emergency service personnel responding to a 911 call or other emergency situation. In some embodiments this information is password protected and generally not available to the service provider unless it happens to also be contained in reports authorized by the consumer as in the examples above.	Very High	Available only for 911 support or enterprise agreement

Figure 41

Partial List of Example Service Policy Functionality Embodiments	Partial Description of Functionality Example	Example Authorization Level Required to Implement Embodiment
Block downstream or upstream traffic	Various embodiments block traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of command usage are access control prior to authorization, access control policy limits as defined by service plan or special device type, access control for ambient activation services, access control for error handling or access control for tamper prevention. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Basic authority to pass or block traffic for access control, authorization, ambient services, or plan specific services typically may be provided by the user when they acknowledge the service plan agreement. Authorization to block traffic access as part of controlling user service costs typically may be provided by they service plan agreement options the user chooses to manage cost or may be provided when the user acknowledges the limitations in the UI notifications.
Pass downstream or upstream traffic	Various embodiments allow traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of command usage are access control prior to authorization, access control policy limits as defined by service plan or special device type, access control for ambient activation services, access control for error handling or access control for tamper prevention. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Same as above.
Limit maximum data rate	Various embodiments limit maximum data rate for traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of how this command can be implemented include limiting data rate to the device according to service plan; limiting data rate by network address identifier, application or content type for the purpose of implementing a tiered garden; limiting data rate in to different levels according to the type of access technology used by the present network connection; limiting data rate to different levels according to the service provider for the present network; or limiting data rate according to an agreement or lack of agreement with a transaction provider. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.
Analyze traffic	Provides capability resident on the device to analyze device or user traffic statistics to determine how to implement adaptive policy control or how best to assist the user with notification messages. In some embodiments it is important to perform traffic analysis locally on the device to reduce network chatter with the Control Processor or to maintain user CRM privacy levels by not sharing sensitive raw traffic usage history needed to determine implementation of less sensitive service control policies. Typical but non-exhaustive examples of command usage are analyzing traffic usage statistics or patterns to determine compliance with service plan limits; analyzing traffic usage statistics or patterns to determine likely future compliance with service plan limits; analyzing traffic statistics or patterns to categorize usage according to network address identifiers, applications, content types, network types or central providers; analyzing traffic demand vs. usage statistics or patterns to determine if user may be better served with another service plan; analyzing traffic statistics or patterns to identify potential tamper threats. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode, but adaptive application of the analysis results is typically associated with adaptive policy control mode.	Authorization to analyze traffic for local device service policy control purposes or 911 service typically may be provided for in the basic service contract. Authorization to transmit a complete or filtered version of the traffic analysis to the Service Controller typically may be provided under user selected options in the service plan contract.
Successive limitation	Provides capability to begin with one limit on access or data rate according to a set of defined service usage trigger criteria, to further limit access or data rate according to said criteria, and then to successively remove limits according to said criteria. In some embodiments this function provides for service usage that starts at a given level for one or more service aspects, but as said service aspect exhibits usage that potentially threatens an overage on service plan limits then the level of service for said service aspect is reduced successively until the threat of service plan overage is reduced or eliminated. In some embodiments, the limits on service level for said service aspect are eventually removed either all at once or successively over a specified time period or set of time periods so that the limits on service level for said service aspect are eventually removed if the service aspect is used less vigorously for a period of time. In this type of embodiment the projection for future service usage by a given service aspect is assisted by the analyze traffic statistics function. As a more specific example, the service aspect may be a URL address that is popular with the user and demands a high service consumption, and the data rate allowed to that URL may start at a relatively high level when the user first begins to surf and as long as the surfing session is finished quickly there is never a reduction in service level, but if the user surfs for a longer time so that service usage begins to threaten plan limit overage, the data rate allowed to that URL is successively reduced the longer the surfing session occurs. Continuing this example embodiment, if the URL is not visited for a defined period of time then the data rate limitation may be removed in steps over multiple pre-defined time periods, or may be removed all at once back to the initial data rate established in the service policy for that URL. Other specific embodiment examples include email download or upload data rate; download or upload rates for certain types of file transfers; or download or upload rates for a given network access technology or central provider. This command is associated with adaptive policy control mode for the Service Processor. In more advanced adaptive embodiments, the policy control system first identifies those service aspects that are consuming a large percentage of the service usage and then begins to successively limit service level only for these highest usage service aspects so that all other service aspects that are not responsible for potential service plan limit overage continue to receive relatively high service levels. In another embodiment, some high usage service aspects may be exempt or partially exempt from limitations in service level, as for example a service aspect that is associated with a secondary source of service or transaction payment or that may be separately accounted for in the service plan usage reporting.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.

Figure 42A

Partial List of Example Service Policy Functionality Embodiments	Partial Description of Functionality Example	Example Authorization Level Required to Implement Embodiment
Limit email file transfers	Sets and enforces limits on email downloads. In some embodiments this can include use of the successively limit functionality. In some embodiments, this is accomplished by identifying specific email downloads or uploads and controlling traffic for those traffic flows. In other embodiments, this includes interacting with the email application to set download or upload file settings. This functionality may be implemented in instantaneous policy implementation mode or adaptive policy control mode, with the more advanced functionality such as successive limitation on email file transfers being implemented in the adaptive policy control mode.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.
Seek to manage below service limit	Implements adaptive policy control in an attempt to manage service usage to reduce service plan limit overages. In some embodiments there are successive limits on service level for overall traffic, or for the highest usage service aspects, with the successive limits being lowered until average service usage is projected to be below service plan limits. The algorithms that may be applied to achieve this adaptive service level limitation are quite varied and only a few are given here. In one embodiment, the service usage for the service plan period is projected using the analyze traffic functionality, and overall device data rate is successively limited until service usage is projected to be below the service plan limit. In another embodiment, the analyze traffic functionality is used to identify those service aspects that are causing the majority of the service plan usage, and then each of those service plan aspects are limited using the successive limitation functionality, with the service level limitations being based on the traffic usage patterns and specific application scenarios for each service aspect. For example, in some embodiments the service aspects that are creating the most service usage are subjected to more service level limitation than service aspects that are creating less service usage. Service usage may be defined as usage of a raw service measurement such as total data consumption, files downloaded or time spent on network, or it may be translated into an economic measure using the lookup service cost functionality. In some embodiments, the period of time elapsed in the service accounting period is taken into account in determining...	Same as above.
Synchronize service usage counters	Synchronizes service usage counters on device from time to time to minimize service accounting errors between the device data base and the central billing data base. In some embodiments this is a part of the Service Processor heartbeat communication system that need not happen every heartbeat. In some embodiments this occurs with a request for update by the device to the central billing system or to a server function in the Ser	Provided for in the basic service agreement.
Lookup service cost	Provides a data base of service usage vs. cost for each type of service offered on the device. Provides for a lookup function of service cost.	Same as above.
Convert service usage to service cost	Uses the service cost vs. usage lookup function to transform one or more service usage aspects to one or more service cost aspect. One example embodiment provides a service cost measure for one specific aspect of service usage, for example total data consumed over a period of time. Another example embodiment provides a total service cost measure for all service usage over a period of time.	Same as above.
Notify user of service overage	Sends a notification message or screen to the UI to inform the user that the one or more aspects of service usage has exceeded the specified limits of one or more service plans. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Same as above.
Project service usage	Uses the analyze traffic functionality and projects an estimate of what the traffic usage will be at the end of a service plan measurement interval if the service usage does not change. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.

Figure 42B

Partial List of Example Service Policy Functionality Embodiments	Partial Description of Functionality Example	Example Authorization Level Required to Implement Embodiment
Notify user of service cost overage	Performs a service cost estimate based on one or more aspects of service usage and informs the user that the one or more aspects of service cost has exceeded the specified limits of a service plan. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Provided for in the basic service agreement.
Notify user of usage behavior likely to run over service usage limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, notifies the user if the projected usage is over the service plan limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Notify user of usage behavior likely to run over cost limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user if the projected cost is over the service plan cost associated with the service plan service limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Project user service cost if usage behavior continues	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user of what the projected cost will be if the service usage behavior remains the same. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Limit access likely to cause overage and notify	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, if the service usage is projected to go over the service limit, notifies the user that limits are being applied to keep service usage or cost under the service limit, applies limits to various aspects of service usage to bring down usage so that projections are within service limits. In one embodiment, the seek to manage below service limit functionality is used.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.
Require acknowledgement of notification	Requires the user to acknowledge a notification of potential service or cost overage or a notification of an option to limit the service overage or cost of service overage.	Provided for in the basic service agreement.
Log or report acknowledgement of notification	In some embodiments, the user acknowledgement of notification is stored, or sent to the Service Controller, or stored and later sent to the service Controller.	Same as above.
Notify user of service plan options prior to running over service usage limit	Notifies the user of options to extend the service plan limit before reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Notify user of service plan options after running over service usage limit	Notifies the user of options to extend the service plan limit after reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Time of day variations	Each of the functionalities for traffic control, service cost, service limits may be modified with a time of day variation so that the values used are different for different times of day.	Same as above.

Figure 42C

Partial List of Example Service Policy Functionality Embodiments	Partial Description of Functionality Example	Example Authorization Level Required to Implement Embodiment
Access control enable list	List of service usage activities that are enabled.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the control data base.
Access control block list	List of service usage activities that are blocked.	Same as above.
User service control option UI	Provides the user with a list of options for how they would like to control service usage or service cost.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to to service controller, VSP or other network function with proper credentials to access the UI pass through screens.
User service notification option preference	Provides the user with a list of options for how they would like service notification information to be displayed. In some embodiments provides the user with the option to turn off one or more aspects of service notification. In some embodiments the user is not allowed to turn off notification for service usage events that require user decision or acknowledgement.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to to service controller, VSP or other network function with proper credentials to access the UI pass through screens.
User CRM or service usage monitoring filtering option preference	Filters the device and/or user information that is being collected before it is reported to the network to maintain the desired level of user privacy. In some embodiments the user defines preferences on user privacy that are used to define the filter settings.	In some embodiments this is not accessible by the network and only may be modified by the user. In other embodiments it may be read but not written by the network and in this case authorization is restricted to service controller, VSP or other network function with proper credentials to access the filter settings data base. In some embodiments the network is allowed to change the CRM filter settings and in this case Authorization restricted to service controller, VSP or other network function with proper credentials to access the CRM filter settings data base.
Service usage billing event record	A record of service usage billing events. In some embodiments this record is transmitted to the billing server or another network function to aid service billing or billing reconciliation.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Bill by account	The bill by account embodiments provide for service billing to accounts different than the main user account, for example tracking network device chatter that is not desired to be billed to the user, transaction partner access costs that are shared with or billed to the transaction partner, ambient service cost tracking, tracking temporary account costs, etc.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Central billing transaction and event recording	Billing event tracking and reporting associated with the central provider open billing embodiments. Some embodiments include generation of billing certificates or receipts. In some embodiments the device may serve as a billing feed.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.

Figure 42D

Partial List of Example Service Policy Functionality Embodiments	Partial Description of Functionality Example	Example Authorization Level Required to Implement Embodiment
Service owner registration or re-registration	Function that allows a portion of the device credentials to be programmed to indicated the VSP.	In some embodiments authorization to write the device is restricted with security signatures or other security methods to the VSP and possibly the central provider. Some embodiments involve provisions to report to a network function when the VSP settings are changed or the software is uninstalled. Other embodiments involve restoring VSP settings or software if removed.
Credentials swap	Function that provides for swapping of credentials, for example temporary credentials to permanent credentials.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the credentials data base.
Account information swap	Function that provides for swapping the account information, for example temporary account to permanent account.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the activation service profile data base.
Configure or re-configure service processor for new device service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Ambient service profile definition	Function that provides for service processor programming for all the information that defines the ambient service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the ambient service profile data base.
Analyze service usage statistics	VSP function to analyzer service usage statistics for a device, defined group of devices, defined group of service plans or service profiles, defined group of users or other groupings.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Dry lab test new service policy	Allows simulated testing of draft service profiles and/or service plans against device usage statistics for a defined group of devices or users or service profiles, or against simulated device service usage behavior. Some embodiments show the estimated profitability of proposed service profile and service plan. Some embodiments allow decomposition of the service usage statistics to identify the user group service usage activities that may be modified by changing the service usage control policies or made more profitable by changing the service plan billing policies.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Beta test publishing system	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters for a beta test device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Publish new service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters for a production device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.

Figure 42E

Partial List of Example Service Policy Functionality Embodiments	Partial Description of Functionality Example	Example Authorization Level Required to Implement Embodiment
Roaming selection service	Function that surveys available roaming service partners, looks up the billing rates for the partners, and displays to the user the set of choices and billing rates. In some embodiments the roaming partner billing rates for one or more roaming partners are applied to a typical user service usage scenario for the purpose of estimating possible projected roaming costs and displaying those costs to the user. In some embodiments the roaming data is stored locally on the device and periodically updated with network refreshes, while in other embodiments the data base is looked up at the time of service. In some embodiments, the user is asked if they would like to modify their service usage notification or control profiles to save roaming costs and if the user responds yes they are provided with a set of options for changing service usage notification or service usage control policies.	Authorization to modify the policies typically restricted to the VSP or other entity responsible for managing the roaming service.
Roaming usage count	Provides a service usage estimate to the user while roaming.	Same as above.
Roaming cost service	Provides a service cost estimate to the user while roaming.	Same as above.
Roaming policy control service	Provides the user or VSP with the capability to switch service usage notification or service usage control policies while roaming. Some embodiments provide for restrictions to roaming carrier options. Some embodiments provide policies based on carrier chosen. Some embodiments provide policies based on the service cost for carrier chosen. Some embodiments specify preferred roaming lists that may be different than the central provider roaming list.	Same as above.
Switch policies for new network	Provides the user or VSP with the capability to switch service usage notification or service usage control policies depending on which network the device is connected to. Some embodiments provide for restrictions to certain network options. Some embodiments provide policies based on network chosen. Some embodiments provide policies based on the service cost for network chosen. Some embodiments provide for a network connection preference list.	Authorization to modify the policies typically restricted to the VSP or other entity responsible for managing the network selection policies.

Figure 42F

Service Processor Authorization

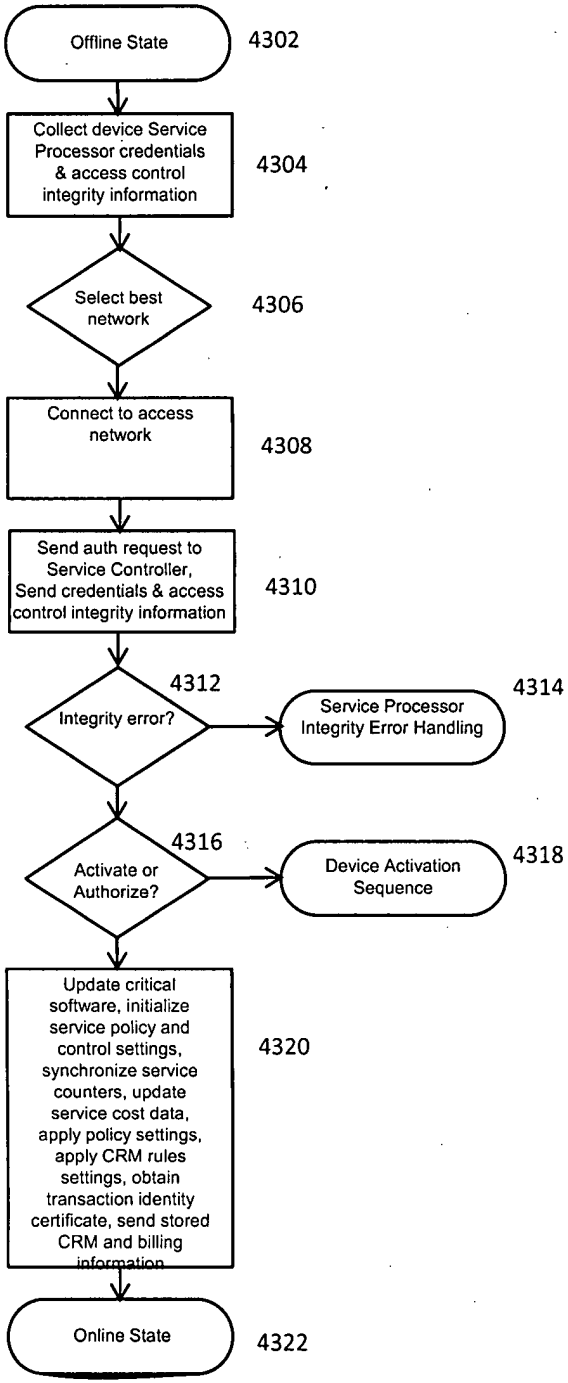


Figure 43A

Service Controller Authorization

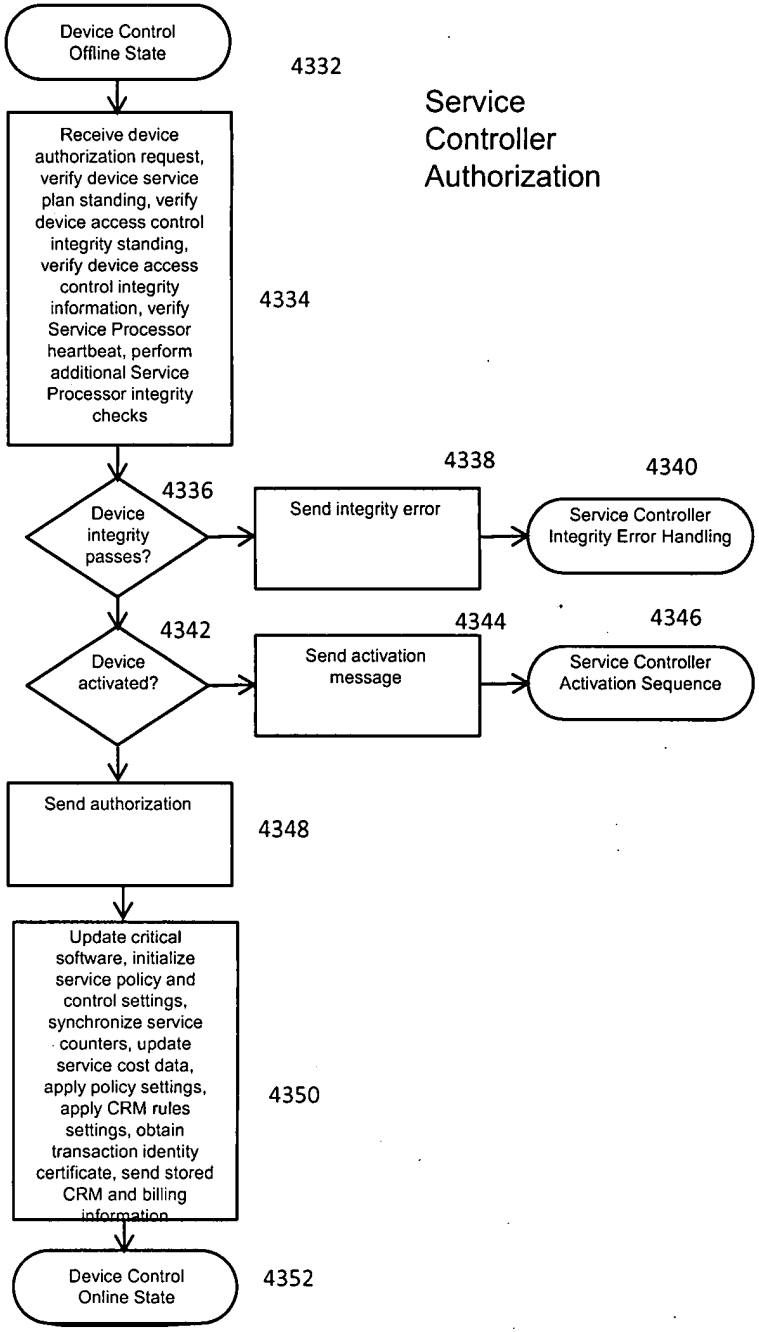


Figure 43B

Figure 43

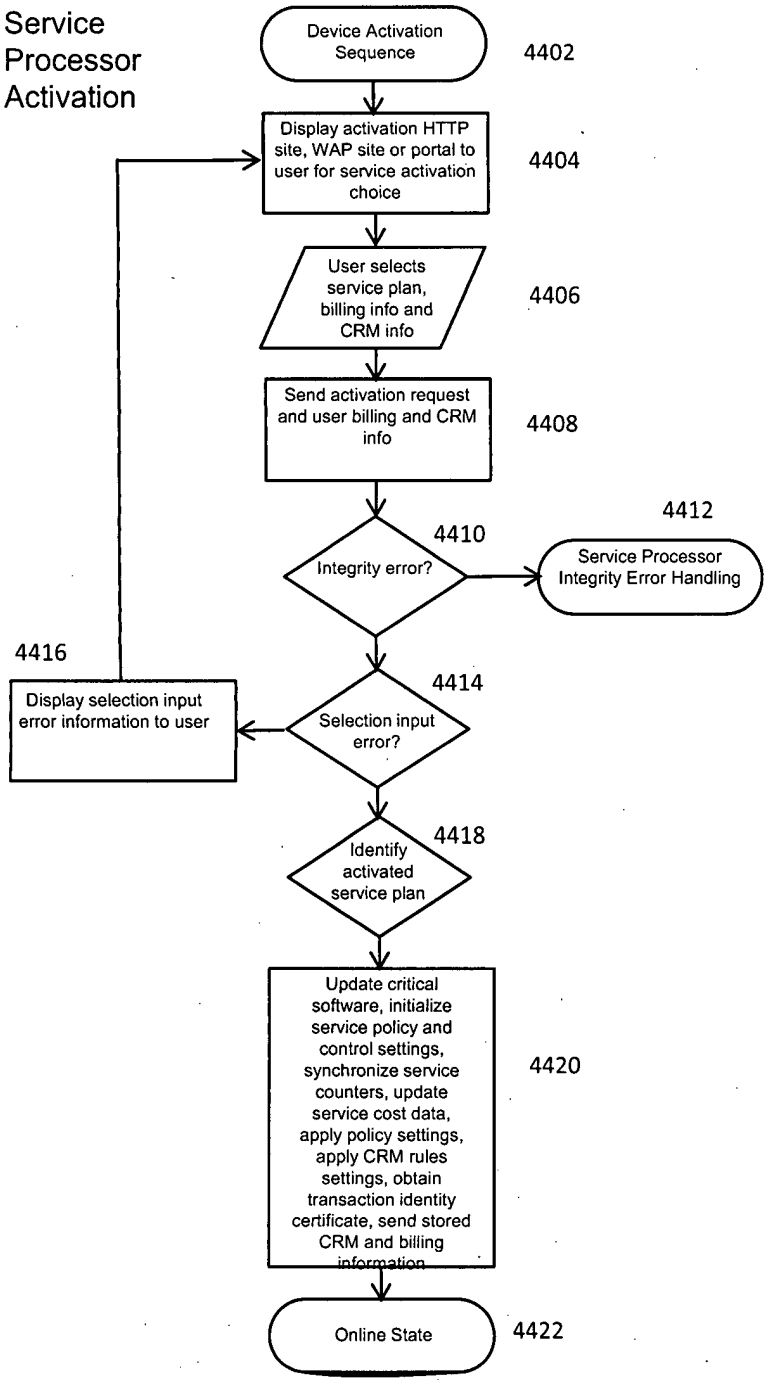


Figure 44A

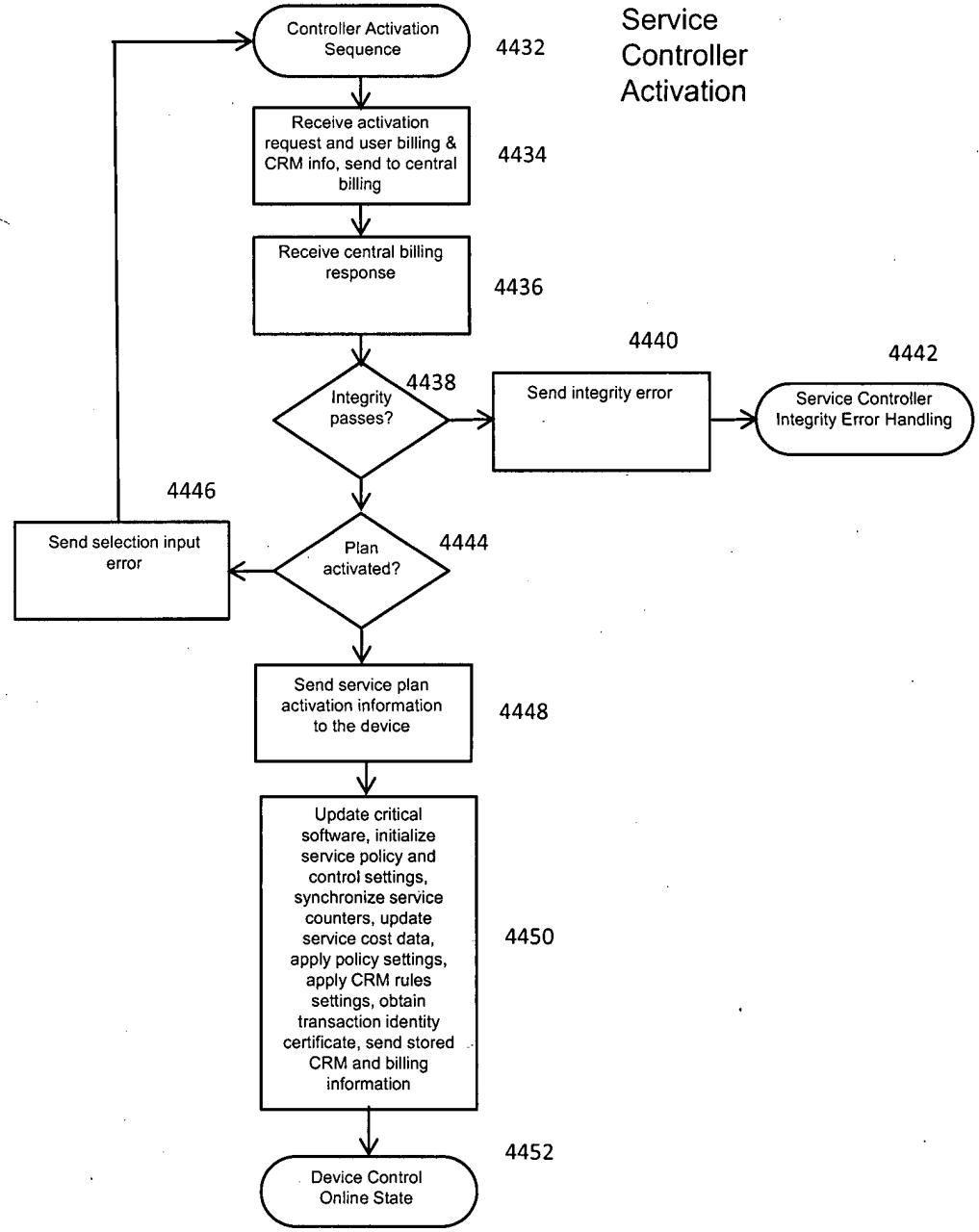


Figure 44B

Figure 44

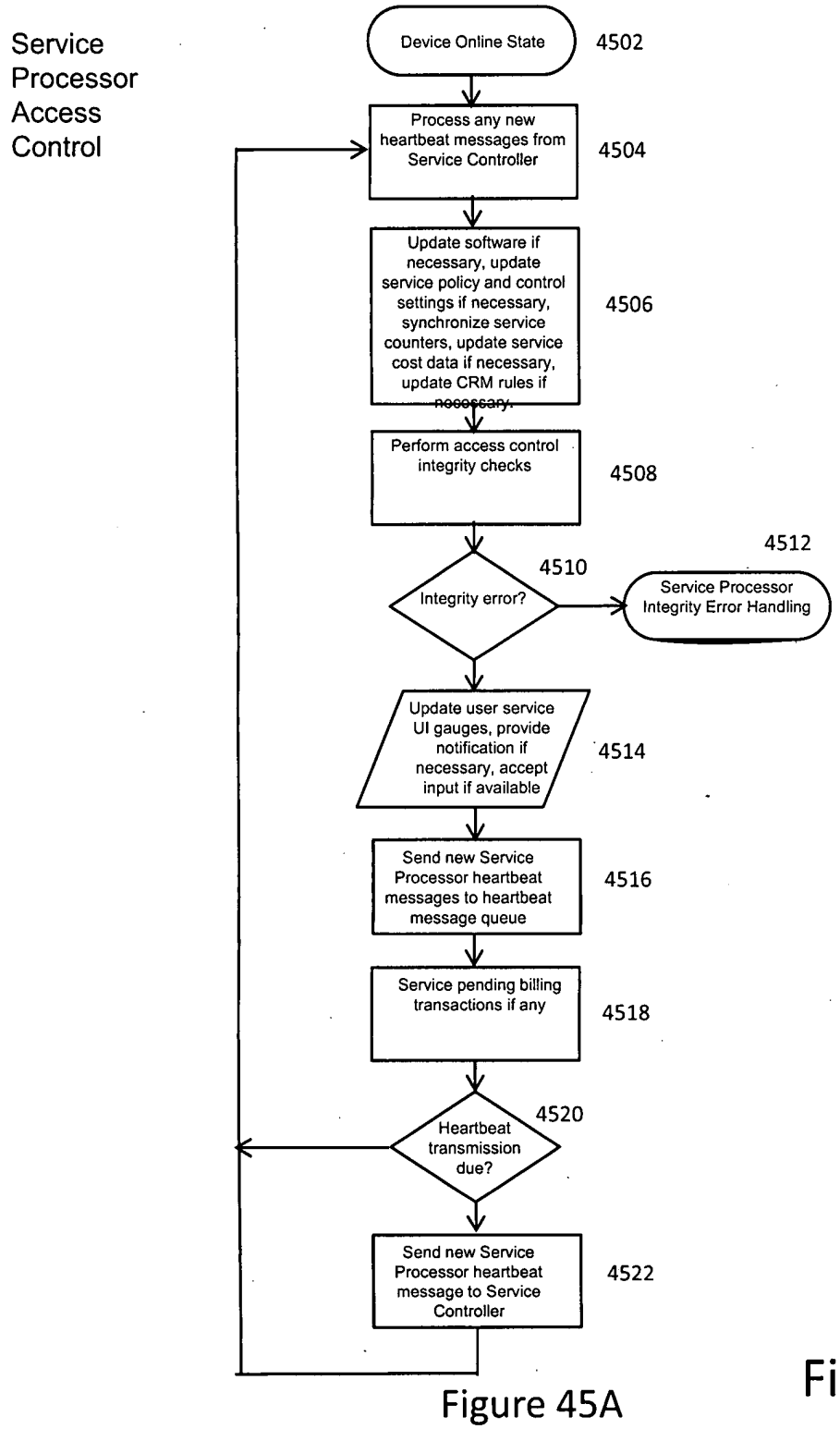


Figure 45A

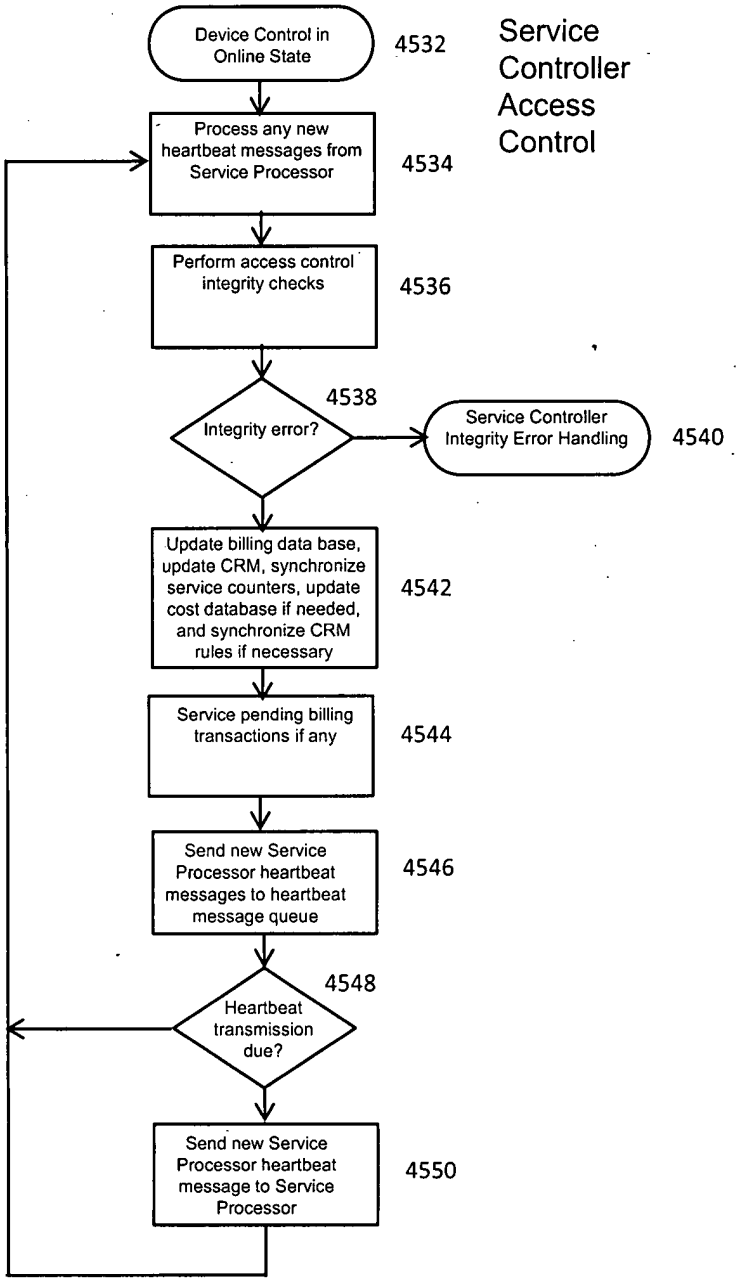


Figure 45B

Figure 45

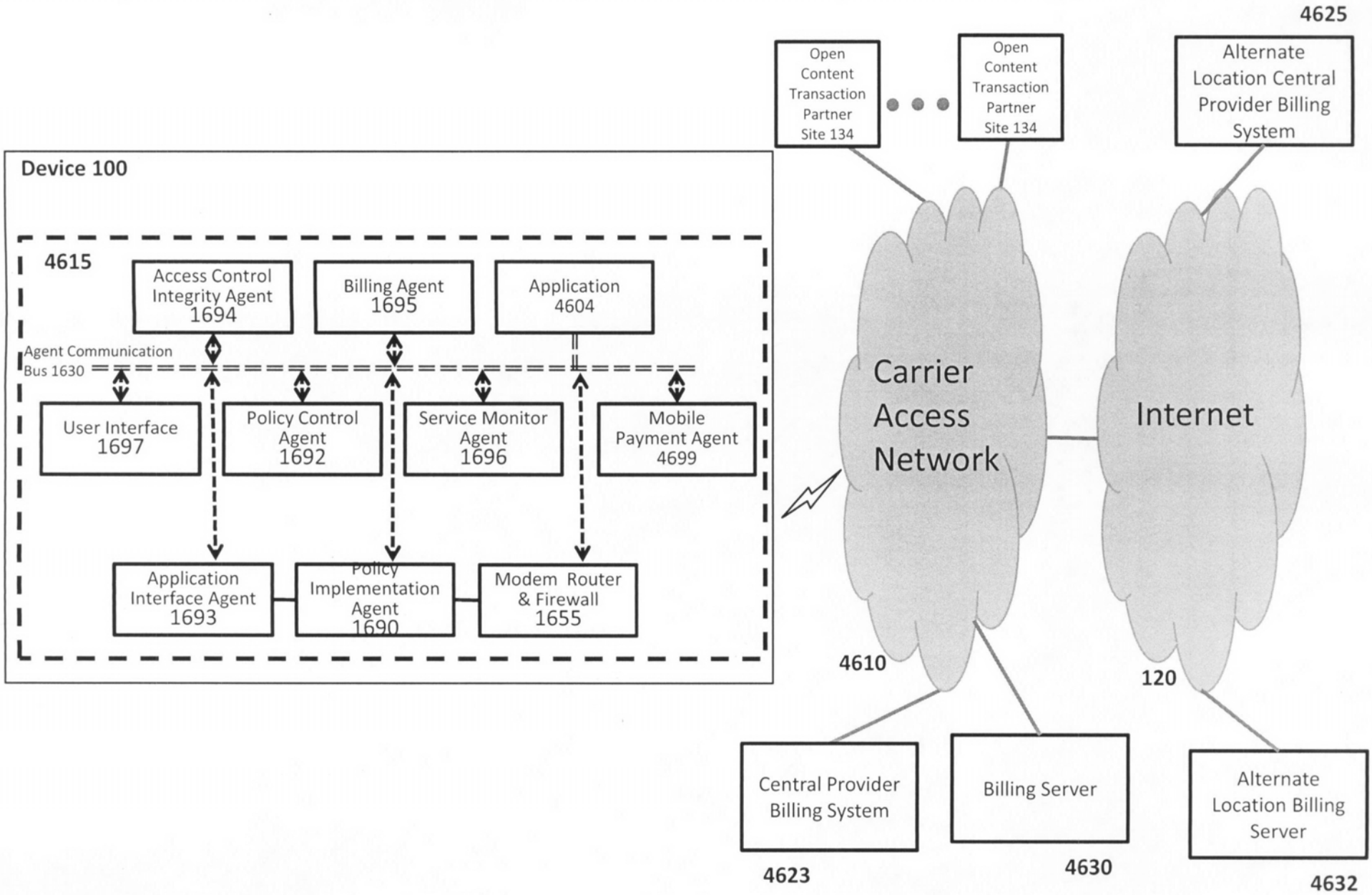

Device 100
4615
Access Control Integrity Agent 1694
Billing Agent 1695
Application 4604
Agent Communication Bus 1630
User Interface 1697
Policy Control Agent 1692
Service Monitor Agent 1696
Mobile Payment Agent 4699
Application Interface Agent 1693
Policy Implementation Agent 1690
Modem Router & Firewall 1655
Open Content Transaction Partner Site 134
Open Content Transaction Partner Site 134
4625
Alternate Location Central Provider Billing System
Carrier Access Network
Internet
4610
120
Central Provider Billing System
Billing Server
Alternate Location Billing Server
4623
4630
4632

Figure 46

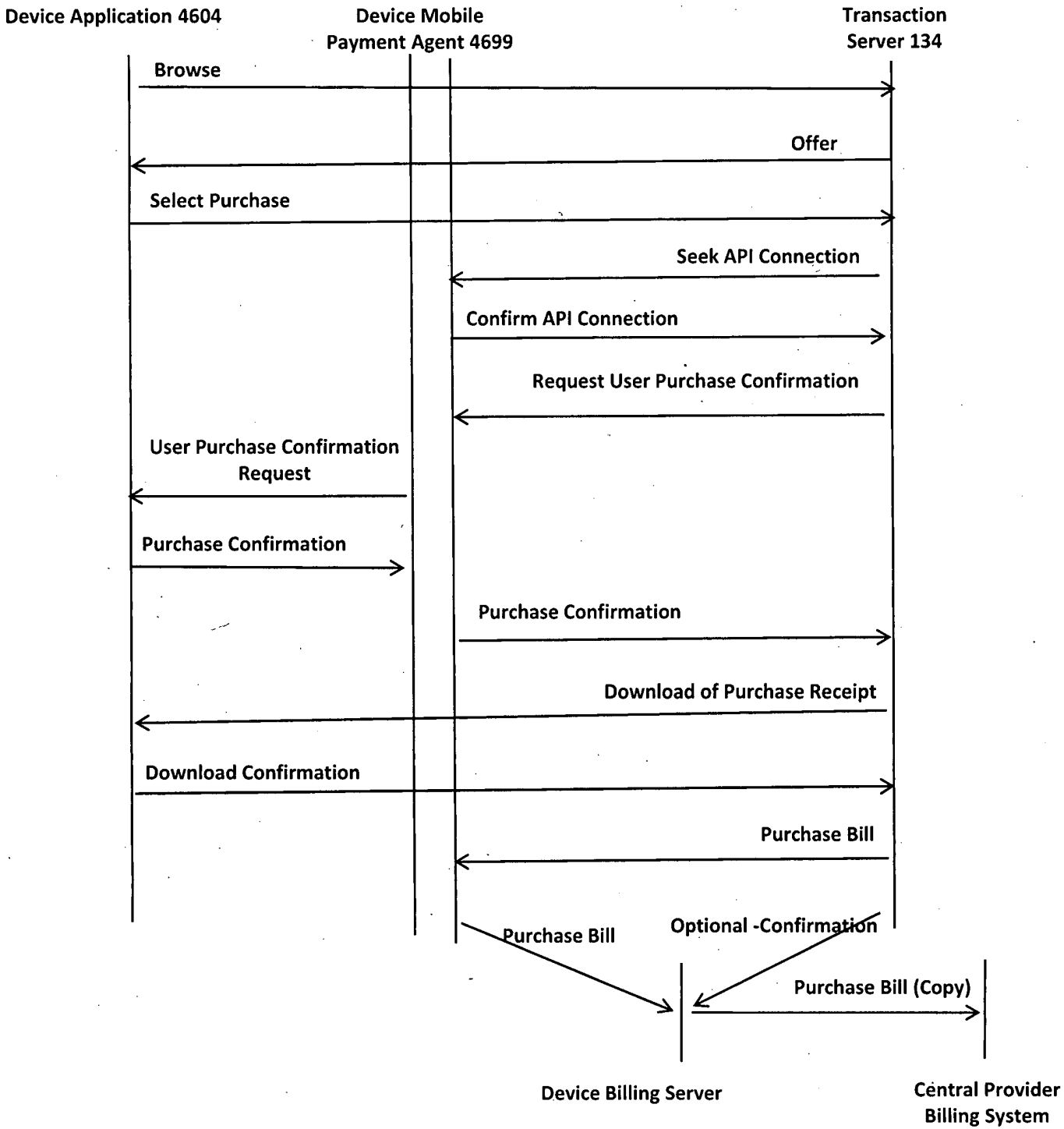

Device Application 4604
Device Mobile Payment Agent 4699
Transaction Server 134
Browse
Offer
Select Purchase
Seek API Connection
Confirm API Connection
Request User Purchase Confirmation
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
Download of Purchase Receipt
Download Confirmation
Purchase Bill
Purchase Bill
Optional -Confirmation
Purchase Bill (Copy)
Device Billing Server
Central Provider Billing System

Figure 47A

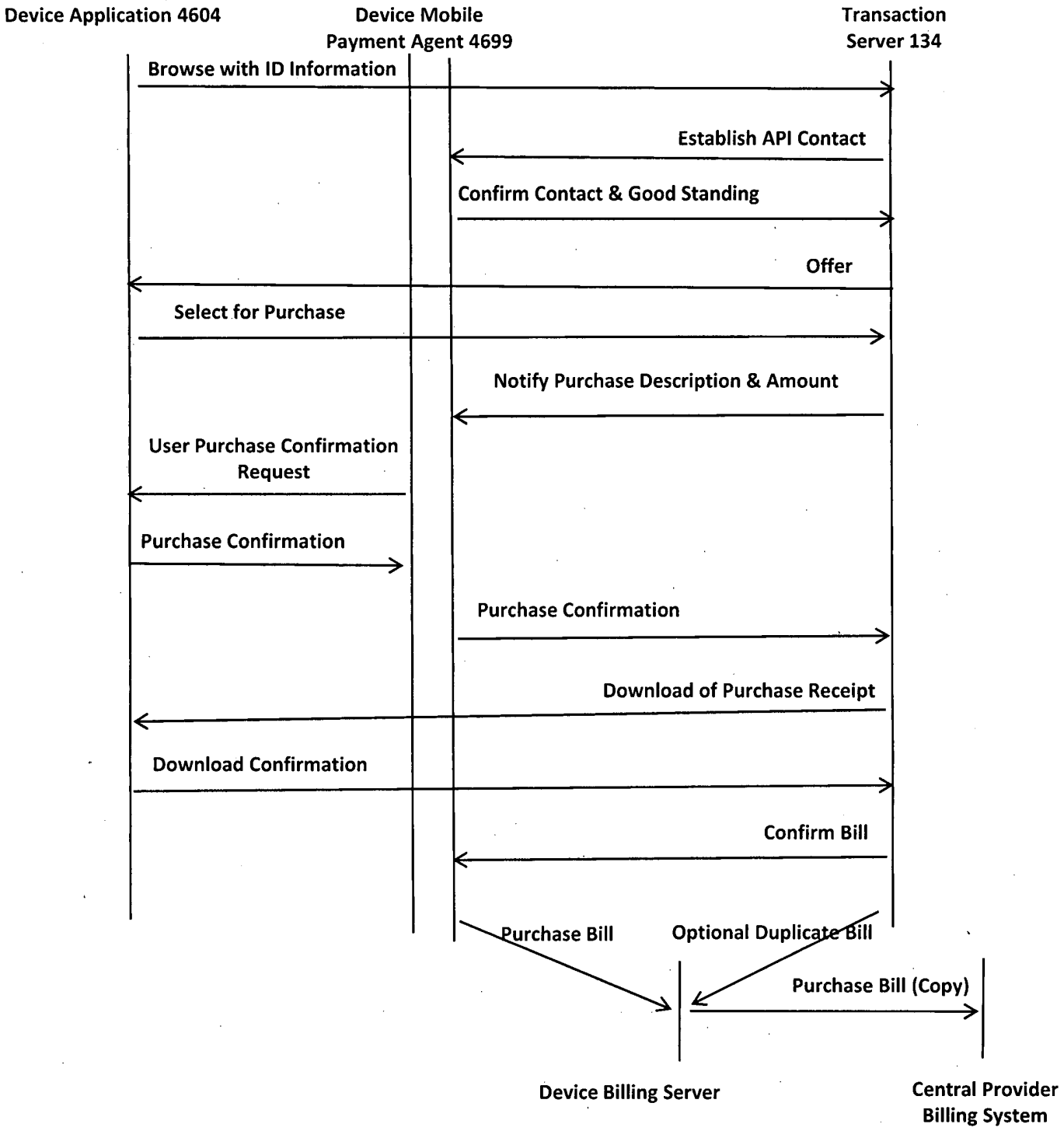

Device Application 4604
Device Mobile Payment Agent 4699
Transaction Server 134
Browse with ID Information
Establish API Contact
Confirm Contact & Good Standing
Offer
Select for Purchase
Notify Purchase Description & Amount
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
Download of Purchase Receipt
Download Confirmation
Confirm Bill
Purchase Bill
Optional Duplicate Bill
Purchase Bill (Copy)
Device Billing Server
Central Provider Billing System

Figure 47B

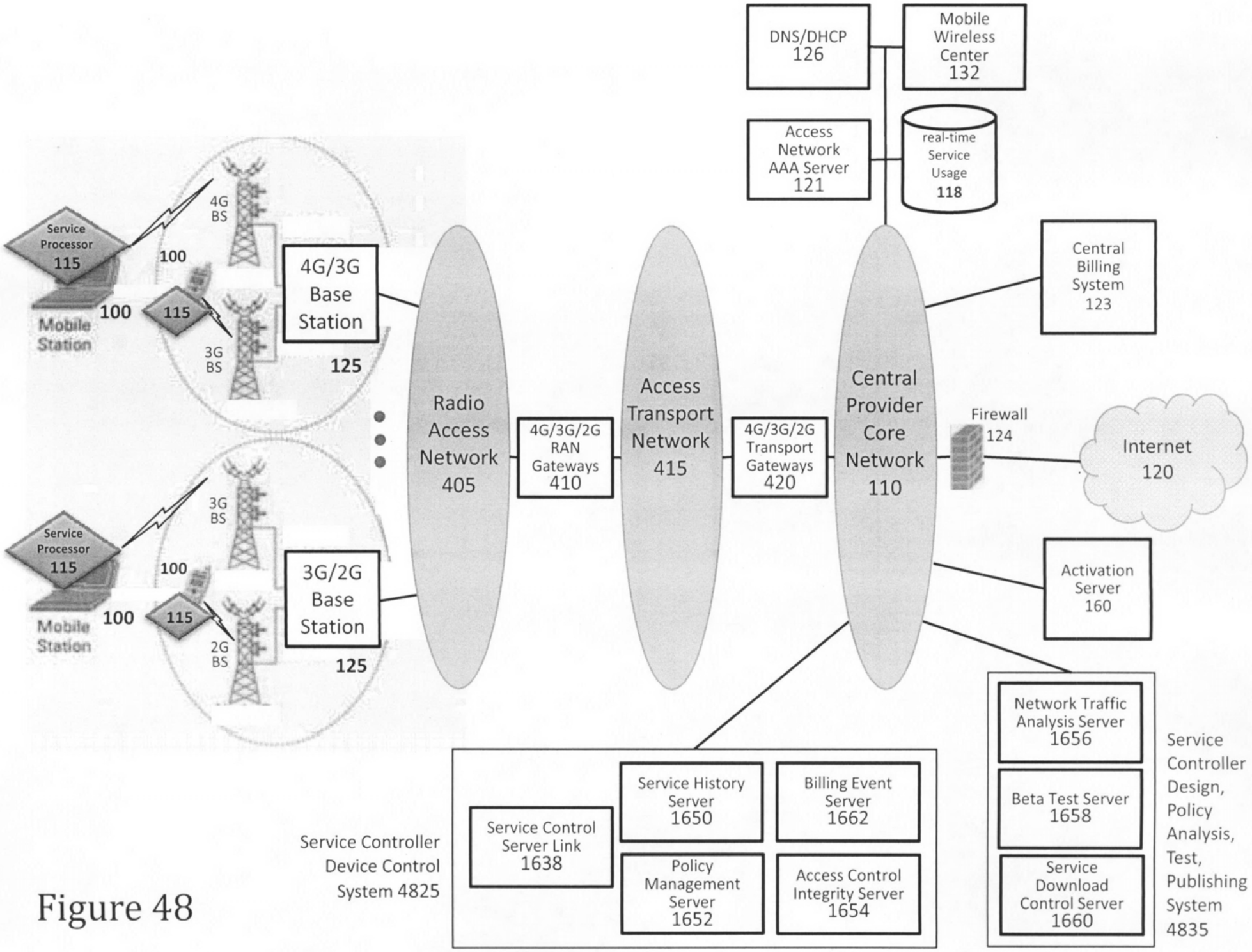

DNS/DHCP
126
Mobile
Wireless
Center
132
Access
Network
AAA Server
121
real-time
Service
Usage
118
Central
Billing
System
123
Service
Processor
115
100
4G
BS
Mobile
Station
100
115
3G
BS
4G/3G
Base
Station
125
Radio
Access
Network
405
4G/3G/2G
RAN
Gateways
410
Access
Transport
Network
415
4G/3G/2G
Transport
Gateways
420
Central
Provider
Core
Network
110
Firewall
124
Internet
120
Service
Processor
115
100
3G
BS
Mobile
Station
100
115
2G
BS
3G/2G
Base
Station
125
Activation
Server
160
Service Controller
Device Control
System 4825
Service Control
Server Link
1638
Service History
Server
1650
Billing Event
Server
1662
Policy
Management
Server
1652
Access Control
Integrity Server
1654
Network Traffic
Analysis Server
1656
Beta Test Server
1658
Service
Download
Control Server
1660
Service
Controller
Design,
Policy
Analysis,
Test,
Publishing
System
4835

Figure 48

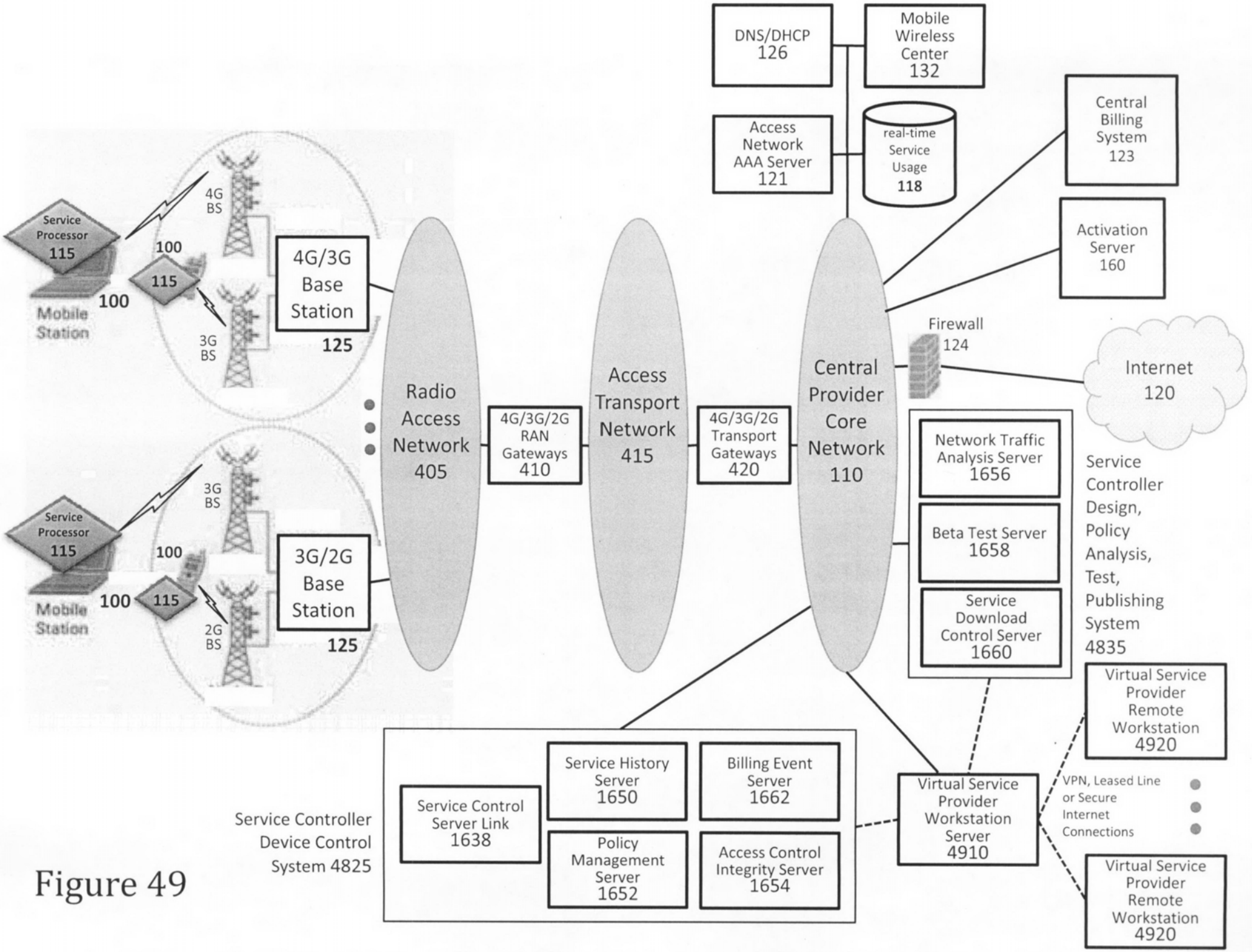

DNS/DHCP
126
Mobile
Wireless
Center
132
Access
Network
AAA Server
121
real-time
Service
Usage
118
Central
Billing
System
123
Activation
Server
160
Service
Processor
115
100
Mobile
Station
4G
BS
3G
BS
4G/3G
Base
Station
125
Radio
Access
Network
405
4G/3G/2G
RAN
Gateways
410
Access
Transport
Network
415
4G/3G/2G
Transport
Gateways
420
Central
Provider
Core
Network
110
Firewall
124
Internet
120
3G
BS
2G
BS
3G/2G
Base
Station
125
Network Traffic
Analysis Server
1656
Beta Test Server
1658
Service
Download
Control Server
1660
Service
Controller
Design,
Policy
Analysis,
Test,
Publishing
System
4835
Virtual Service
Provider
Remote
Workstation
4920
Service Control
Server Link
1638
Service History
Server
1650
Billing Event
Server
1662
Policy
Management
Server
1652
Access Control
Integrity Server
1654
Service Controller
Device Control
System 4825
Virtual Service
Provider
Workstation
Server
4910
VPN, Leased Line
or Secure
Internet
Connections

Figure 49

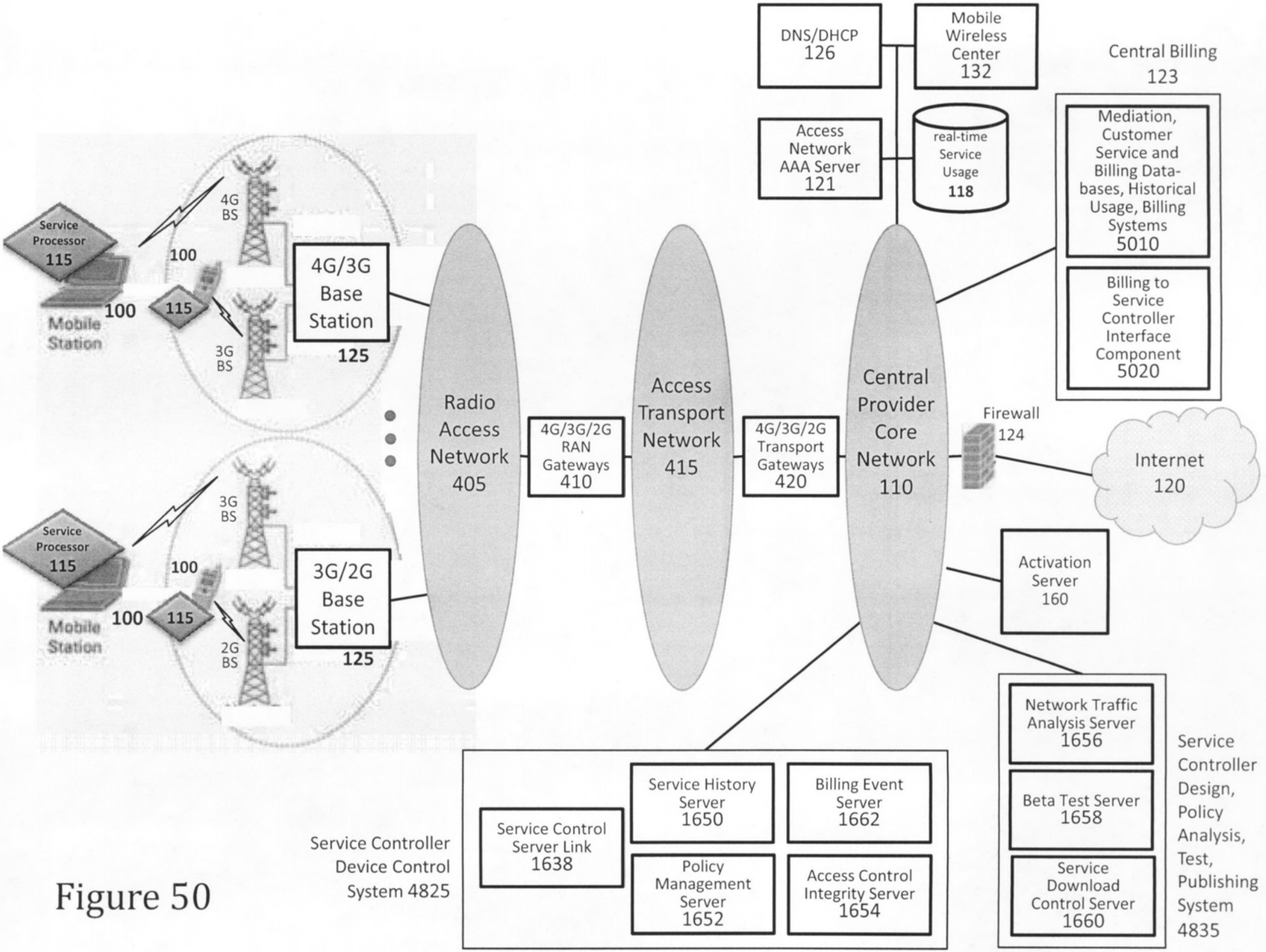

DNS/DHCP 126
Mobile Wireless Center 132
Central Billing 123
Access Network AAA Server 121
real-time Service Usage 118
Mediation, Customer Service and Billing Data-bases, Historical Usage, Billing Systems 5010
Billing to Service Controller Interface Component 5020
Service Processor 115
4G BS
100
Mobile Station
100
115
4G/3G Base Station 125
3G BS
Radio Access Network 405
4G/3G/2G RAN Gateways 410
Access Transport Network 415
4G/3G/2G Transport Gateways 420
Central Provider Core Network 110
Firewall 124
Internet 120
Service Processor 115
3G BS
100
Mobile Station
100
115
3G/2G Base Station 125
2G BS
Activation Server 160
Service Controller Device Control System 4825
Service Control Server Link 1638
Service History Server 1650
Billing Event Server 1662
Policy Management Server 1652
Access Control Integrity Server 1654
Network Traffic Analysis Server 1656
Beta Test Server 1658
Service Download Control Server 1660
Service Controller Design, Policy Analysis, Test, Publishing System 4835

Figure 50

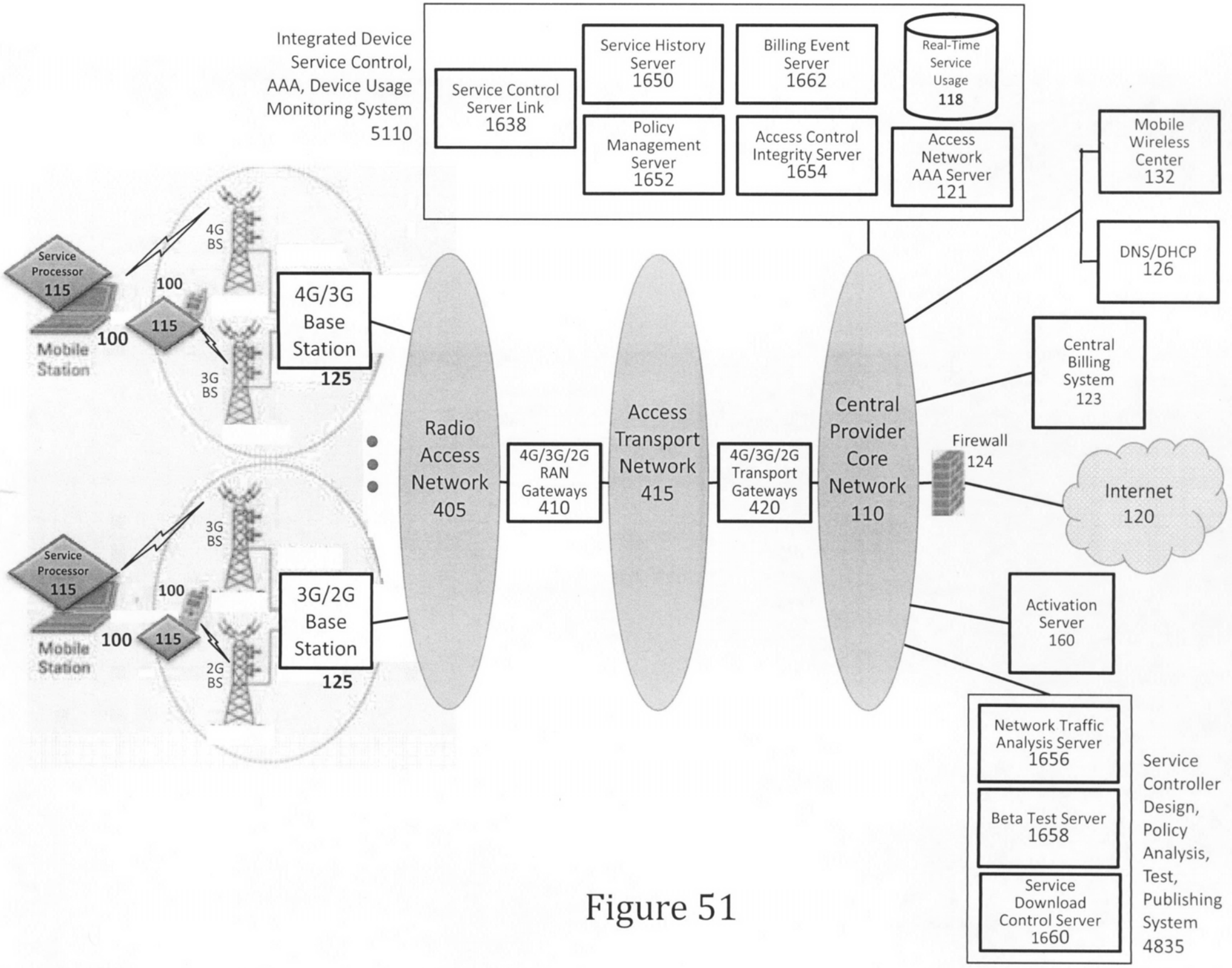

Integrated Device Service Control, AAA, Device Usage Monitoring System 5110
Service Control Server Link 1638
Service History Server 1650
Billing Event Server 1662
Real-Time Service Usage 118
Policy Management Server 1652
Access Control Integrity Server 1654
Access Network AAA Server 121
Mobile Wireless Center 132
DNS/DHCP 126
Central Billing System 123
Service Processor 115
Mobile Station
100
115
4G BS
3G BS
4G/3G Base Station 125
3G/2G Base Station 125
2G BS
Radio Access Network 405
4G/3G/2G RAN Gateways 410
Access Transport Network 415
4G/3G/2G Transport Gateways 420
Central Provider Core Network 110
Firewall 124
Internet 120
Activation Server 160
Network Traffic Analysis Server 1656
Beta Test Server 1658
Service Download Control Server 1660
Service Controller Design, Policy Analysis, Test, Publishing System 4835

Figure 51

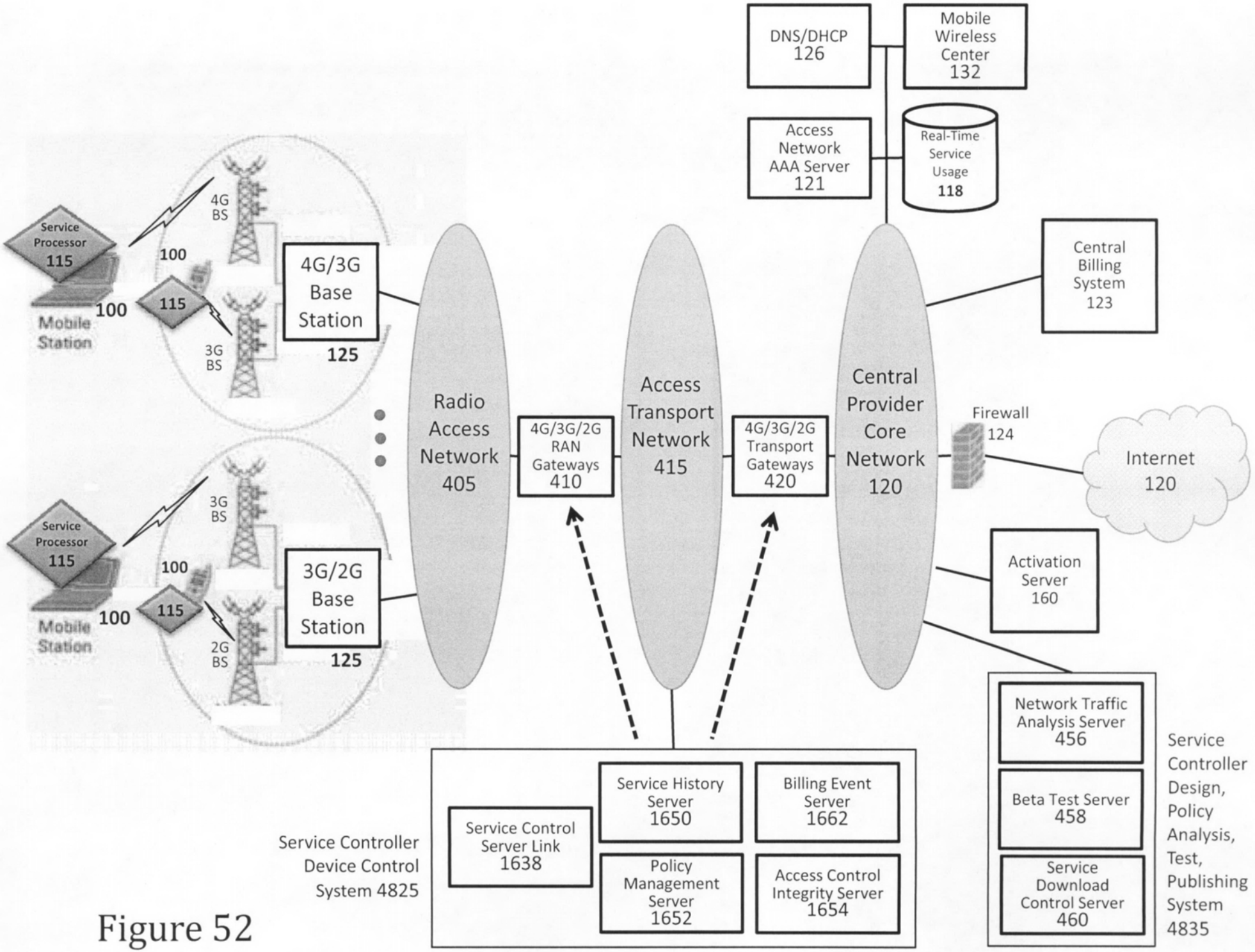

DNS/DHCP
126
Mobile
Wireless
Center
132
Access
Network
AAA Server
121
Real-Time
Service
Usage
118
Central
Billing
System
123
Service
Processor
115
100
Mobile
Station
100
115
4G
BS
3G
BS
4G/3G
Base
Station
125
Radio
Access
Network
405
4G/3G/2G
RAN
Gateways
410
Access
Transport
Network
415
4G/3G/2G
Transport
Gateways
420
Central
Provider
Core
Network
120
Firewall
124
Internet
120
Service
Processor
115
100
Mobile
Station
100
115
3G
BS
2G
BS
3G/2G
Base
Station
125
Activation
Server
160
Network Traffic
Analysis Server
456
Beta Test Server
458
Service
Download
Control Server
460
Service Controller
Design,
Policy
Analysis,
Test,
Publishing
System
4835
Service Controller
Device Control
System 4825
Service Control
Server Link
1638
Service History
Server
1650
Billing Event
Server
1662
Policy
Management
Server
1652
Access Control
Integrity Server
1654

Figure 52

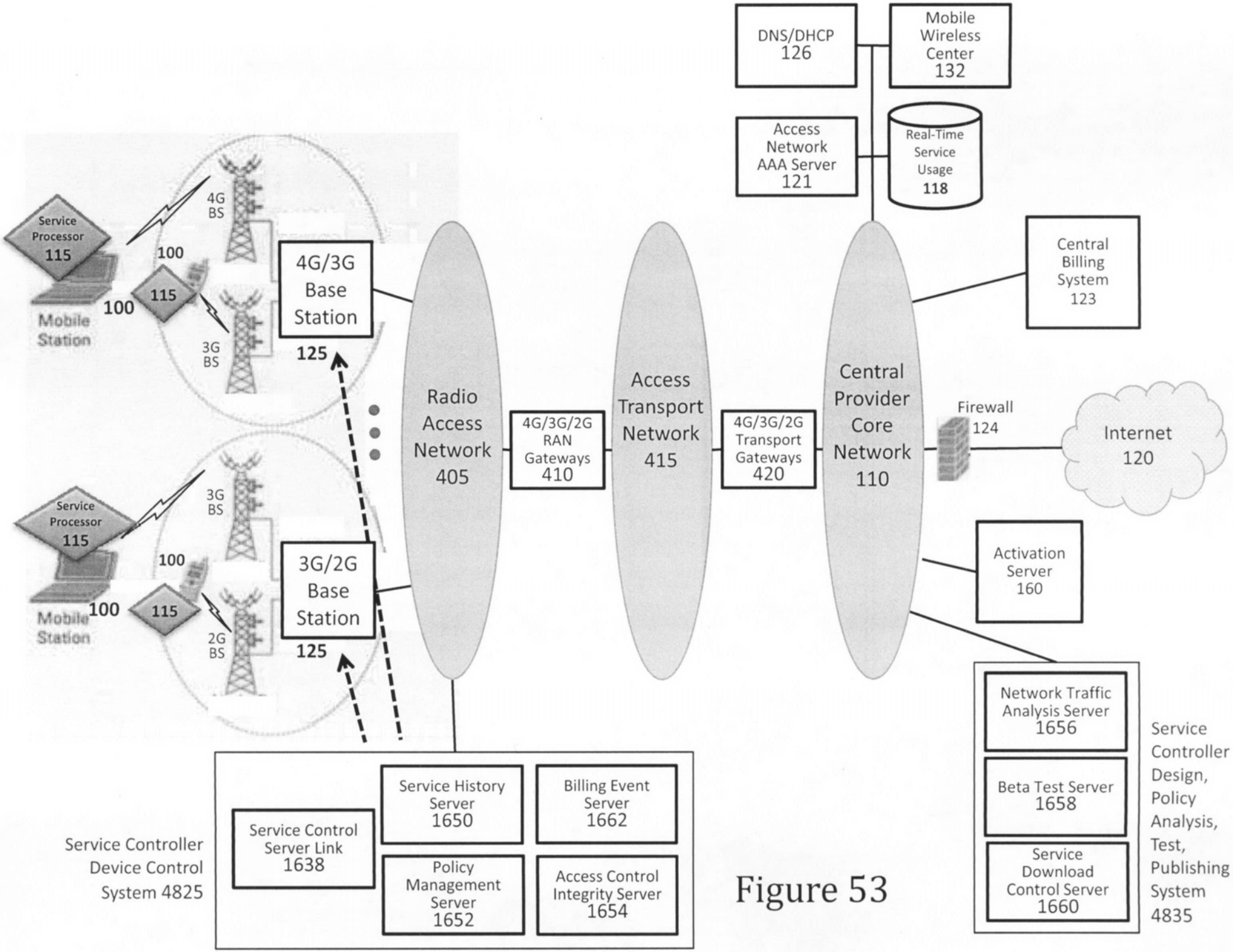

DNS/DHCP
126
Mobile
Wireless
Center
132
Access
Network
AAA Server
121
Real-Time
Service
Usage
118
Central
Billing
System
123
Service
Processor
115
100
115
100
Mobile
Station
4G
BS
3G
BS
4G/3G
Base
Station
125
Radio
Access
Network
405
4G/3G/2G
RAN
Gateways
410
Access
Transport
Network
415
4G/3G/2G
Transport
Gateways
420
Central
Provider
Core
Network
110
Firewall
124
Internet
120
Service
Processor
115
100
115
100
Mobile
Station
3G
BS
2G
BS
3G/2G
Base
Station
125
Activation
Server
160
Service Controller
Device Control
System 4825
Service Control
Server Link
1638
Service History
Server
1650
Billing Event
Server
1662
Policy
Management
Server
1652
Access Control
Integrity Server
1654
Network Traffic
Analysis Server
1656
Beta Test Server
1658
Service
Download
Control Server
1660
Service
Controller
Design,
Policy
Analysis,
Test,
Publishing
System
4835

Figure 53

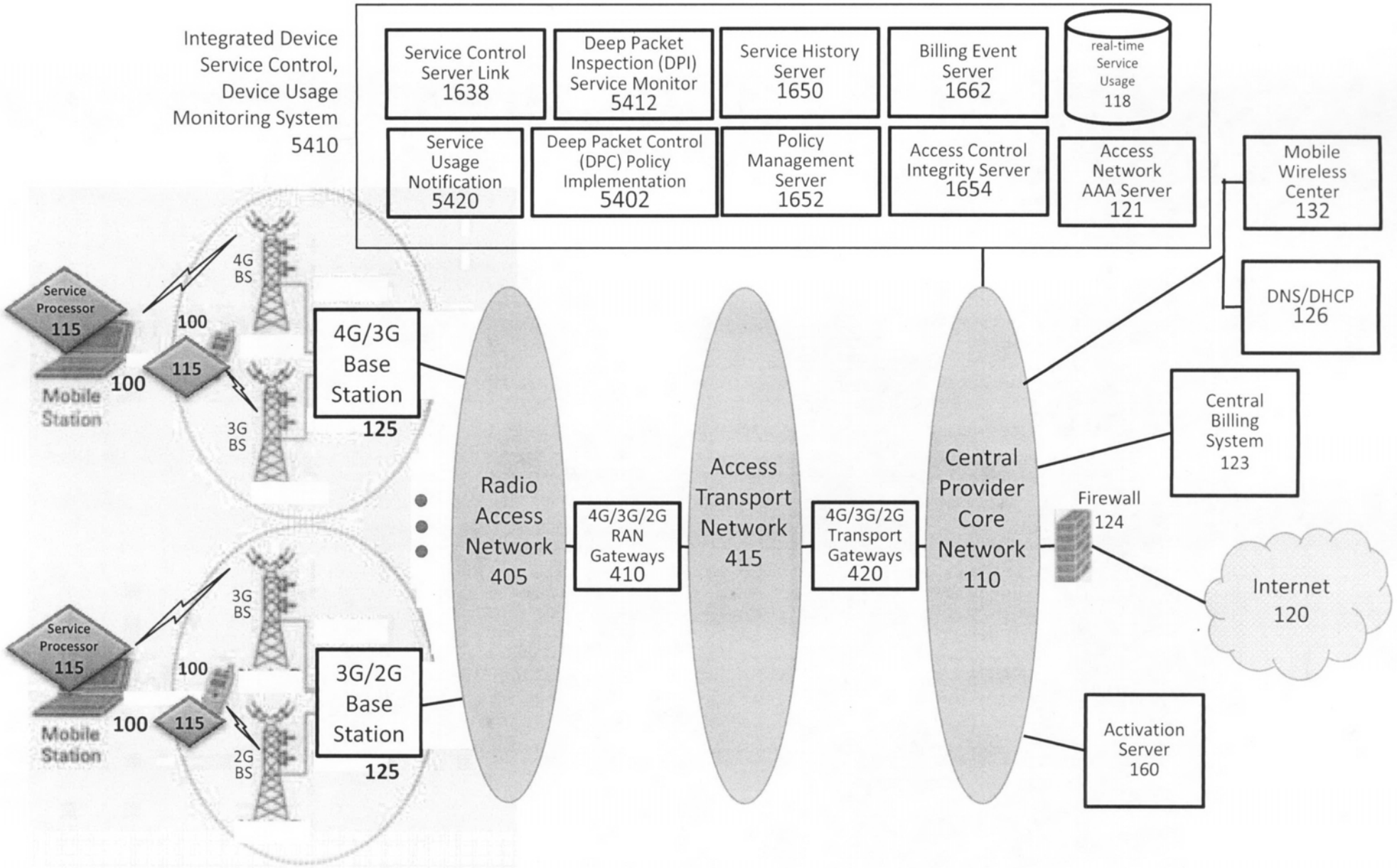

Integrated Device Service Control, Device Usage Monitoring System 5410
Service Control Server Link 1638
Deep Packet Inspection (DPI) Service Monitor 5412
Service History Server 1650
Billing Event Server 1662
real-time Service Usage 118
Service Usage Notification 5420
Deep Packet Control (DPC) Policy Implementation 5402
Policy Management Server 1652
Access Control Integrity Server 1654
Access Network AAA Server 121
Mobile Wireless Center 132
DNS/DHCP 126
Central Billing System 123
Service Processor 115
Mobile Station
100
115
4G BS
3G BS
4G/3G Base Station 125
3G/2G Base Station 125
2G BS
Radio Access Network 405
4G/3G/2G RAN Gateways 410
Access Transport Network 415
4G/3G/2G Transport Gateways 420
Central Provider Core Network 110
Firewall 124
Internet 120
Activation Server 160

Figure 54

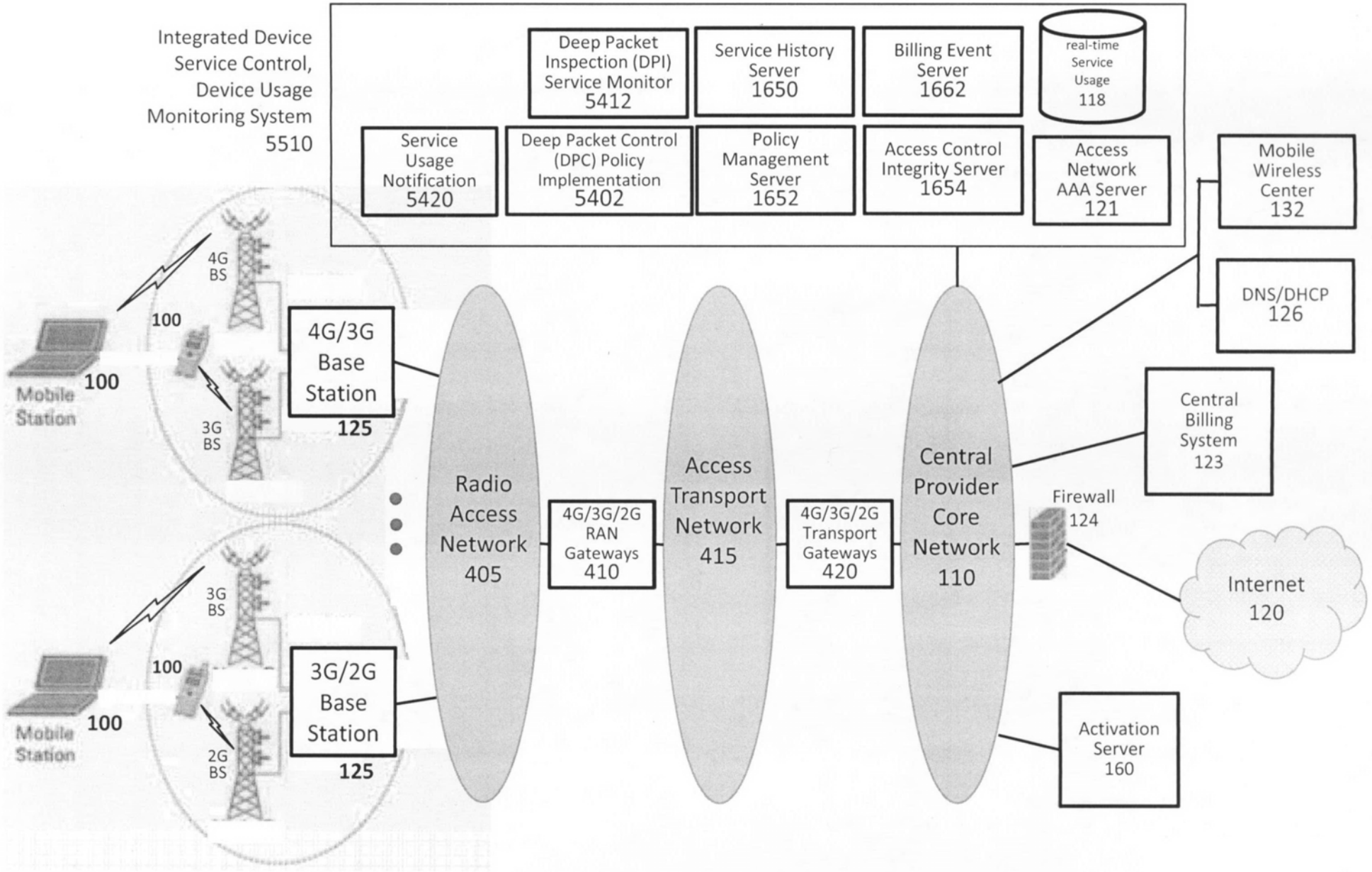

Integrated Device Service Control, Device Usage Monitoring System 5510
Deep Packet Inspection (DPI) Service Monitor 5412
Service History Server 1650
Billing Event Server 1662
real-time Service Usage 118
Service Usage Notification 5420
Deep Packet Control (DPC) Policy Implementation 5402
Policy Management Server 1652
Access Control Integrity Server 1654
Access Network AAA Server 121
Mobile Wireless Center 132
DNS/DHCP 126
Central Billing System 123
Mobile Station 100
4G BS
3G BS
4G/3G Base Station 125
3G/2G Base Station 125
2G BS
Radio Access Network 405
4G/3G/2G RAN Gateways 410
Access Transport Network 415
4G/3G/2G Transport Gateways 420
Central Provider Core Network 110
Firewall 124
Internet 120
Activation Server 160

Figure 55

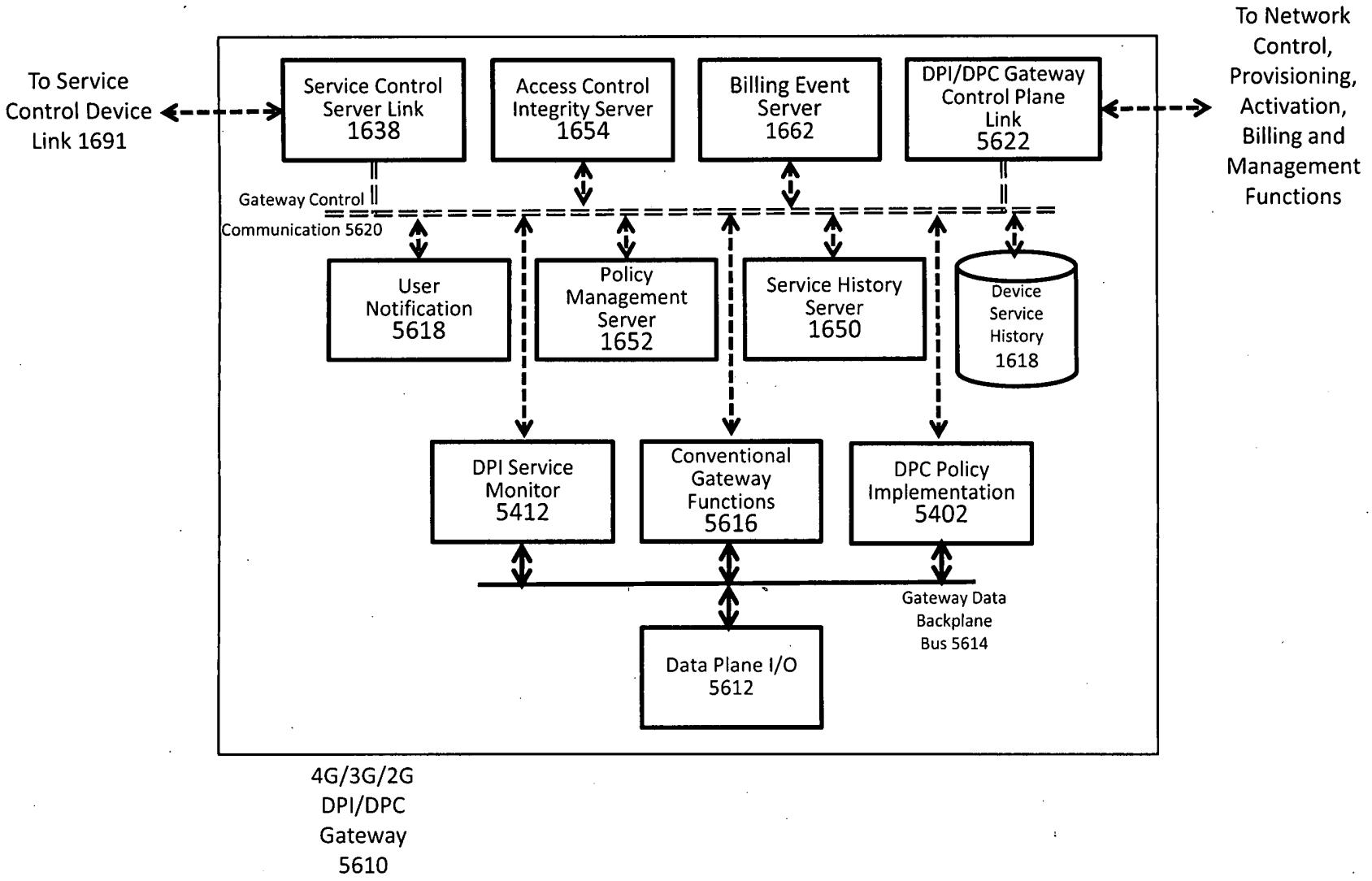

To Service Control Device Link 1691
Service Control Server Link 1638
Access Control Integrity Server 1654
Billing Event Server 1662
DPI/DPC Gateway Control Plane Link 5622
To Network Control, Provisioning, Activation, Billing and Management Functions
Gateway Control Communication 5620
User Notification 5618
Policy Management Server 1652
Service History Server 1650
Device Service History 1618
DPI Service Monitor 5412
Conventional Gateway Functions 5616
DPC Policy Implementation 5402
Gateway Data Backplane Bus 5614
Data Plane I/O 5612
4G/3G/2G DPI/DPC Gateway 5610

Figure 56

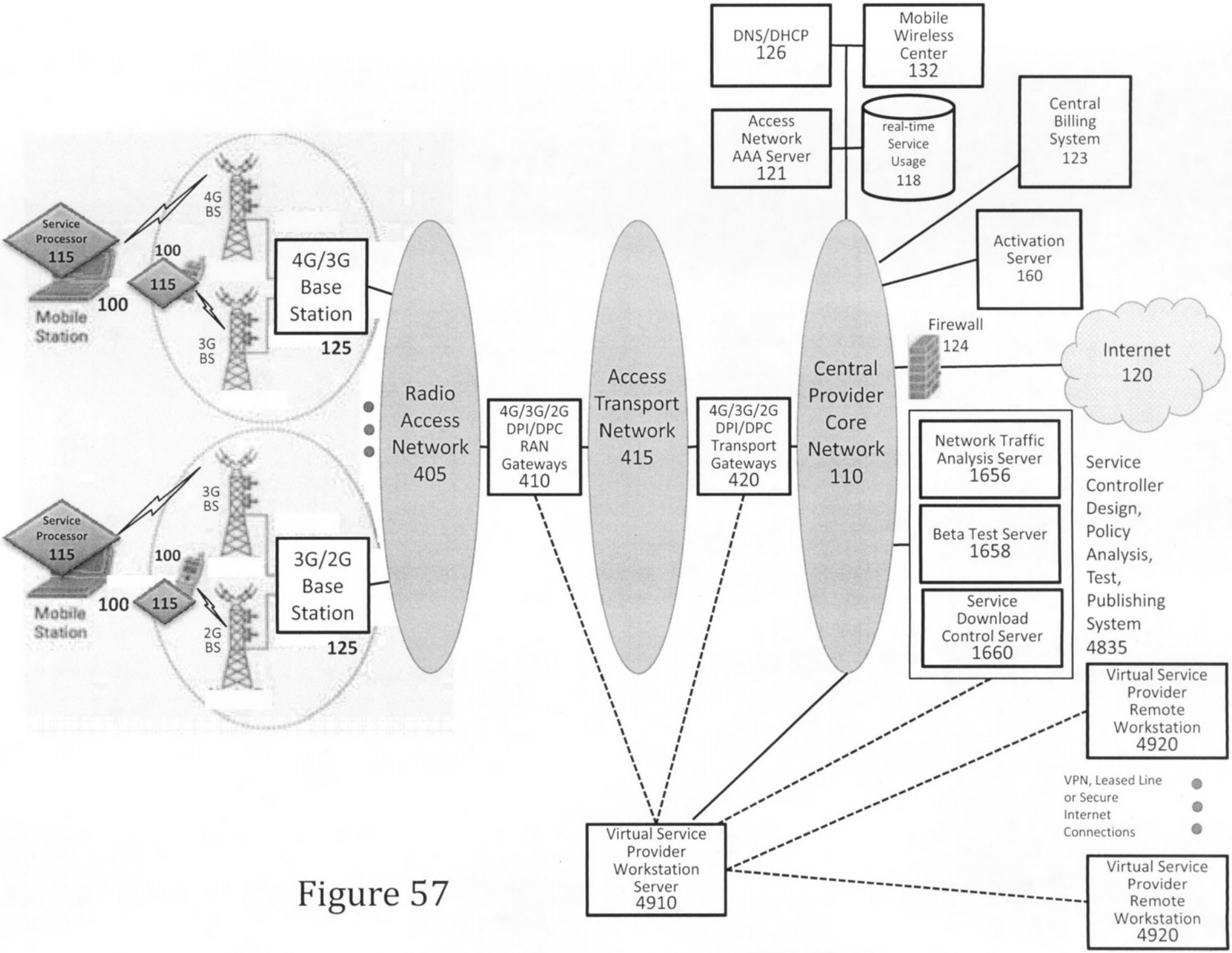

DNS/DHCP
126
Mobile
Wireless
Center
132
Access
Network
AAA Server
121
real-time
Service
Usage
118
Central
Billing
System
123
Activation
Server
160
Firewall
124
Internet
120
Service
Processor
115
100
115
100
Mobile
Station
4G
BS
3G
BS
4G/3G
Base
Station
125
Radio
Access
Network
405
4G/3G/2G
DPI/DPC
RAN
Gateways
410
Access
Transport
Network
415
4G/3G/2G
DPI/DPC
Transport
Gateways
420
Central
Provider
Core
Network
110
Network Traffic
Analysis Server
1656
Beta Test Server
1658
Service
Download
Control Server
1660
Service
Controller
Design,
Policy
Analysis,
Test,
Publishing
System
4835
Service
Processor
115
100
115
100
Mobile
Station
3G
BS
2G
BS
3G/2G
Base
Station
125
Virtual Service
Provider
Remote
Workstation
4920
VPN, Leased Line
or Secure
Internet
Connections
Virtual Service
Provider
Workstation
Server
4910
Virtual Service
Provider
Remote
Workstation
4920

Figure 57

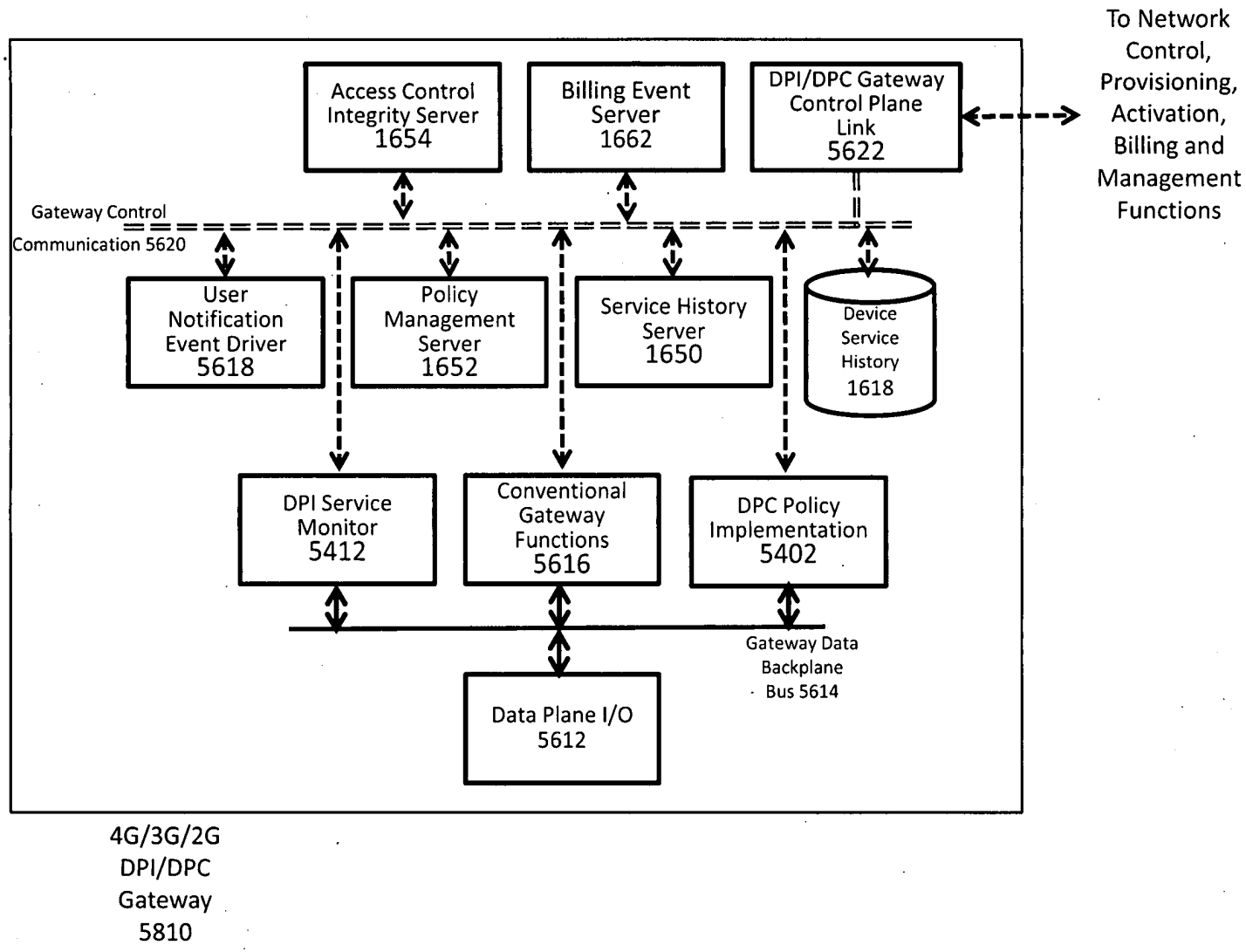

Access Control Integrity Server 1654
Billing Event Server 1662
DPI/DPC Gateway Control Plane Link 5622
To Network Control, Provisioning, Activation, Billing and Management Functions
Gateway Control Communication 5620
User Notification Event Driver 5618
Policy Management Server 1652
Service History Server 1650
Device Service History 1618
DPI Service Monitor 5412
Conventional Gateway Functions 5616
DPC Policy Implementation 5402
Gateway Data Backplane Bus 5614
Data Plane I/O 5612
4G/3G/2G DPI/DPC Gateway 5810

Figure 58

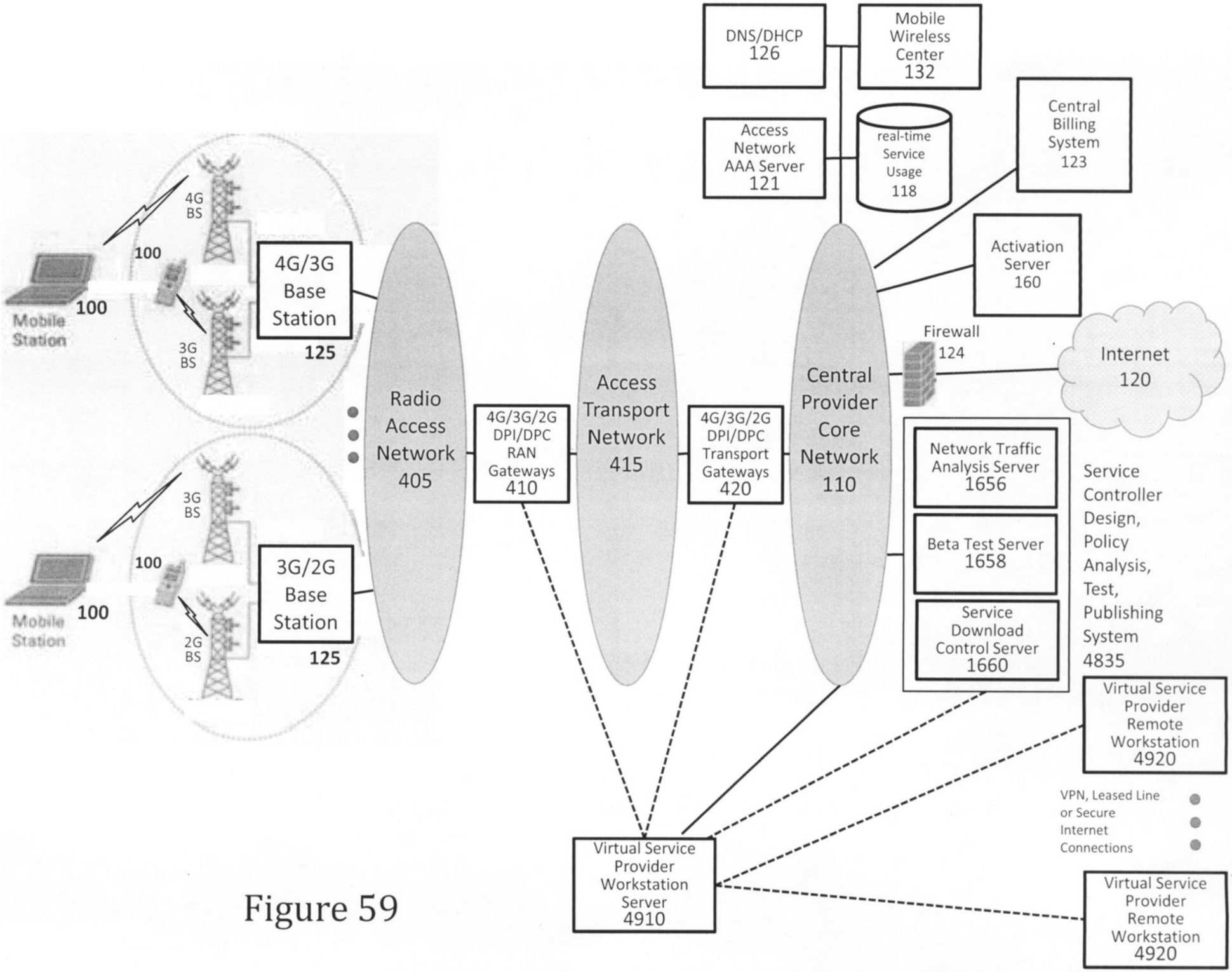

DNS/DHCP
126
Mobile
Wireless
Center
132
Access
Network
AAA Server
121
real-time
Service
Usage
118
Central
Billing
System
123
Activation
Server
160
Firewall
124
Internet
120
4G
BS
100
Mobile
Station
100
3G
BS
4G/3G
Base
Station
125
Radio
Access
Network
405
4G/3G/2G
DPI/DPC
RAN
Gateways
410
Access
Transport
Network
415
4G/3G/2G
DPI/DPC
Transport
Gateways
420
Central
Provider
Core
Network
110
Network Traffic
Analysis Server
1656
Beta Test Server
1658
Service
Download
Control Server
1660
Service
Controller
Design,
Policy
Analysis,
Test,
Publishing
System
4835
3G
BS
100
Mobile
Station
100
2G
BS
3G/2G
Base
Station
125
Virtual Service
Provider
Remote
Workstation
4920
VPN, Leased Line
or Secure
Internet
Connections
Virtual Service
Provider
Workstation
Server
4910
Virtual Service
Provider
Remote
Workstation
4920

Figure 59

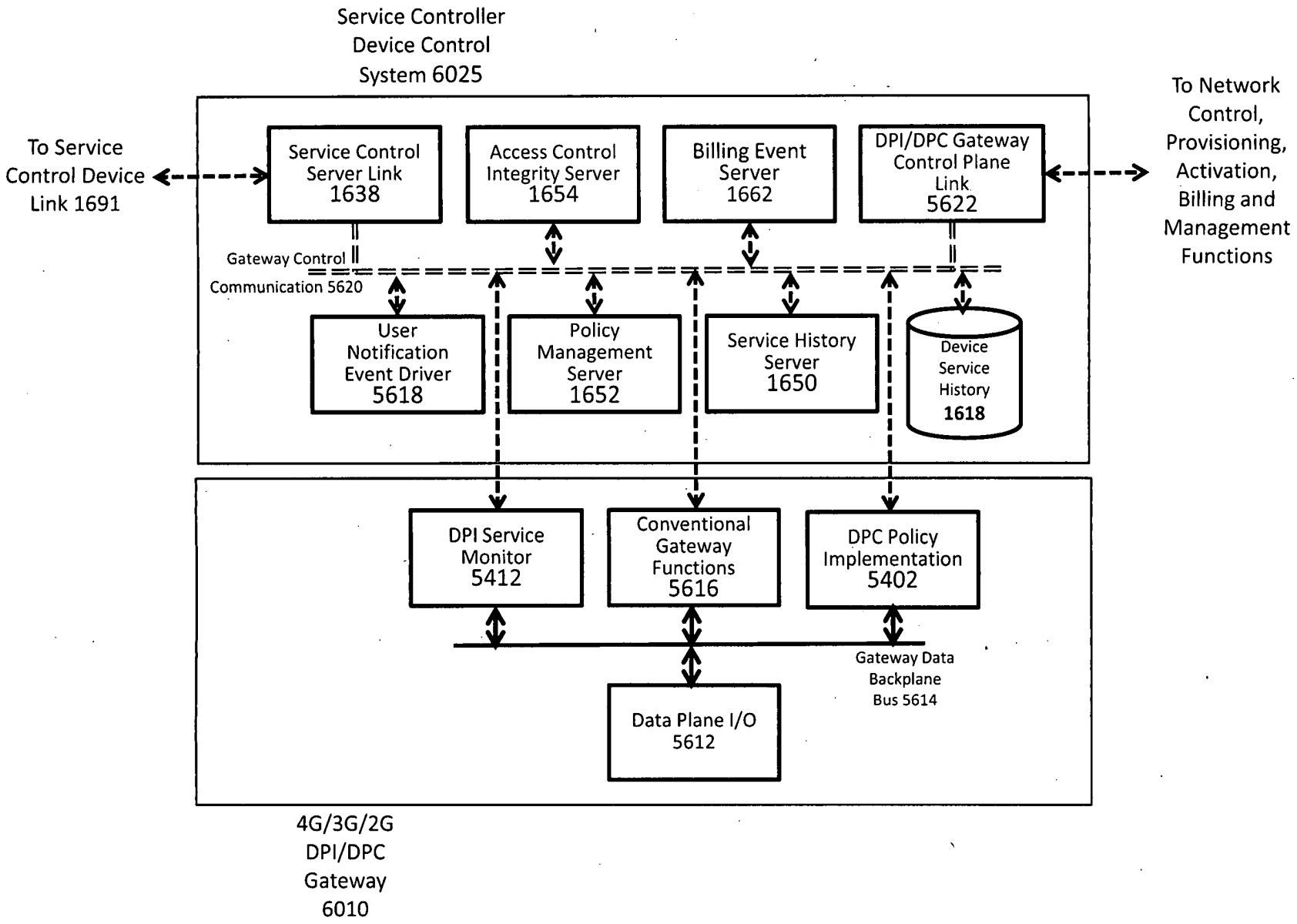

Service Controller
Device Control
System 6025
To Service
Control Device
Link 1691
Service Control
Server Link
1638
Access Control
Integrity Server
1654
Billing Event
Server
1662
DPI/DPC Gateway
Control Plane
Link
5622
To Network
Control,
Provisioning,
Activation,
Billing and
Management
Functions
Gateway Control
Communication 5620
User
Notification
Event Driver
5618
Policy
Management
Server
1652
Service History
Server
1650
Device
Service
History
1618
DPI Service
Monitor
5412
Conventional
Gateway
Functions
5616
DPC Policy
Implementation
5402
Gateway Data
Backplane
Bus 5614
Data Plane I/O
5612
4G/3G/2G
DPI/DPC
Gateway
6010

Figure 60

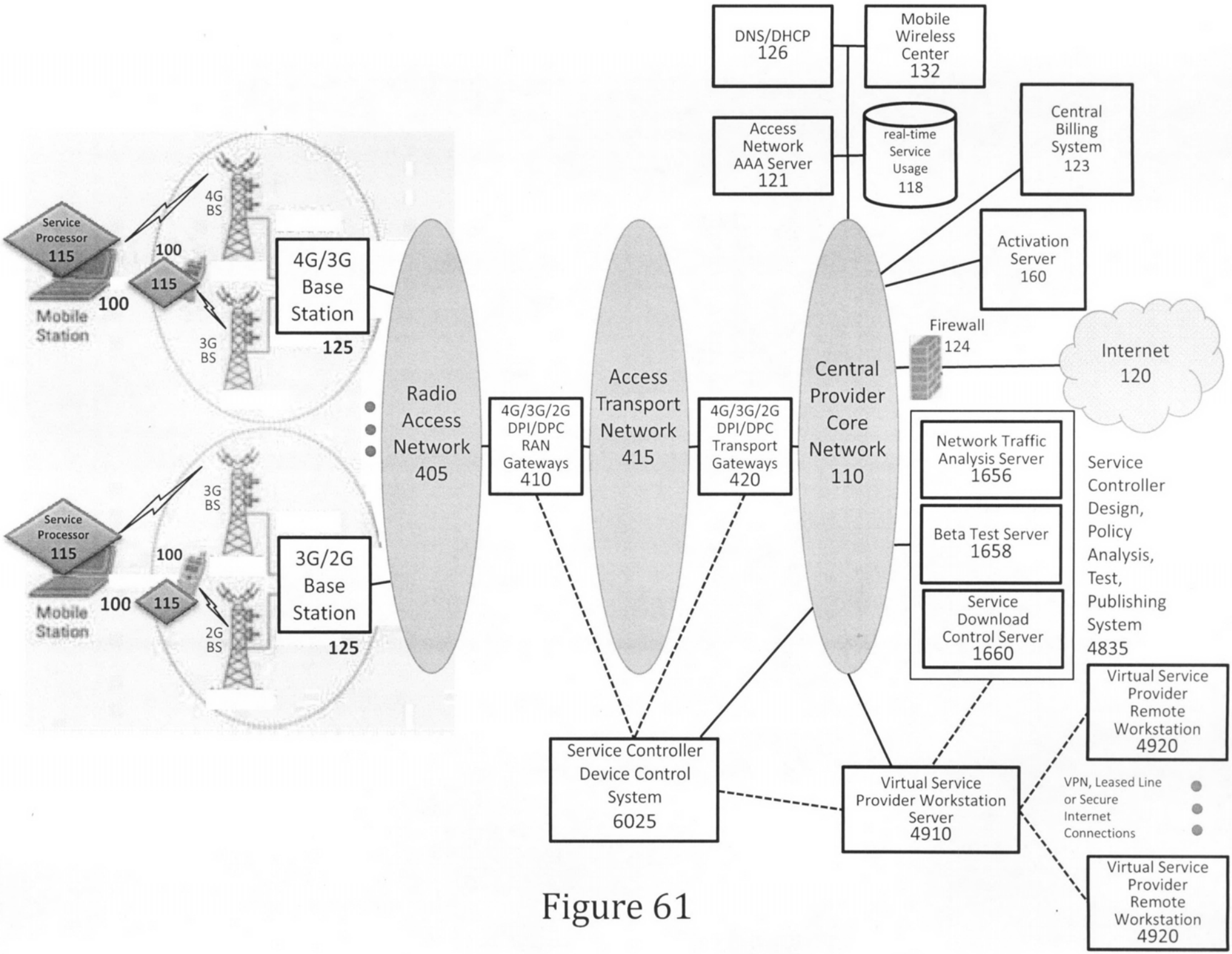

DNS/DHCP
126
Mobile
Wireless
Center
132
Access
Network
AAA Server
121
real-time
Service
Usage
118
Central
Billing
System
123
Activation
Server
160
Service
Processor
115
100
115
100
Mobile
Station
4G
BS
3G
BS
4G/3G
Base
Station
125
Radio
Access
Network
405
4G/3G/2G
DPI/DPC
RAN
Gateways
410
Access
Transport
Network
415
4G/3G/2G
DPI/DPC
Transport
Gateways
420
Central
Provider
Core
Network
110
Firewall
124
Internet
120
Network Traffic
Analysis Server
1656
Beta Test Server
1658
Service
Download
Control Server
1660
Service
Controller
Design,
Policy
Analysis,
Test,
Publishing
System
4835
Service
Processor
115
100
115
100
Mobile
Station
3G
BS
2G
BS
3G/2G
Base
Station
125
Service Controller
Device Control
System
6025
Virtual Service
Provider Workstation
Server
4910
Virtual Service
Provider
Remote
Workstation
4920
VPN, Leased Line
or Secure
Internet
Connections
Virtual Service
Provider
Remote
Workstation
4920

Figure 61

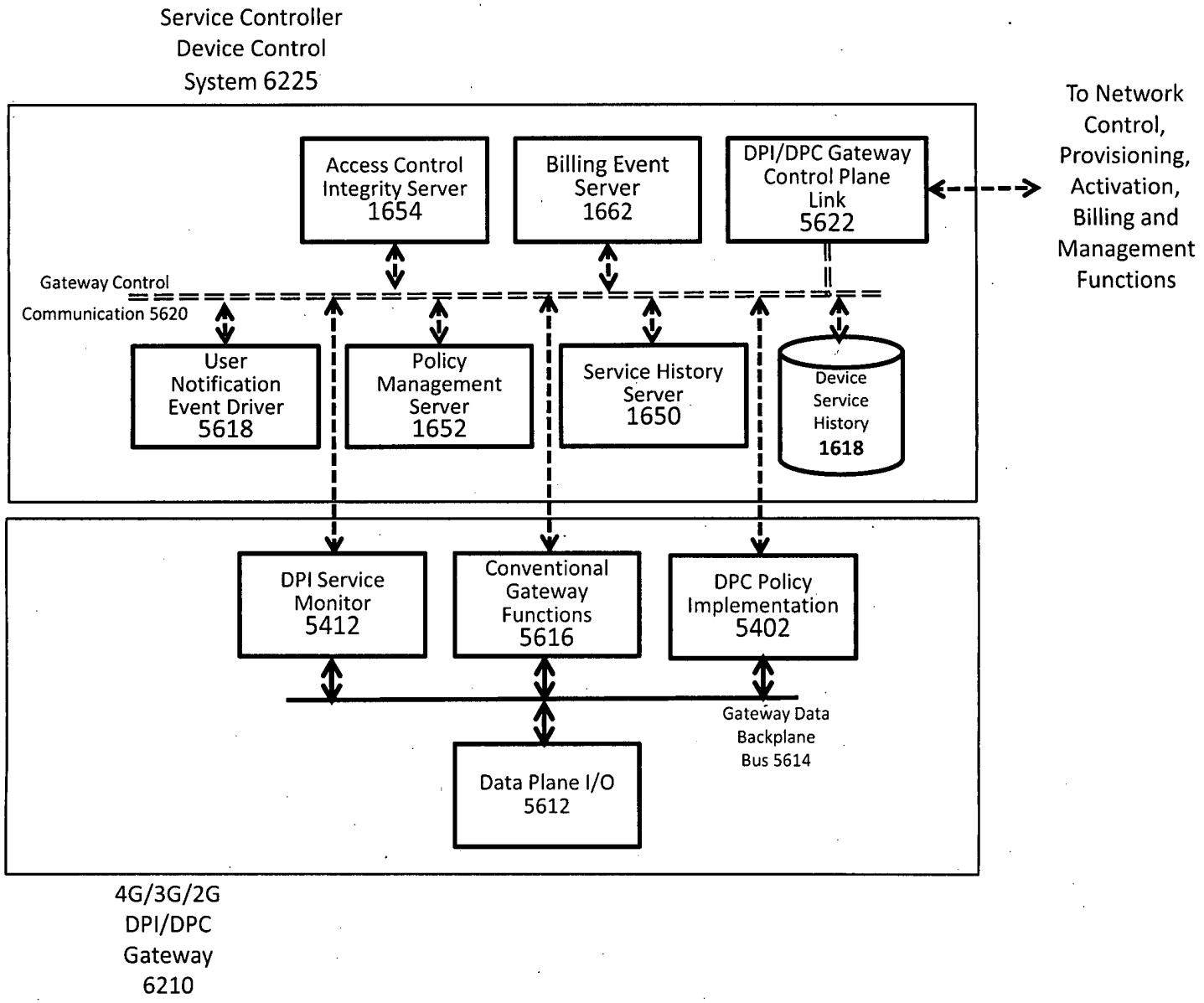

Service Controller
Device Control
System 6225
Access Control
Integrity Server
1654
Billing Event
Server
1662
DPI/DPC Gateway
Control Plane
Link
5622
To Network
Control,
Provisioning,
Activation,
Billing and
Management
Functions
Gateway Control
Communication 5620
User
Notification
Event Driver
5618
Policy
Management
Server
1652
Service History
Server
1650
Device
Service
History
1618
DPI Service
Monitor
5412
Conventional
Gateway
Functions
5616
DPC Policy
Implementation
5402
Gateway Data
Backplane
Bus 5614
Data Plane I/O
5612
4G/3G/2G
DPI/DPC
Gateway
6210

Figure 62

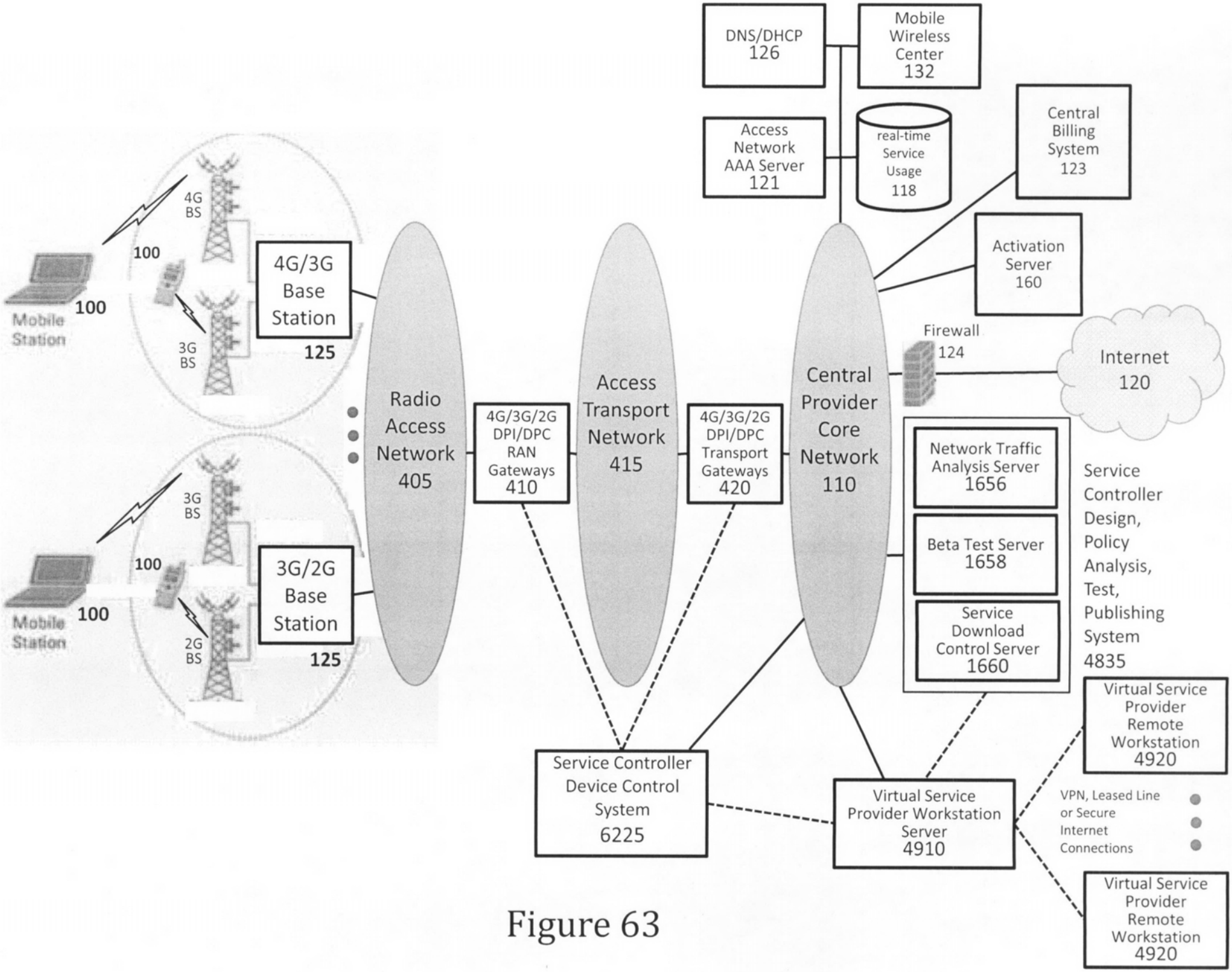

DNS/DHCP
126
Mobile
Wireless
Center
132
Access
Network
AAA Server
121
real-time
Service
Usage
118
Central
Billing
System
123
Activation
Server
160
Firewall
124
Internet
120
4G
BS
100
100
Mobile
Station
4G/3G
Base
Station
125
3G
BS
Radio
Access
Network
405
4G/3G/2G
DPI/DPC
RAN
Gateways
410
Access
Transport
Network
415
4G/3G/2G
DPI/DPC
Transport
Gateways
420
Central
Provider
Core
Network
110
Network Traffic
Analysis Server
1656
Beta Test Server
1658
Service
Download
Control Server
1660
Service
Controller
Design,
Policy
Analysis,
Test,
Publishing
System
4835
3G
BS
100
100
Mobile
Station
3G/2G
Base
Station
125
2G
BS
Virtual Service
Provider
Remote
Workstation
4920
Service Controller
Device Control
System
6225
Virtual Service
Provider Workstation
Server
4910
VPN, Leased Line
or Secure
Internet
Connections
Virtual Service
Provider
Remote
Workstation
4920

Figure 63

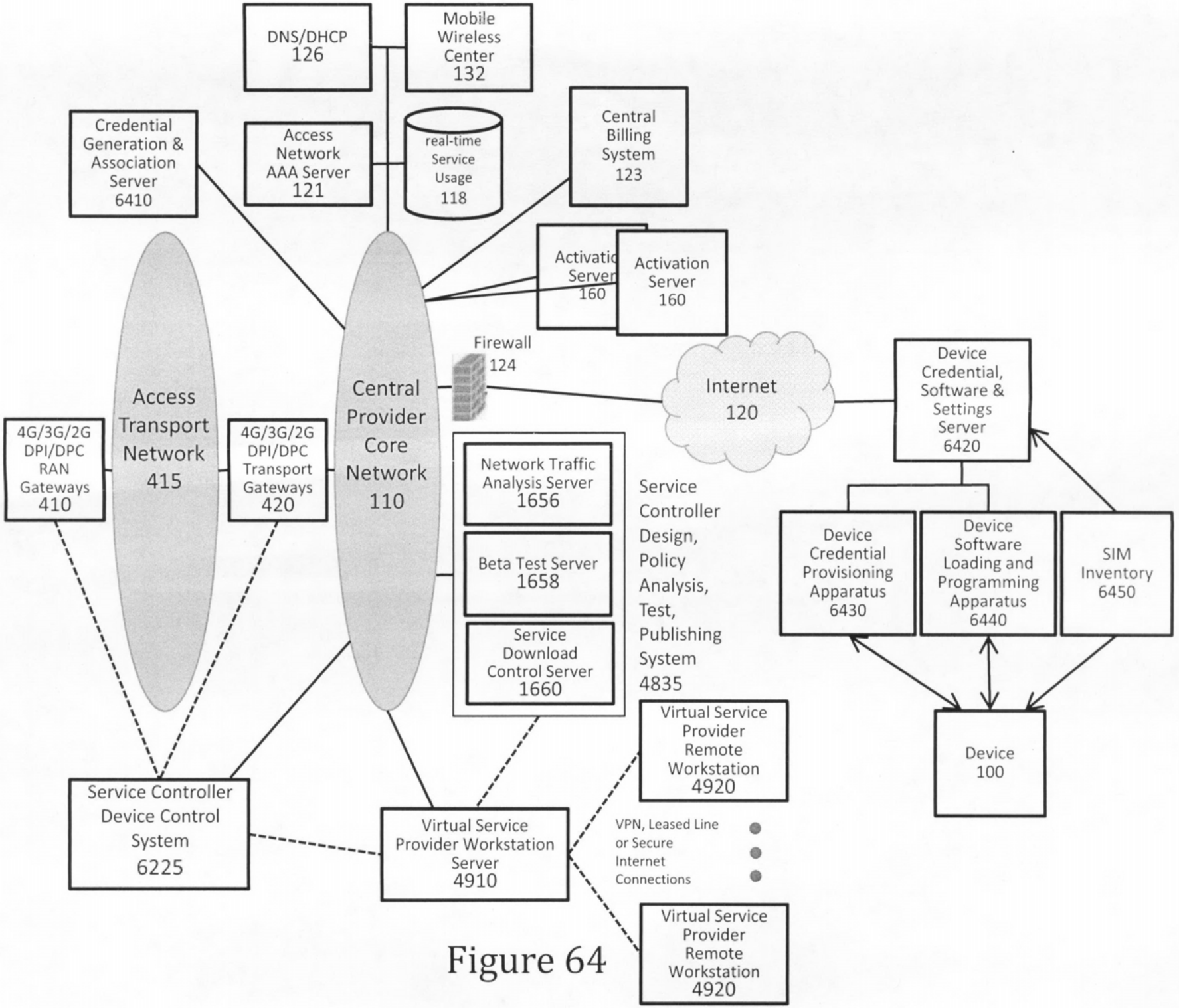

DNS/DHCP
126
Mobile
Wireless
Center
132
Credential
Generation &
Association
Server
6410
Access
Network
AAA Server
121
real-time
Service
Usage
118
Central
Billing
System
123
Activation
Server
160
Activation
Server
160
Firewall
124
Internet
120
Device
Credential,
Software &
Settings
Server
6420
Access
Transport
Network
415
Central
Provider
Core
Network
110
4G/3G/2G
DPI/DPC
RAN
Gateways
410
4G/3G/2G
DPI/DPC
Transport
Gateways
420
Network Traffic
Analysis Server
1656
Beta Test Server
1658
Service
Download
Control Server
1660
Service
Controller
Design,
Policy
Analysis,
Test,
Publishing
System
4835
Device
Credential
Provisioning
Apparatus
6430
Device
Software
Loading and
Programming
Apparatus
6440
SIM
Inventory
6450
Device
100
Virtual Service
Provider
Remote
Workstation
4920
Service Controller
Device Control
System
6225
Virtual Service
Provider Workstation
Server
4910
VPN, Leased Line
or Secure
Internet
Connections
Virtual Service
Provider
Remote
Workstation
4920

Figure 64