



(51) International Patent Classification:

H04W 40/24 (2009.01) *H04W 84/18* (2009.01)

(21) International Application Number:

PCT/IB2018/000075

(22) International Filing Date:

24 January 2018 (24.01.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/450,350 25 January 2017 (25.01.2017) US

(71) Applicant: **AIRTIES KABLOSUZ İLETİSİM SANAYİ VE DİŞ TİCARET A.Ş.** [TR/TR]; Mithat Ünlü Sk. No:23, Esentepe, İstanbul 34394 (TR).(72) Inventors: **ALPER, Akcan**; Mithat Ünlü Sk. No:23, Esentepe, İstanbul 34394 (TR). **ACAR, İrfan**; Mithat Ünlü Sk. No:23, Esentepe, İstanbul 34394 (TR). **HATİPOĞLU, Bilal**; Mithat Ünlü Sk. No:23, Esentepe, İstanbul 34394 (TR).**KARACA, Mustafa**; Mithat Ünlü Sk. No:23, Esentepe, İstanbul 34394 (TR). **PAKKAN, Mujdat**; Mithat Ünlü Sk. No:23, Esentepe, İstanbul 34394 (TR). **MUNGAN, Devin**; Mithat Ünlü Sk. No:23, Esentepe, İstanbul 34394 (TR).(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

(54) Title: ISLAND TOPOLOGIES AND ROUTING IN HYBRID MESH NETWORKS

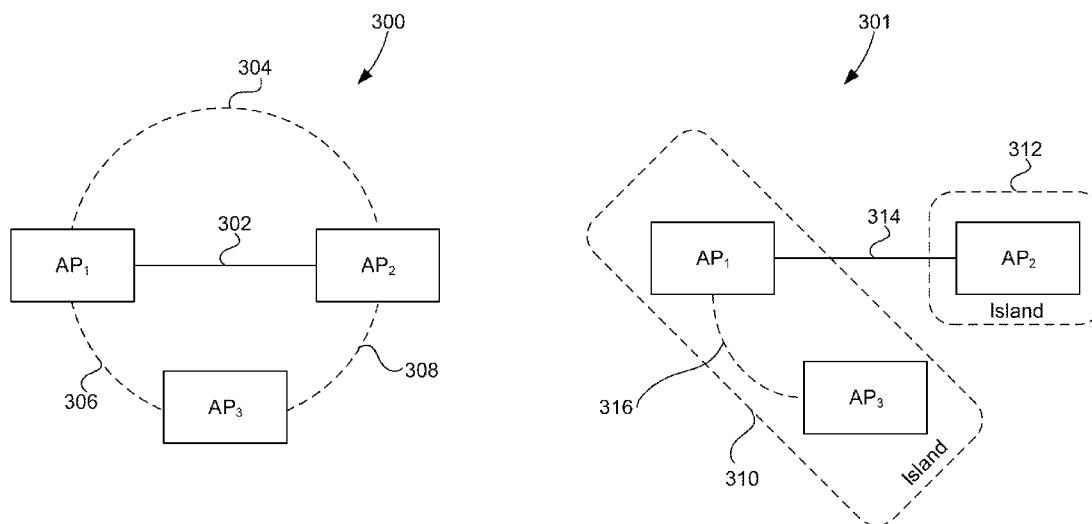


FIG. 3

(57) **Abstract:** A wireless network device may receive, over an interface, a broadcasted hello message that indicates network topology and interface information of neighbor nodes in a network. The wireless network device may transmit an announce message to unblocked hello peers of the wireless network device. The wireless network device may receive, on a wired interface from another node, a hello message. The wireless network device and the another node may each be identified as island heads based on the received hello message. The wired interface may be utilized for connecting the island heads.



EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

ISLAND TOPOLOGIES AND ROUTING IN HYBRID MESH NETWORKS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 62/450,350, filed January 25, 2017, which is incorporated by reference as if fully set forth.

BACKGROUND

[0002] Hybrid mesh networks are being utilized to extend coverage areas, provide better coverage areas with fewer dead spots, improve throughput and reliability, or the like. Hybrid mesh networks also provide diverse networks by combining different wired and wireless interfaces between access points (APs), gateways, routers, nodes, client devices, or the like. Specialized protocols for discovery, formation, routing, and learning algorithms are desirable to quickly and automatically build and maintain reliable hybrid mesh networks.

SUMMARY

[0003] An island or cluster may be formed in a hybrid mesh network with nodes utilizing different wired or wireless interfaces. A hybrid mesh network may be partitioned into mesh islands or clusters using a protocol to reduce disruptions, interference, or the like. Once an island or cluster topology is formed, optimal routes or paths from a source node in the hybrid mesh network to any destination node that minimize or meet a target metric or path cost may be utilized.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] A more detailed understanding may be had from the following description, given by way of example in conjunction with the accompanying drawings, wherein like reference numerals in the figures indicate like elements, and wherein:

[0005] FIG. 1 is a diagram illustrating an example of an access point (AP), router, gateway, or node;

[0006] FIG. 2 is a diagram illustrating an exemplary topology of a mesh network;

[0007] FIG. 3 is a diagram illustrating an exemplary topology of a mesh network with islands;

[0008] FIG. 4 is a diagram illustrating exemplary mesh island networks with island heads;

[0009] FIG. 5 is a diagram illustrating an exemplary topology having an ethernet loop;

[0010] FIG. 6 is a diagram illustrating an exemplary topology with access point (AP) and/or router island heads utilizing ethernet;

[0011] FIG. 7 is a diagram illustrating an example of routing in a mesh network;

- [0012] FIG. 8 is a diagram illustrating an exemplary routing process in a mesh network;
- [0013] FIG. 9 is a diagram illustrating an exemplary process for *hello* message processing;
- [0014] FIG. 10 is a diagram illustrating an exemplary process for *announce* message processing;
- [0015] FIG. 11 is a diagram illustrating an exemplary process for peer learning;
- [0016] FIG. 12 is a diagram illustrating another exemplary process for peer learning;
- [0017] FIG. 13 is a diagram illustrating an exemplary process for interface blocking in relation to post-routing;
- [0018] FIG. 14 is a diagram illustrating an exemplary process for interface blocking in relation to local-in operations;
- [0019] FIG. 15 is a diagram illustrating an exemplary process for interface blocking in relation to local-out operations;
- [0020] FIG. 16 is a diagram illustrating an exemplary process for routing; and
- [0021] FIG. 17 is a diagram illustrating an example of a process of protocol message handling with recalculation of routing paths and updating of a routing table.

DETAILED DESCRIPTION

[0022] In the examples given herewith, information may be communicated, signaled, conveyed, or provided in island or cluster of a hybrid mesh network. Although hybrid mesh networks are referenced, the examples of island formation, routing, interference management, topologies or the like may be utilized, configured, or applicable to any mesh network that employs two or more communication interfaces. Also, in the examples given herewith, a packet, traffic, a part of traffic, or frame may be used interchangeably.

[0023] Although any protocol or communication layer, sub-layer, partial layer, a portion of a layer, a layer portion, or the like may be utilized, examples of utilizing layer 2 to form topologies or networks are given herewith. In addition, layer 2 may comprise sub-layers, partial layers, a portion of a layer, or the like. A routing algorithm for hybrid mesh networks may comprise nodes with any combination of 802.11xx (e.g., 802.11ac, 802.11ax, etc.), Wi-Fi, ethernet, power-line communication (PLC), multimedia over coax alliance (MoCA), personal area network (PAN), small cell, metropolitan area network (MAN), and wide area network (WAN) network interfaces or links.

[0024] Nodes in a mesh network may be partitioned into mesh islands connected or coupled to one another by the 802.11xx, Wi-Fi, ethernet, PLC, and/or MoCA links of commodity devices in the network. A commodity device may be home networking devices, wireless routers, routers, wireless gateways, gateways, range extenders, wireless bridges, bridges, wireless

switches, switches, ethernet switches, or the like. In addition to preventing or reducing possible mutual disruptions between a mesh routing algorithm and “learning” processes of commodity devices, examples are given to reduce overall wireless interference. For example, such interference may be reduced by configured or operating mesh islands on non-interfering wireless channels or resources.

[0025] In the examples given herewith, for identified island heads or cluster gateways, mesh nodes may be assigned to islands such that path costs to the island heads may be reduced, minimized, or optimized. Once an island topology is formed, the best or optimal route from any source node in the mesh network to any destination node may be determined such that the path cost is reduced, minimized, or optimized.

[0026] Using multiple 802.11xx access points (APs) and/or routers with meshing may improve or expand the wireless coverage area, connection speed, or throughput in a network. APs and/or routers may form a mesh network topology and cooperate in the distribution of data that originates from or is destined to wireless clients or other nodes.

[0027] FIG. 1 is a diagram illustrating an example of an AP, router, gateway, or node 100. An AP, router, gateway, or node 100 may include one or more processors/controllers 102 that utilize memory(s) 104 to process *hello* messages, *announce* messages, routing information, or the like communicated with one or more wireless/wired interface(s) 106 as given in the examples herewith. The AP, router, gateway, or node 100 may include one or more power source(s) 108.

[0028] One or more processors/controllers 102 may be a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Array (FPGA) circuits, any other type of integrated circuit (IC), a state machine, and the like. Memory(s) 104 may include one or more of a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, flash memory, magnetic media such as internal hard disks and removable disks, magneto-optical media, and optical media, or the like. One or more wireless/wired interface(s) 106 may include one or more transceivers, transmitters, receivers, amplifiers, signal converters, antennas, or the like to facilitate networking.

[0029] Examples are given herewith to automate set up and administering and reducing maintenance of network devices, such as commodity devices, to enhance or simplify usability. For example, when system requirements are reduced to an essential set and a mesh network is formed in the presence of an Internet gateway, which also dictates the mesh network configuration, complications may be avoided. Also, when device drivers and low-level software libraries provided

by chip vendors may need modification or are incapable of updates, software maintenance may be simplified, version upgrades may be smoother, and addition of mesh support to commodity gateways may be quicker with the examples given herewith.

[0030] An approach for automatic configuration and maintenance of gateway-centric Wi-Fi mesh networks is described in U.S. Provisional Patent Application 62/448,718, filed January 25, 2017, which is incorporated by reference as if fully set forth. APs or routers that form a mesh network may be paired with a gateway device by simply pushing a button. Initial network or system configuration information and/or any subsequent changes needed by the gateway device may be automatically propagated throughout a mesh network with little or no user intervention. Replacement of the gateway device of a mesh network or pairing of an AP and/or router with another gateway device may also be handled automatically by a simple button push. In addition, an operating channel(s) of a mesh network may be automatically changed when a radar signal is detected by any node in the mesh network.

[0031] Examples are given herewith for configurations and/processes to form mesh islands and routing of traffic, such as layer 2 traffic, between mesh nodes based on path costs. This may be performed and desired after a mesh node is paired with another and basic network configuration information, such as network service set identifier (SSID), operating channel, and passphrase, are shared by mesh nodes. Routing algorithms and island formation algorithms for hybrid mesh networks may be performed as given in U.S. Patent Application Serial No. 14/166,040, which issued on August 30, 2016 as U.S. Patent No. 9,432,990, and U.S. Patent Application Serial No. 14/757,422, filed December 23, 2015, respectively, which are incorporated by reference as if fully set forth.

[0032] In the examples given herewith, once encrypted links between mesh nodes are established, a layer 2 routing protocol may be performed. Finding the best, good, or optimal routes between mesh nodes may need mesh network topology information. Topology discovery may be accomplished by exchanging messages such as *hello* or *announce* messages. The *hello* messages may enable nodes to discover neighbors or nearby nodes and thus establish and maintain neighbor relationships. The *announce* messages may propagate network topology information throughout the mesh network.

[0033] In an example, certain messaging may be handled by a custom or optimized layer 2 transport module using a custom EtherType field. The layer 2 transport protocol may provide reliable, ordered, fragmented, and/or error-checked delivery service of packets, traffic, a part of traffic, or frames between nodes of a mesh network. For certain configurations, messages may be acknowledged utilizing a message type and sequence number. If an expected acknowledgement is

not received, the message may be retransmitted for a maximum retry count. Although any maximum retry count may be configured, a retry count of 4, using a delay scheme of, for example, 1, 2, 3, and 5 seconds may be utilized or configured. Fragmentation size may be configured based on the maximum transmission unit (MTU) size of the medium.

[0034] An optimized transport module may also provide generic communication services between software modules running on mesh nodes. This service may be used by higher layer applications through an exposed payload Application Programming Interface (API). Applications may bind to a payload ID in the range from 0 to 255, for example, and send and receive encrypted and authenticated payloads facilitated by the cryptographic encryption and authentication algorithms. These algorithms may be included in the user space library. In addition, each payload may be encrypted by a user supplied secret key and/or a globally unique nonce. Nonce lengths such as 128-bit or any other length may be utilized.

[0035] The message type for a *hello* or *announce* message may be indicated by a field in the message header. A sequence number in the message header may enable ordered delivery and a hash-based message authentication code (HMAC) field may provide data integrity and authentication. Messages larger than a configured MTU size may be fragmented. Fragmentation may be performed utilizing a fragment number field in the message header and reassembled by a receiver.

[0036] In the examples given herewith, message contents may be encoded as type-length-value (TLV) elements inside a message body. An element value field may be any size, such as 256 bytes. However, larger elements may be sent divided into chunks, such as 256 bytes, and then reassembled by the receiver. Examples of TLV elements that may be included in *hello* and *announce* messages are listed in Table 1 and Table 2, respectively.

Node ID
Node Medium Access Control (MAC) address
Node capabilities
Interface ID
Interface MAC address
Interface type

Table 1: *Hello* message

Message flags
Node ID
Node Medium Access Control (MAC) address
Node capabilities
Node lifetime
Node sequence
Interface ID
Interface MAC address
Interface type
Interface metric
Peer ID
Peer MAC address
Peer flags

Table 2: *Announce* message

[0037] In the examples given herewith, a mesh node may have multiple network interfaces such as 802.11xx, Wi-Fi, ethernet, PLC, and/or MoCA (for clients and mesh peers). A separate *hello* message may be broadcast by a node on each configured network interface. The *Interface type* element in the *hello* message may indicate the type of the particular interface. The *hello* messages may enable nodes to discover their neighbors and interfaces being utilized. The *hello* messages may be broadcasted, for example, every 1-10 seconds on the 802.11xx, Wi-Fi, ethernet, PLC, and/or MoCA and wireless distribution system (WDS) links.

[0038] In certain exemplary configurations, a node that receives a *hello* message over a WDS link may initialize a sending peer in a *blocked* state and *announce* this information to the network. A *hello* message count may be utilized for WDS links for network management. On ethernet, PLC, and MoCA links, a sending node may be initialized as an unblocked peer. The peer state information may be carried in the *Peer Flags* element of the *announce* message. When a peer is in a blocked state, protocol messages, other than *hello*, data packets, traffic, a part of traffic, or frames may not be processed.

[0039] A receiving node may also flush *learned peer* information for a given receiving interface. Such flushing may be desirable for partitioning of the network to mesh islands. After

receiving, for example, 10 *hello* messages from a peer an operation to transition to an *unblocked* state may be performed and announced to the network. The time needed to unblock a peer may depend on a configured *hello* period.

[0040] Mesh nodes may propagate network topology information by sending periodic *announce* messages to unblocked *hello* peers. Such *announce* messages may be utilized in particular for ethernet, PLC, MoCA, or WDS links. The *announce* messages may be sent upon a topology change in order to quickly respond to topology changes.

[0041] In the examples given herewith, an announcement period may be configured to any value from 0 to infinite seconds (e.g., every 30 seconds). Configuring the interval to zero may disable periodic announcements. For this configuration, the announcements may be sent or triggered when a topology, node, link, etc. changes rather than being sent regularly. In addition, *announce* messages may be unicasted. For unicasting, a message may be acknowledged and also forwarded by recipients. Forwarded messages may be terminated with the help of message sequence numbers.

[0042] A node that receives an *announce* message may update mesh network nodes and a routing table upon any changes. In certain configurations, a receiving node may forward an *announce* message only when network information is changed. A generic communication service provided by the transport module may be piggy-backed on *announce* messages for applications that can tolerate a delay of at most equal to the announcement period.

[0043] Nodes may periodically check node lists to ensure that old, expired, stale, etc. information is removed. For example, if a node is idle for more than 120 seconds it may be invalidated. A learned peer idle for more than, for example, 300 seconds, may be deleted. Expiration times for idleness may be configured according to the value of the announcement period and should preferably be on the order of a few times the announcement period. In either configuration, routes may be updated and event-based announcements may be sent. As the *announce* message reception times may be random, the staleness checking period may be adjusted for a trade-off between computation load and responsiveness of the algorithm.

[0044] Again referring to Table 2, the *Interface Metric* field may indicate the cost of transmissions from the node to the peer through the given interface. The quality of a link may be assessed by using different cost metrics. Multiple examples exist for computing the cost metric for a link. Examples can be found in UK Patent Application Number GB1700997.8, which is incorporated by reference herein as if fully set forth. A possible link cost metric is given in Equation (1).

$$C = \frac{50000}{1 + \lfloor R/20 \rfloor} \quad \text{Equation (1)}$$

Cost metric C may be inversely proportional to a current physical layer transmission rate R in Kbps to the peer node. Thus, faster links may have lower costs and favored. Cost may also be proportional to transmission airtime. A link cost metric may be computed by another software process running on the node and passed on to a routing process via a software bus. Optimum routes from any source to destination node in a mesh network may be computed using link costs to minimize total transmission cost.

[0045] To prevent replay attacks, each node may generate a new random number every, for example, 30 seconds to include in transmitted *hello* messages. Each interface that receives a peer node's random number may include it in its own *hello* messages along with its own node's random number. If a received *hello* message does not include the receiving node's current random number, it may be discarded. A current random number with message integrity provided by the HMAC may provide sufficient security for the routing algorithm.

[0046] As traffic flows through the ports of a commodity switch (e.g. ethernet switch), sent frames may be examined by attached nodes and source Medium Access Control (MAC) addresses recorded. A switch may thus build a MAC address versus port number table and "learn" locations or existence of MAC destinations. In certain configurations or examples given herewith, a switch may forward received frames directly to a correct port without flooding or broadcasting on all ports.

[0047] FIG. 2 is a diagram illustrating an exemplary topology 200 of a mesh network. Wireless links 214, 212, and 216 may connect or couple STA₁, STA₂, and STA₃ to AP₁, AP₂, AP₃, respectively. An STA may be a mobile device, sensor, internet of thing (IoT) device, laptop, notebook, tablet, smart phone, television, display, wireless audio device, wireless speaker, or the like. AP₂ and AP₃ may be connected to a switch (e.g. ethernet switch) using wired links 202 or 206. AP₁ may be connected to both AP₂ and AP₃ via WDS links 208 or 210, respectively. STA₄ may be connected or coupled to the switch via wired link 204.

[0048] In certain configurations, WDS link 208 between AP₁ and AP₂ may have a smaller or desired cost compared to the cost of WDS link 210 between AP₁ and AP₃. Link costs may be lower due to physical proximity allowing a much higher data rate or throughput due to higher signal strength or signal to noise ratio (SNR). If STA₁ has data to send to STA₄, a mesh routing algorithm may utilize path STA₁ → AP₁ → AP₂ → STA₄ due to lower cost. In topology 200, data packets or frames originating from STA₁ may enter the switch on its port x . Correspondingly, the switch may "learn" from the source MAC address of these packets or frames that STA₁ is reachable through port x . Thus, when STA₄ tries to send data to STA₁, the switch may forward these data packets or frames to port y and x .

[0049] Costs of wireless links may change over time and costs may be asymmetric. For example, AP_1 may move closer to AP_3 or a strong interferer might appear near AP_2 . In addition, while the cost of the link $AP_1 \rightarrow AP_2$ might be lower than the cost of $AP_1 \rightarrow AP_3$, the cost of $AP_3 \rightarrow AP_1$ might be lower than the cost of $AP_2 \rightarrow AP_1$. For this situation, it might be more beneficial to use the $AP_3 \rightarrow AP_1$ link instead of the $AP_2 \rightarrow AP_1$ link. The $AP_3 \rightarrow AP_1$ link may also be preferred to obtain better quality of service (QoS) or improved load balancing.

[0050] If link 208 between AP_2 and AP_1 is temporarily broken or unavailable, a switch may still attempt to send packets or frames destined to STA_4 to port x utilizing link 202. These packets or frames may get lost even though link 210 between AP_3 and AP_1 is available to carry the information to the destination. In examples given herewith, conflicts may be avoided when a learning process of a switch operates independent of the mesh routing algorithm run by the APs.

[0051] In addition, for load balancing or QoS purposes multiple paths may be utilized at the same time. For instance, AP_1 may send a packet or frame through AP_2 and the next through AP_3 . However, frequent path changes may complicate or confuse the learning process of the switch. For instance, it may appear that STA_1 is quickly moving between port x and port z. When utilizing multiple paths, the internal routing table updates of the switch might not be able to keep up leading to dropped packets or frames or unpredictable forwarding decisions.

[0052] Commodity switches may run a spanning tree protocol (STP) to prevent the formation of network loops. However, switch ports blocked by the STP may interfere with the mesh routing protocol and prevent the routing protocol messages from reaching their destinations. In order to avoid this scenario, when two or more mesh nodes are connected via a switch, a mesh network may be partitioned into mesh islands or clusters. Nodes that are connected via a switch may become island heads, cluster gateways, or gateways between mesh islands.

[0053] In certain configurations, commodity PLC devices in a mesh network may keep their own MAC address tables and run their own MAC layer routing and repeating algorithms which might interfere with the mesh network routing. Therefore, a mesh network may also be partitioned into islands when two or more mesh nodes are connected via a commodity PLC device. PLC network interfaces of mesh nodes may be controlled by routing algorithms given herewith and thus may not need to be considered for partition separators.

[0054] It may also be desirable to separate a mesh network into islands so that that each island operates on a different channel or resources reducing interference with other islands that are within a transmission and/or interference range. This may reduce the broadcast collision domain and increase available airtime for active mesh nodes. In addition, partitioning a mesh network into

smaller mesh islands may alleviate multi-hop unfairness observed in other or larger wireless mesh network configurations.

[0055] FIG. 3 is a diagram illustrating an exemplary topology of a mesh network with islands. Topology or graph 300 may be a mesh network where AP_1 and AP_2 are connected or coupled with wired link 302 (e.g., ethernet). WDS links 304, 306, or 308 may be utilized to mesh AP_1 , AP_2 , and AP_3 . Since there is a wired link 302 between AP_1 and AP_2 , the APs may be identified or designated as island heads.

[0056] Two mesh islands 310 and 312 may be formed around island heads AP_1 and AP_2 as shown in topology or graph 301 by utilizing wired link 314 and WDS link 316. The third node AP_3 may be assigned to one of the islands and with wireless links with nodes in other islands being blocked, disabled, disallowed, forbidden, or the like. In topology or graph 301, the third node AP_3 may be assigned to the island of node AP_1 since WDS link 316 to AP_1 may have a lower cost, and a wireless link to node AP_2 is removed. Moreover, APs or routers may have multiple interfaces (e.g. ethernet) that are part of an embedded switch. Thus, in topology or graph 301 the interfaces of two wireless APs or routers may be connected via a switch or directly via a wire or cable.

[0057] FIG. 4 is a diagram illustrating exemplary mesh island networks with island heads 400. As *announce* messages propagate the topology graph information throughout a mesh network, nodes may have the necessary information to separate the mesh nodes into islands (402). Nodes that may be *island heads* may be found or identified (404). If a node has a *hello* peer on any ethernet, PLC, and/or MoCA interface, it may be marked as an island head. Thus, the number of mesh nodes that are island heads may be equal to the number of mesh nodes that have an ethernet, PLC, and/or MoCA peer.

[0058] To form mesh island networks with island heads, a large or all amount of island partitioning possibilities may be computed with the constraint that wireless data connections between nodes in different islands may be blocked, disabled, disallowed, forbidden, or the like and a partitioning scheme that minimizes a metric, such as link costs, may be selected. A possible metric may be the maximum cost of a node to the nearest island head or the sum of the costs of all nodes in a given island to its head.

[0059] Considering a large or all possibilities may quickly become computationally intensive as the number of mesh nodes increases, especially when the network topology changes and it is desirable for a routing algorithm to respond quickly. An iterative algorithm may be utilized to approximate the optimum solution. After determining mesh island heads, wireless data links between island heads may be blocked, disabled, disallowed, or forbidden.

[0060] Nodes that are *hello* peers of at least one island head may be determined and a minimum path cost computed to each one of the island heads. In addition, other possible metrics could be sum of the costs of all nodes in an island to island head or the maximum cost in an island to the island head. A minimum or shortest path between nodes in a mesh network may be determined by using any deterministic algorithms such as the Dijkstra algorithm or the Bellman-Ford algorithm.

[0061] Once a node that has the smallest minimum path cost in a group is identified, it may be assigned to the corresponding island head. This process may continue to form an initial group of nodes that are *hello* peers of island heads. Wireless links that may exist between this node and any one of the other island heads may then be blocked, disabled, disallowed, forbidden, or the like. Remaining nodes in the initial group may then be considered and their minimum path costs to each one of the island heads may be re-computed. Any wireless data links that may exist between this node and any other island may be also blocked. This may be repeated until all remaining nodes in the initial group are assigned to an island.

[0062] A second group may comprise orphan nodes (406) that are *hello* peers of at least one node in the first group. An orphan node may be a non-assigned node in any group. The nodes in the second group may be assigned (408) to islands using algorithms given herewith. Minimum path costs to island heads are recomputed, and in each step the node with the smallest minimum path cost is assigned to the corresponding island and its wireless links to other islands are blocked, disabled, disallowed, forbidden, or the like until all nodes in the second group are assigned to an island. This may be repeated until all nodes in the network are assigned to an island.

[0063] FIG. 5 is a diagram illustrating an exemplary topology 500 having an ethernet loop due to a configuration error, glitch, or the like. The loop created between a switch, AP₁, and AP₂ with wired links 502, 504, and 506 may cause broadcast storms. Although STP may prevent such loops, in the examples given herewith such loops may be avoided in a mesh network. For instance, a *root* node may trace the *hello* peers of nodes to prevent such a loop.

[0064] In the examples given herewith, an arbitrary node may be selected and only related *hello* peers considered. Each one of these peers and its *hello* peers may be looked at among the remaining nodes. At a given iteration, if a starting node is reached a loop in the topology may be identified. Such a loop may be broken by blocking, disabling, disallowing, forbidding, or the like one of the links in the chain. The link to block can be determined, for example, by selecting the link with the slowest connection speed. Other approaches could be to block the link such that the resulting topology minimizes the maximum number of hops to the gateway of the mesh network. Path costs may be accounted or computed, such as with Equation (1), and the maximum cost among the loop

nodes to the mesh gateway minimized. If the gateway is not known, minimizing the maximum number of hops or maximum path cost between any two nodes in the loop may be attempted.

[0065] FIG. 6 is a diagram illustrating an exemplary topology 600 with AP and/or router island heads utilizing ethernet. For this topology, AP₁, AP₂, AP₃, and AP₄ may be configured as island heads since they may have ethernet *hello* peers across links 602, 604, and 610. For certain configurations, island separation or partition algorithms may block, disable, disallow, forbid, or the like wireless connections between different islands. However, this may result in disconnections between islands 612 and 614. Without wireless links 606 or 608, AP₁ would only be connected to AP₂, and AP₃ would only be connected to AP₄. Thus, no connection between islands 612 and 614 would exist. To prevent possible disconnections between islands, a wireless link may be reinstated to obtain a fully connected topology. However, the two island heads connected with a wireless link may have to operate on the same wireless channel or resource causing potential interference.

[0066] A *root* node of a mesh network may be elected based on the node IDs and node MAC addresses to prevent undesirable network configurations or architectures. For instance, the node that has the smallest node ID and MAC address combination may be elected. The *root* node may check for disconnected clusters after identifying island heads and determines which wireless links should be reinstated to form a fully connected graph. Suitable metrics could be, for example, the maximum path cost among all nodes to the mesh gateway or the maximum path cost between any two mesh nodes if the gateway is not known.

[0067] FIG. 7 is a diagram illustrating an example of routing 700 in a mesh network. Incoming and outgoing packets, traffic, a part of traffic, or frames on each interface may be filtered for mesh routing, peer learning, protocol message handling, or the like. Traffic 702 from a network interface may be inputted for pre-routing. Pre-routing may be triggered by incoming traffic from any network interface after entering the network stack. Once triggered, any routing decision may be halted.

[0068] Traffic from pre-routing output 704 may be conveyed for further routing. Traffic from routing output 706 may be conveyed to a local-in component for output 708 to a local process. Traffic from local process input 712 may be conveyed to a local-out component for processing. Traffic from local-out output 710 may be conveyed for further routing. Traffic from routing output 714 may be conveyed for post-routing. Traffic from post-routing output 716 may be conveyed to the network interface.

[0069] Pre-routing, local-in, local-out, and post-routing may be operations related to packet filtering in a protocol or network stack of an operating system or operating system kernel. A packet or frame that enters a networking system may trigger these hooks while progressing through a

stack, allowing programs or applications that register with these hooks to interact at different points of a process. A pre-routing hook may be triggered by any incoming traffic soon after entering a network stack. This hook may be processed before any routing decisions are made of where to send the packet or frame. A local-in hook may be triggered after an incoming packet or frame is routed if the packet or frame is destined for a local system. The local-out hook may be triggered by any locally created outbound traffic soon after arriving at the network stack. The post-routing hook may be triggered by any outgoing traffic after routing has taken place and just before communication or signaling on a network interface.

[0070] As an example, Linux Netfilter operations for pre-routing, local-in, local-out, and post-routing may be utilized to determine if a packet or frame is going to be accepted, dropped, or passed to the routing process. Protocol message handling may include forwarding *announce* messages, updating a routing table, invalidating nodes, deleting a learned peer, or the like.

[0071] FIG. 8 is a diagram illustrating an exemplary routing process 800 in a mesh network. Once pre-routing (802) is initialized at a node(s), a determination or check is made if the received packet is a *hello* message (804). As an example, a *hello* message may be identified using a custom EtherType with a hello message type in a packet or frame header. If a *hello* message is identified, the *hello* message is processed (804) and subsequently dropped (806).

[0072] If the received packet is not a *hello* message a determination or check is made if the received packet is an *announce* message (810). As an example, an *announce* message may be identified using a custom EtherType with an announce message type in a packet or frame header. If an *announce* message is identified, the *announce* message is processed (812) and subsequently dropped (806). If the received packet is not an *announce* message, peer learning (814) and subsequently routing (816) are performed.

[0073] FIG. 9 is a diagram illustrating an exemplary process 900 for *hello* message processing. After initialization or processing of a *hello* message (902) at a node(s), existence of a peer (904) is determined. If a peer exists, a determination if a peer is blocked is made (906). If a peer is blocked, receipt of traffic on a WDS (908) and checking if a *hello* count is above a limit (910) are determined. If a *hello* count is above a limit, the peer is unblocked (912), an *announce* message is sent (914) to unblocked *hello* peers, and the process is stopped (916).

[0074] If a peer does not exist, a blocked peer is created (918), learned peers are flushed (920), an *announce* message is sent (914) to unblocked *hello* peers, and the process is stopped (916). If a peer is not blocked, a peer's idle time may be updated (922) and the process is stopped (916). Moreover, if WDS traffic is not received, the peer is unblocked (912) and process 900 proceeds as given herewith. Also, if the *hello* count is below a limit, the process is stopped (916).

[0075] FIG. 10 is a diagram illustrating an exemplary process 1000 for *announce* message processing. After initialization or processing of an *announce* message (1002) at a node(s), a determination of a topology change is made (1004). If the topology changed, a route update is processed (1006) and the *announce* message is forwarded (1008) to node peers to disseminate topology information. If a topology is the same or unchanged, the process is stopped (1010).

[0076] FIG. 11 is a diagram illustrating an exemplary process 1100 for peer learning. Peer learning may be a process or operation of discovering devices that are not mesh nodes. In peer learning, a mesh topology may be propagated via *announce* messages such that every node finds out about every other node and its connections or interfaces. However, in certain peer learning configurations commodity devices not configured for meshing will not send *announce* messages. Examples are given herewith for such devices to “learn” a network topology.

[0077] Process 1100 may be performed as part of a pre-routing operation. After initialization of a peer learning operation (1102) at a node(s), a determination of an interface being capable of peer learning is made (1104). If capable, a determination that the peer was already learned is made (1106). If a peer was already learned, the process is stopped (1108). Otherwise, a determination of a need to learn about the peer is made (1110).

[0078] If learning is unneeded, the process is stopped (1108). If learning is needed, the peer is learned (1112), an *announce* message may be sent (1114) to unblocked *hello* peers, and the operation is stopped (1108).

[0079] FIG. 12 is a diagram illustrating another exemplary process 1200 for peer learning. In certain configurations, process 1200 may be performed as part of a pre-routing operation. A mesh node may learn the source MAC address of an interface in the network similar to the learning processes of commodity switches (e.g. ethernet switches). An interface (e.g. ethernet interface) which does not belong to a mesh node and is not a peer of another mesh node may be a candidate for learning. Also if an interface and two mesh nodes are connected to the same switch, the interface may be learned by both of these mesh nodes. In certain configurations, two mesh nodes may need to be *hello* peers in order to learn the same interface.

[0080] After a determination of the need for peer learning is made (1202) at a node(s), a determination of the source being a mesh node is made (1204). If the source is a mesh node, peer learning may not be needed or performed (1216). If the source is not a mesh node, a determination of the interface having a *hello* peer is made (1206). If the interface does not have a *hello* peer, peer learning may be performed (1214).

[0081] If the interface has a *hello* peer, a determination of the source having another node's peer is made (1208). If the source is not another node's peer, peer learning may be

performed (1214). If the source is another node's peer, a determination of the source being on another island is made (1210). If the source is on another island, peer learning may not be needed or performed (1216).

[0082] If the source is not on another island, a determination if this and peer's node are island heads is made (1212) and if yes peer learning may be performed (1214). If this and peer's node are not island heads, peer learning is not needed or performed (1216).

[0083] FIG. 13 is a diagram illustrating an exemplary process 1300 for interface blocking in relation to post-routing. A post-routing operation may be triggered by outgoing or forwarded traffic after routing has taken place and before a packet or frame is being sent out by any network interface. Post-routing may be utilized for interface blocking or the like by dropping the frames. A post-routing process may be performed (1302) after a routing decision is made and a packet or frame is destined for a non-local device. A determination of an interface being blocked is made (1304). This may be designated specific to an outgoing interface selected by a routing block for the destination of a packet or frame. If an interface is blocked (1306), the packet, traffic, a part of traffic, or frame may be dropped (1306). Otherwise, if the interface is not blocked the packet, traffic, or frame is sent (1308).

[0084] FIG. 14 is a diagram illustrating an exemplary process 1400 for interface blocking in relation to local-in operations. Interface blocking by a local-in operation may be triggered after an incoming packet or frame that is destined for the local system is already or previously routed. If the network interface is blocked, the incoming frame may be dropped. In process 1400, after initialization of a local-in operation (1402) at a node(s), a determination of an interface being blocked is made (1404). If an interface is blocked, the packet, traffic, a part of traffic, or frame is dropped (1406). Otherwise, the packet, traffic, a part of traffic, or frame is accepted (1408) for further processing or routing.

[0085] FIG. 15 is a diagram illustrating an exemplary process 1500 for interface blocking in relation to local-out operations. A local-out operation may be triggered or performed by any locally created outbound traffic entering a network stack. A local-out operation may be utilized to pass locally generated outgoing packets or frames to routing. In process 1500, after initialization of a local-out operation (1502), a determination of an interface being blocked is made (1504). This determination may include a local network interface accepting a packet from the local system. If an interface is blocked, the packet, traffic, part of traffic, or frame is dropped (1506). Otherwise, the packet, traffic, a part of traffic, or frame is conveyed for further routing (1508).

[0086] When a packet, traffic, a part of traffic, or frame is passed to a routing process, it may be delivered to a target or an intermediate node on the best or optimal path to the target via a

routing table look up. A routing table may be updated on a topology change when needed. For instance, an update operation may be performed when a protocol message is received indicating a change or stale information is identified after a periodic timer is expired. If there is no entry in a routing table for a destination address, a routing process may queue packets or frames until the routing table is corrected or fixed. As an example, a maximum queue size may be 16 packets, and may be configured at runtime. A routing process may utilize acceleration back-ends for network delivery.

[0087] As an example, acceleration may refer to a 802.11xx or WiFi System on Chip (SoC) for certain configurations or scenarios forwarding packets or traffic entering a physical interface to the correct destination physical interface without passing the packet or traffic up a networking stack of the operating system first for further processing. This shortcut or hardware acceleration may provide higher throughput by avoiding the processing time of the packets or traffic in the networking stack.

[0088] FIG. 16 is a diagram illustrating an exemplary process 1600 for routing. After initialization of a routing operation (1602) at a node(s), a determination of an entry existing in a table is made (1604). If an entry exists, a determination of the traffic being for a local destination is made (1606). If the traffic is for a local destination, a local-in operation may be performed (1608). If the traffic is not for a local destination, a determination an interface existing is made (1616). If an interface exists, acceleration may be set (1618) and post routing may be performed (1622).

[0089] If a table entry does not exist, an entry is created (1610) and a determination of a queue being full is made (1612). Similarly, if an interface does not exist, a determination of a queue being full is made (1612). If a queue is full, the traffic may be dropped (1614). Otherwise, acceleration may be cleared (1620) and a queue operation performed (1624).

[0090] FIG. 17 is a diagram illustrating an example of a process 1700 of protocol message handling with recalculation of routing paths and updating of a routing table. After initialization of a route update (1702) at a node(s), learned peers may be validated (1704). During this process, invalid learned peers or peers that should not be learned may be deleted. Switched peers may be handled by deleting any peer nodes that have been disconnected and then connected to some other node (1706). An island graph may be built (1708) based on peer to peer connection topology. In the island graph, blocked peer to peer connections between islands may be marked.

[0091] A routing graph may be built out of nodes, interfaces, and/or peers based on connection topology and island setup (1710). A reverse routing graph may be built only for nodes (1712). A reverse graph may be utilized for node validation and may enable a network to dynamically or quickly respond to topology changes. A topology change may be caused by

disappearing nodes. The reverse graph may be checked to validate nodes (1714) for node connectivity and disappeared nodes may be marked as invalid. A validation of *hello* peers may be performed (1716) by marking peers in blocked *hello* status as invalid.

[0092] Moreover, in process 1700 invalid routes may be deleted (1718) for nodes, interfaces, or peers from the routing table. Blocked routes may be deleted for nodes, interfaces, or peers from the routing table (1720). A routing table may be calculated (1722) and populated for valid nodes, interfaces, and peers. Invalid nodes, interfaces, and peers may be deleted and marked as invalid from the topology graph (1724). Any unnecessary flags of nodes, interfaces, or peers may be cleared (1726).

[0093] Although features and elements are described above in particular combinations, one of ordinary skill in the art will appreciate that each feature or element can be used alone or in any combination with the other features and elements. In addition, the methods described herein may be implemented in a computer program, software, or firmware incorporated in a computer-readable medium for execution by a computer or processor. Examples of computer-readable media include electronic signals (transmitted over wired or wireless connections) and computer-readable storage media. Examples of computer-readable storage media include, but are not limited to, a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as internal hard disks and removable disks, magneto-optical media, and optical media such as CD-ROM disks, and digital versatile disks (DVDs).

* * *

CLAIMS

What is claimed is:

1. A wireless network device comprising:
 - a transceiver configured to receive a broadcasted hello message that indicates network topology and interface information of neighbor nodes in a network;
 - a processor configured to generate an announce message that includes the network topology and interface information;
 - the transceiver configured to transmit the announce message to unblocked hello peers of the wireless network device;
 - the transceiver configured to receive, on a wired interface from another node, a hello message, wherein the wireless network device and the another node are identified as island heads based on the received hello message and wherein the wired interface is utilized for communication between the island heads; and
 - the processor configured to identify immediate neighbor nodes, wherein immediate neighbor nodes having a least path cost are assigned to the wireless network device and wireless links between different island nodes are not configured.
2. The wireless network device of claim 1, wherein each identified immediate neighbor node is configured to assign neighboring nodes having another least path cost such that other wireless links between different nodes of an island are not configured.
3. The wireless network device of claim 1, wherein a wireless device in the network is configured to discover neighbors and island heads without another hello message.
4. The wireless network device of claim 1, wherein the broadcasted hello message is not forwarded.
5. The wireless network device of claim 1, wherein the announce message is forwarded.
6. The wireless network device of claim 1, wherein the processor is configured to determine, based on the broadcasted hello message, existence of a peer of another island, wherein the peer is blocked from wireless communication with the wireless network device.
7. The wireless network device of claim 1, wherein a peer is blocked from wireless communication with the wireless network device based on a hello count being above a limit or threshold.
8. The wireless network device of claim 1, wherein the wireless network device is configured to perform peer learning based on a source being a mesh node or the source not being another node's peer.

9. The wireless network device of claim 1, wherein the wireless network device is configured to recalculate a routing path, to validate a peer, and to update a routing table or a routing graph based on the announce message or the broadcasted hello message.

10. A method performed by a wireless network device, the method comprising:
receiving, by the wireless network device, a broadcasted hello message that indicates network topology and interface information of neighbor nodes in a network;

generating, by the wireless network device, an announce message that includes the network topology and interface information;

transmitting, by the wireless network device, the announce message to unblocked hello peers of the wireless network device;

receiving, by the wireless network device on a wired interface from another node, a hello message, wherein the wireless network device and the another node are identified as island heads based on the received hello message and wherein the wired interface is utilized for communication between the island heads; and

identifying, by the wireless network device, immediate neighbor nodes, wherein immediate neighbor nodes having a least path cost are assigned to the wireless network device and wireless links between different island nodes are not configured.

11. The method of claim 10, wherein each identified immediate neighbor node assigns neighboring nodes having another least path cost such that other wireless links between different nodes of an island are not configured.

12. The method of claim 10, wherein a wireless device in the network discovers neighbors and island heads without another hello message.

13. The method of claim 10, wherein the broadcasted hello message is not forwarded.

14. The method of claim 10, wherein the announce message is forwarded.

15. The method of claim 10, further comprising determining, by the wireless network device, based on the broadcasted hello message, existence of a peer of another island, wherein the peer is blocked from wireless communication with the wireless network device.

16. The method of claim 10, wherein a peer is blocked from wireless communication with the wireless network device based on a hello count being above a limit or threshold.

17. The method of claim 10, wherein the wireless network device performs peer learning based on a source being a mesh node or the source not being another node's peer.

18. The method of claim 10, wherein the wireless network device recalculates a routing path, validates a peer, and updates a routing table or a routing graph based on the announce message or the broadcasted hello message.

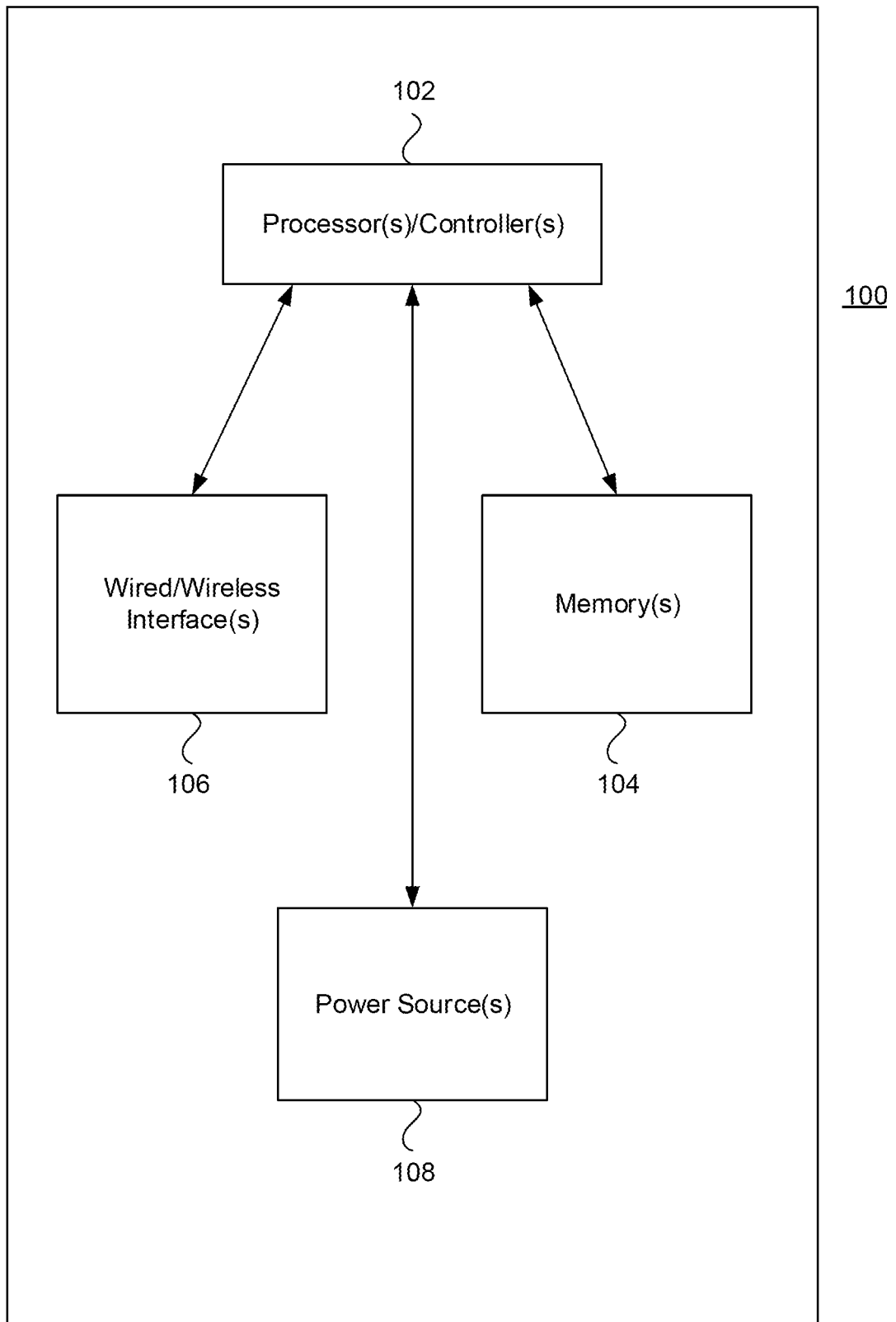


FIG. 1

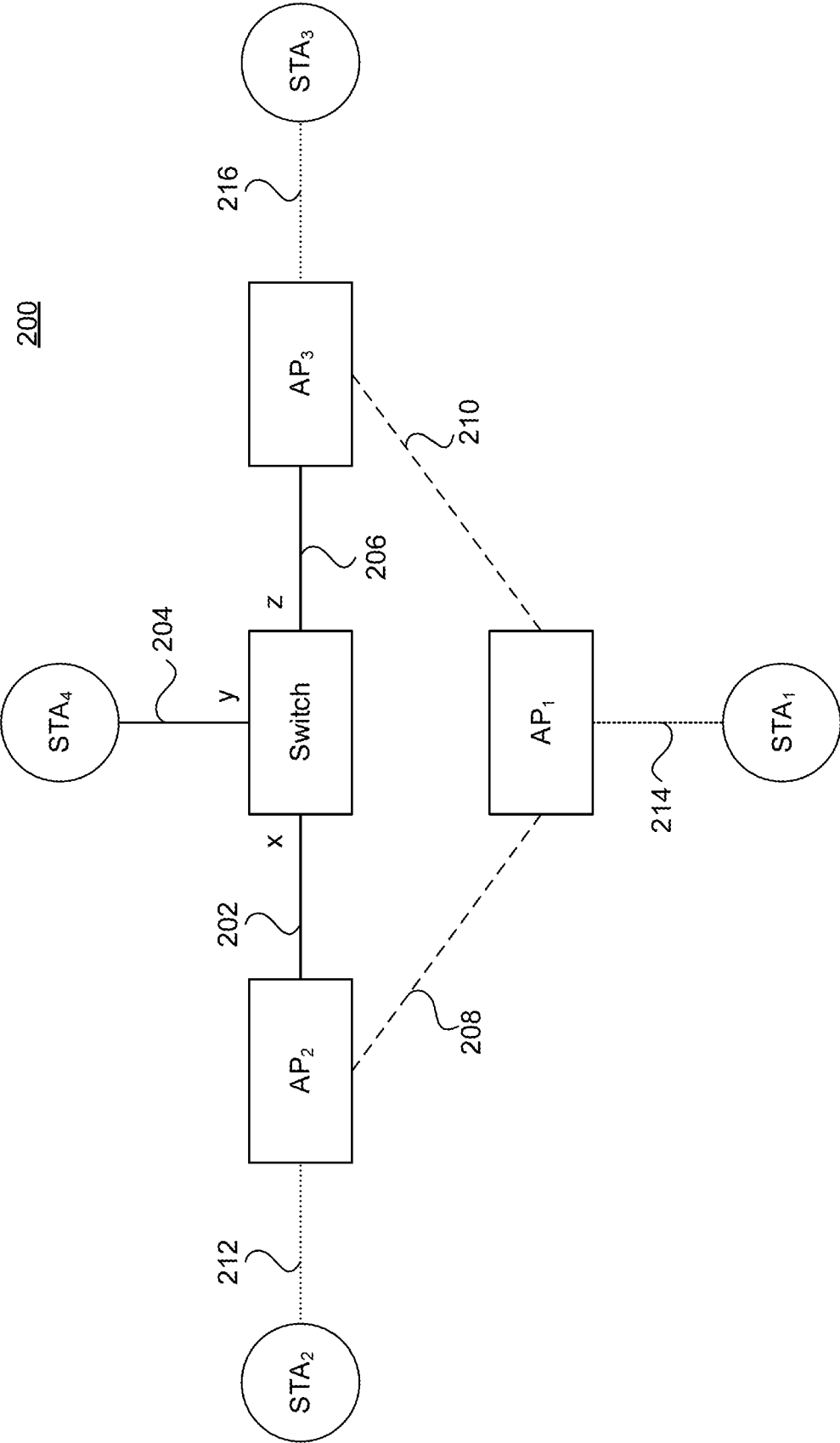


FIG. 2

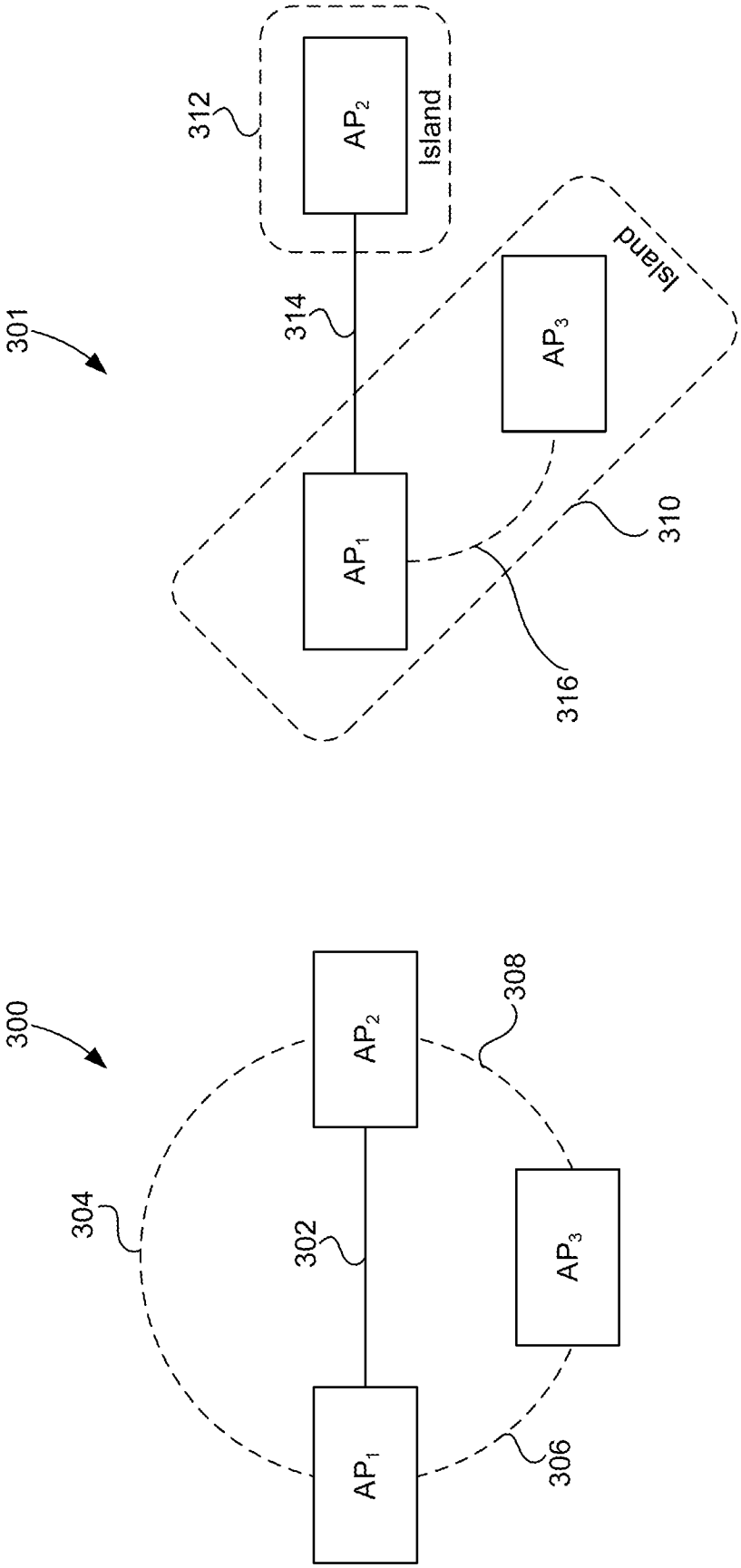
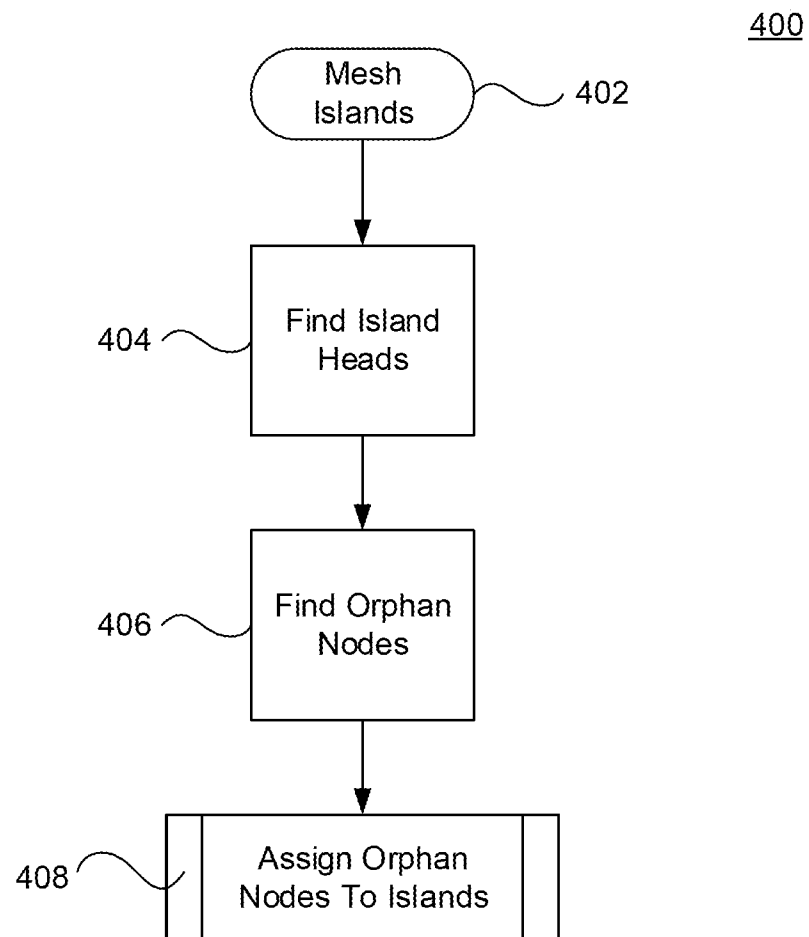
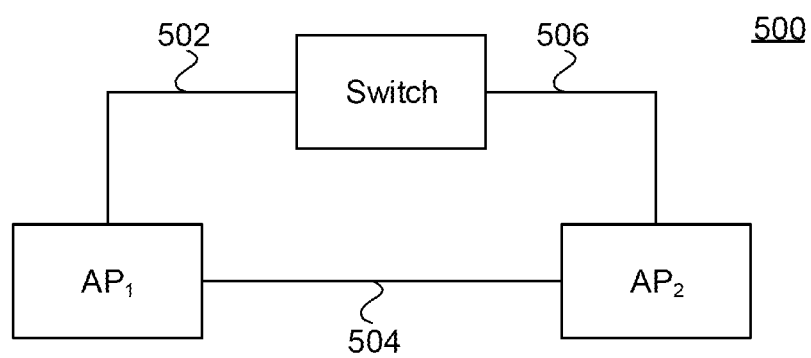


FIG. 3

**FIG. 4****FIG. 5**

600

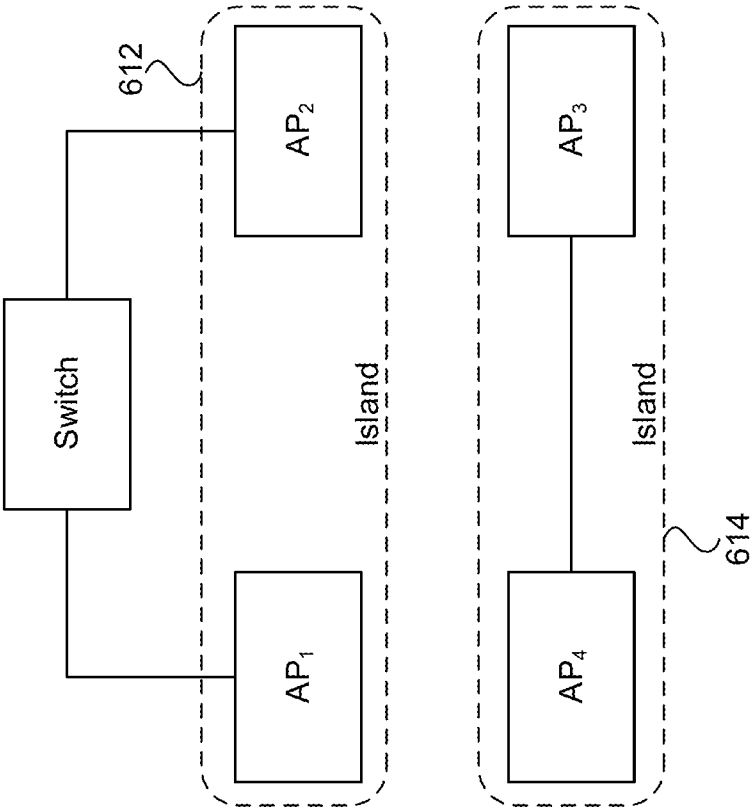
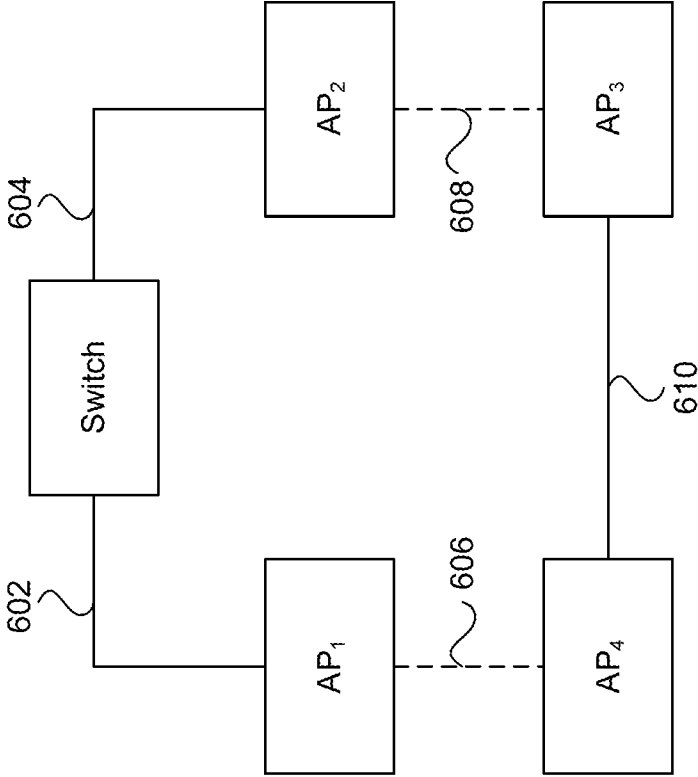


FIG. 6

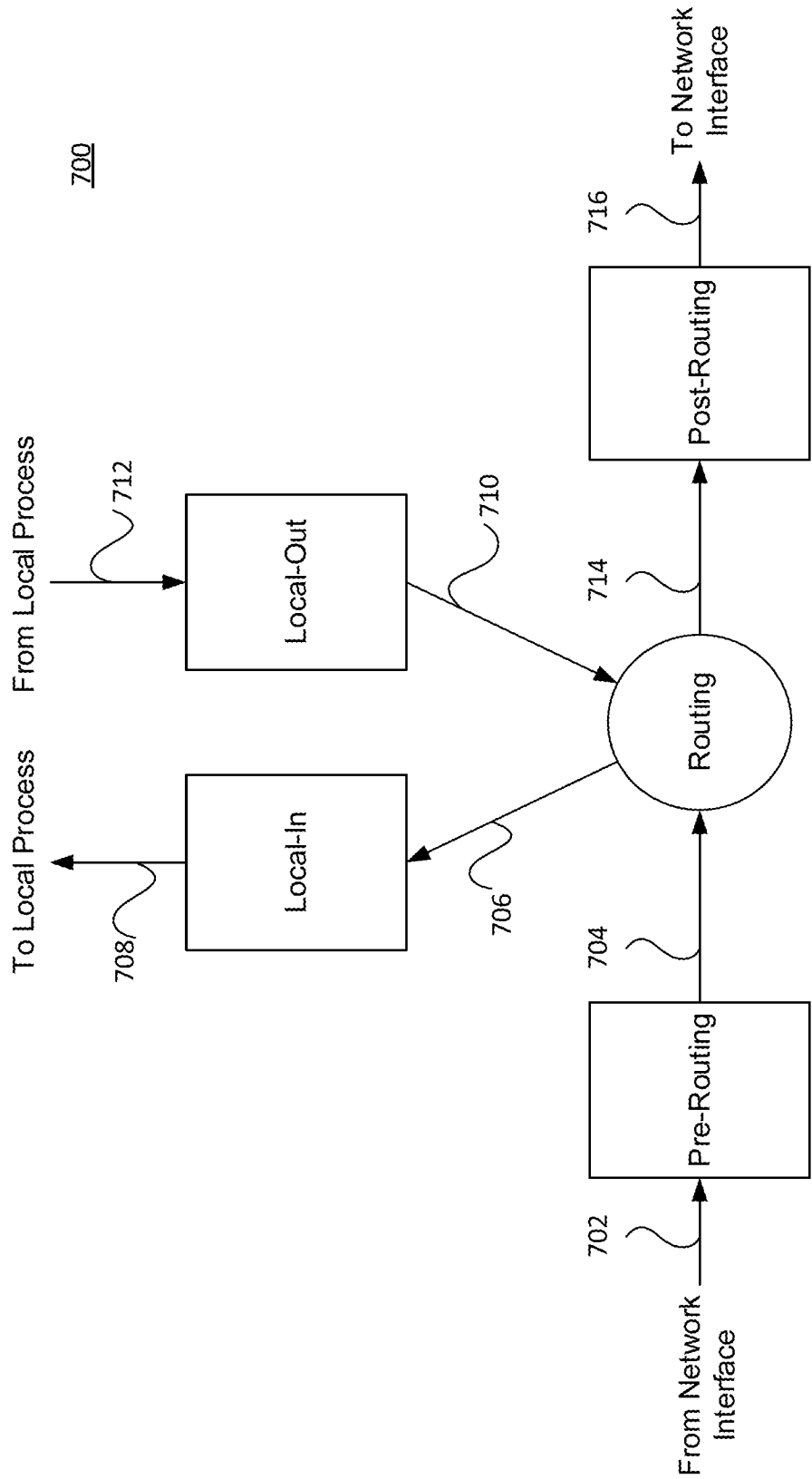


FIG. 7

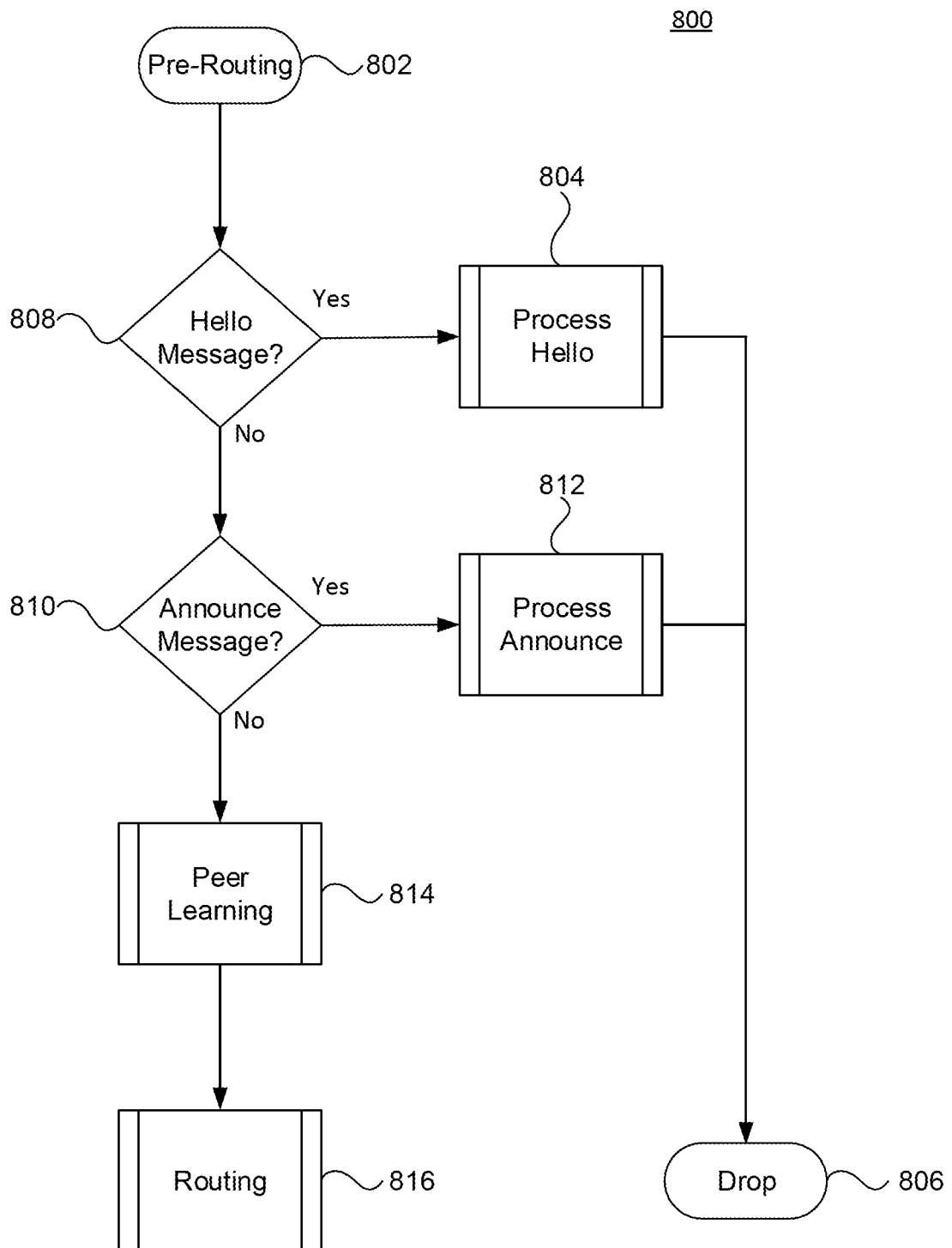


FIG. 8

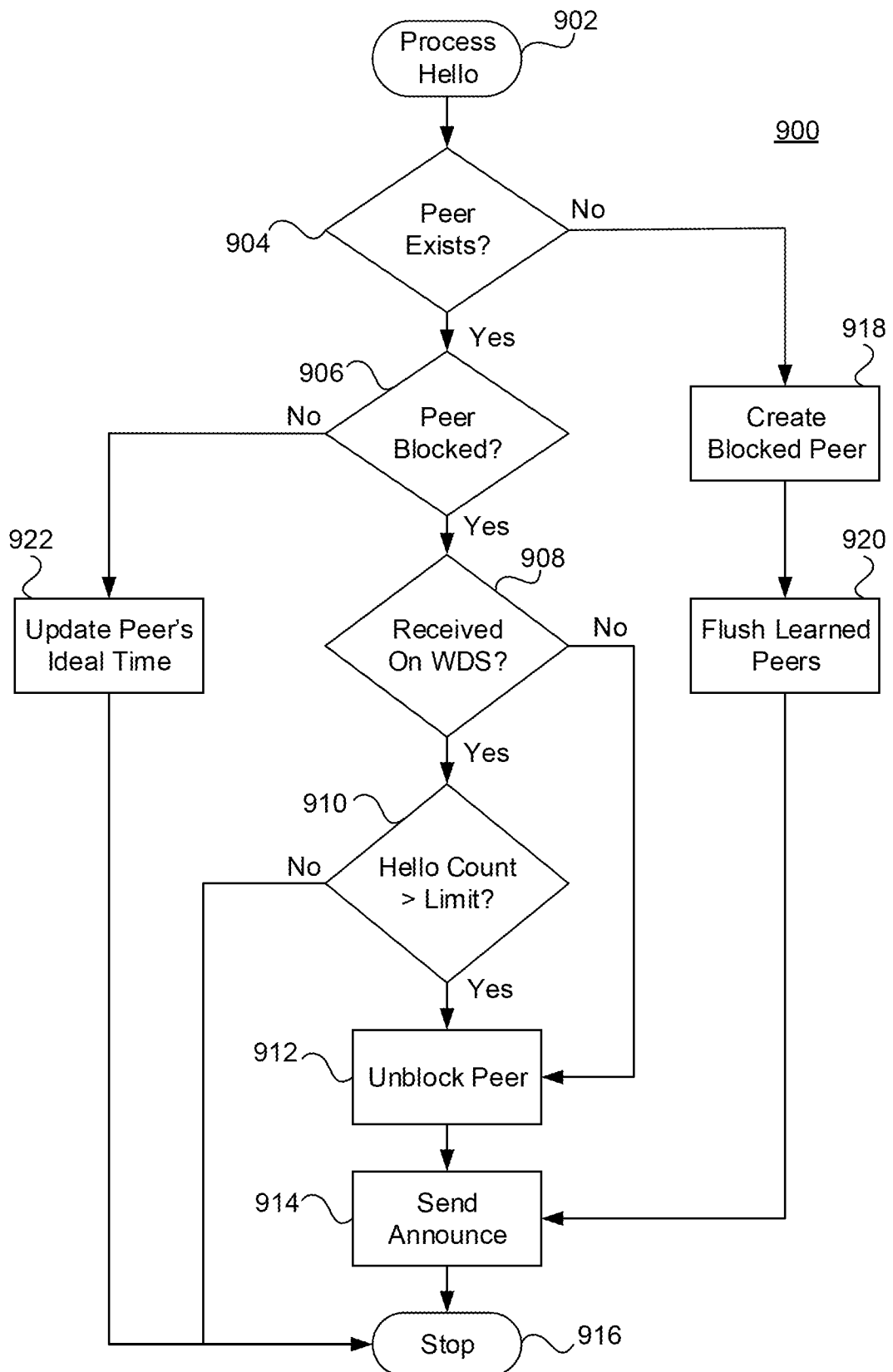
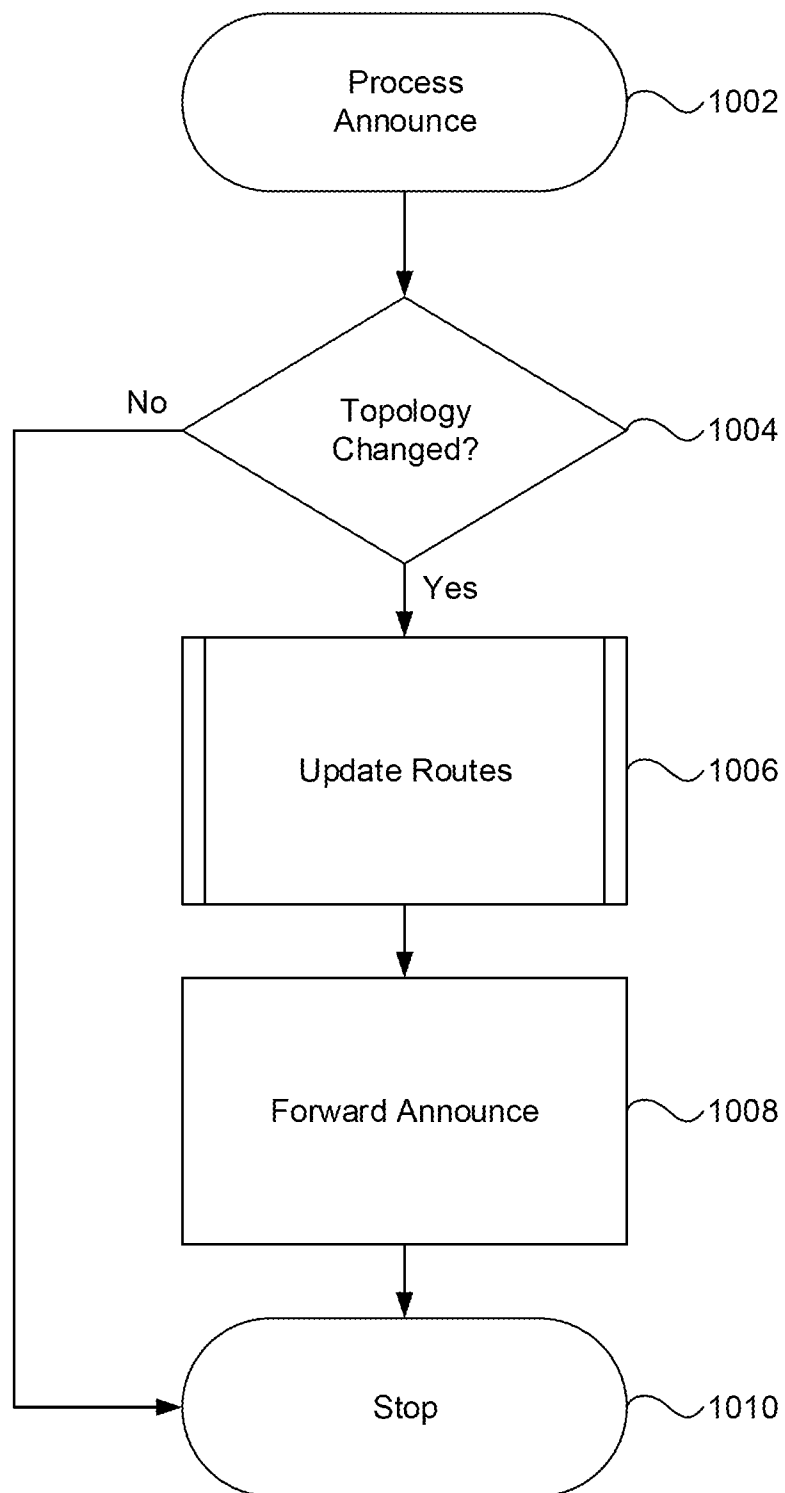


FIG. 9

1000**FIG. 10**

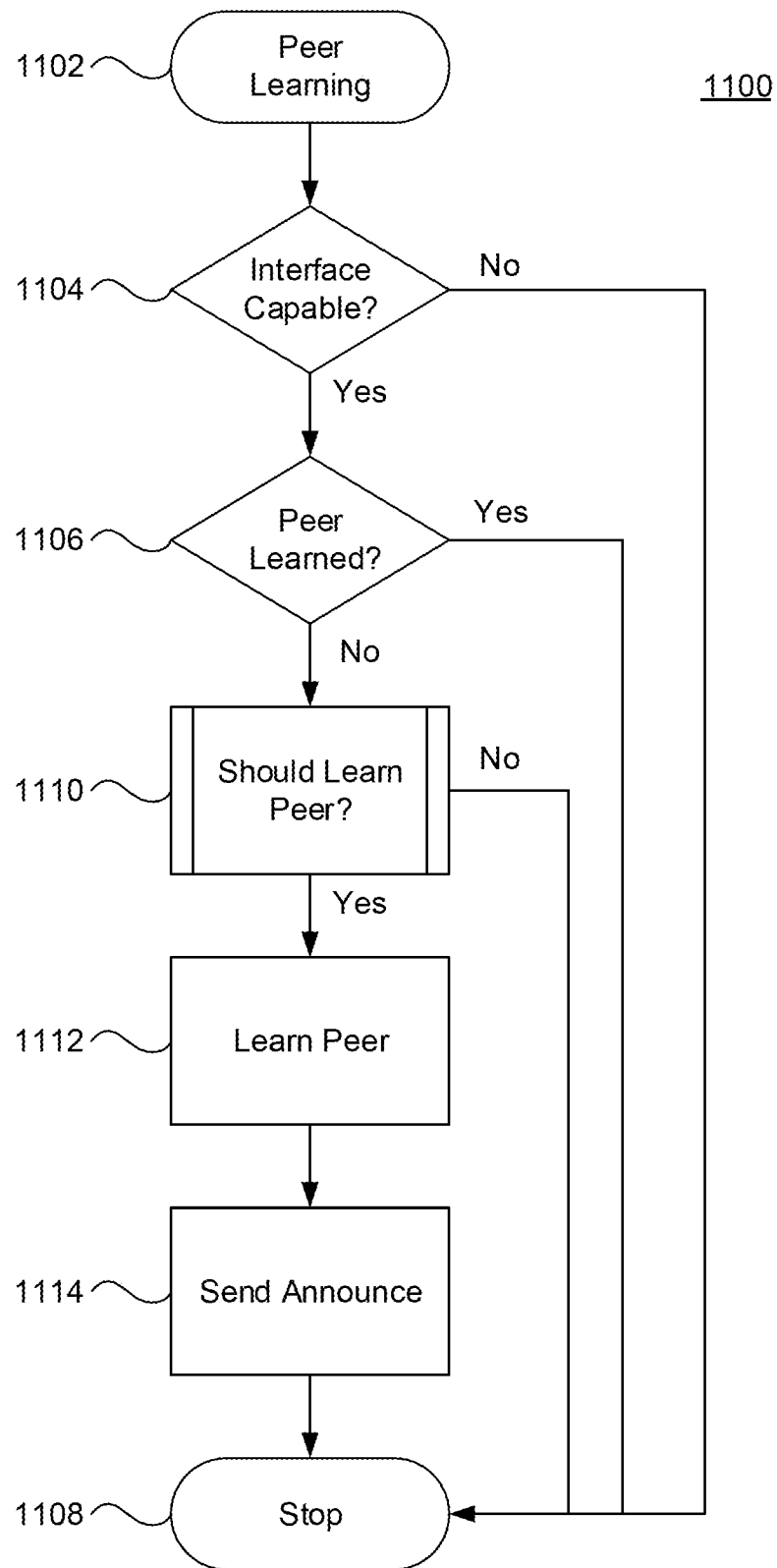


FIG. 11

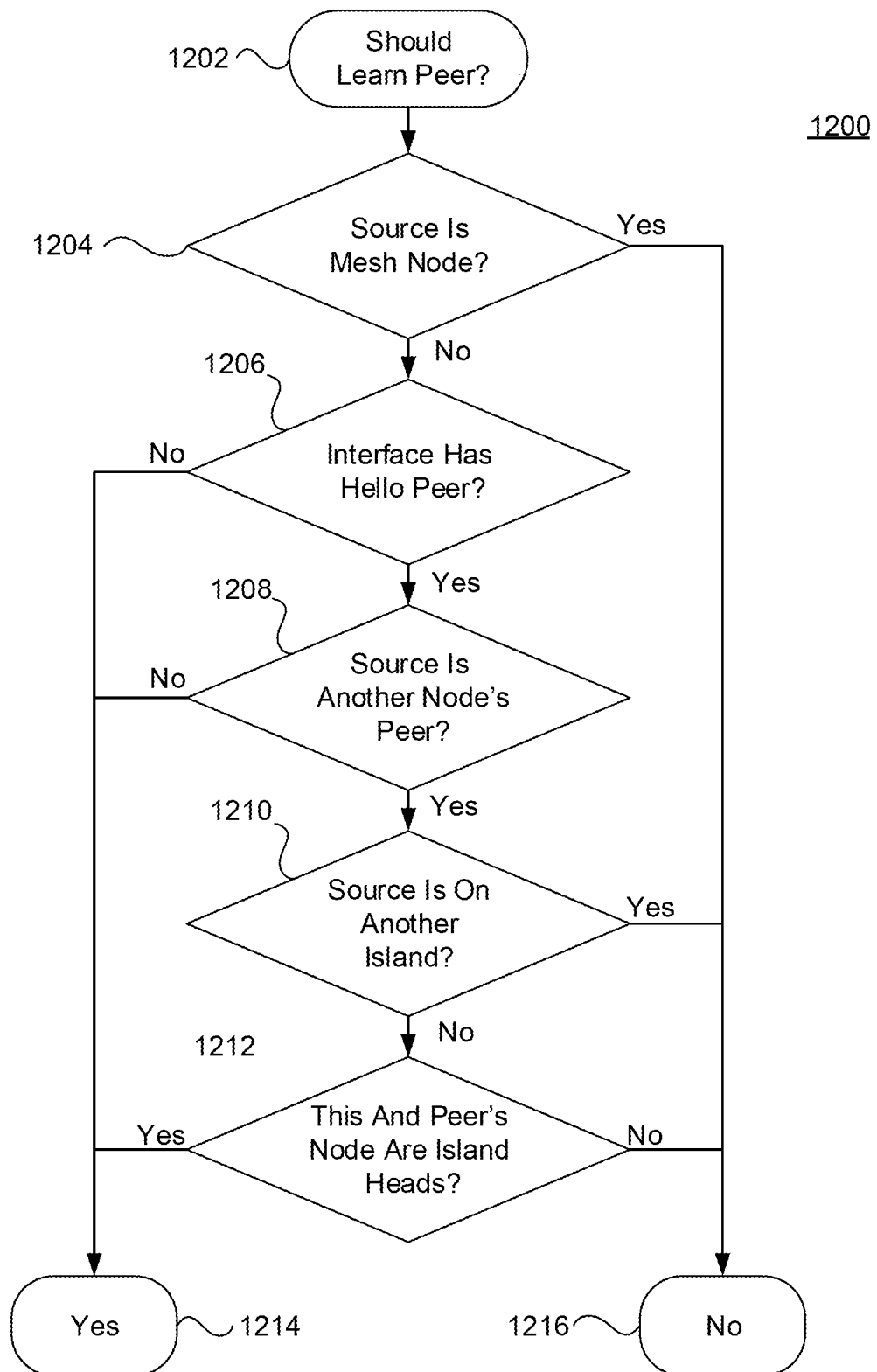
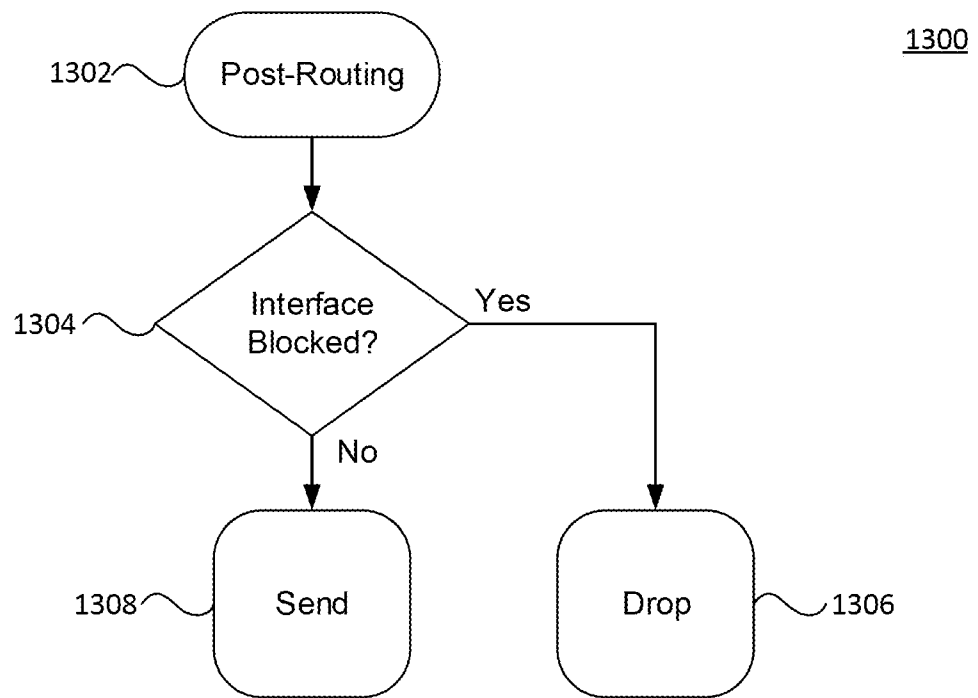
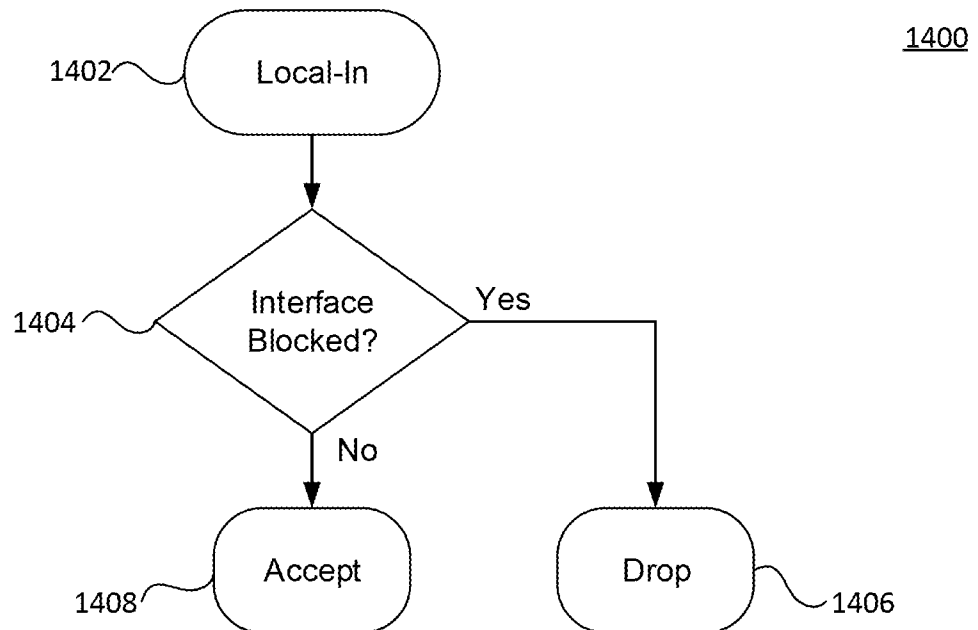


FIG. 12

**FIG. 13****FIG. 14**

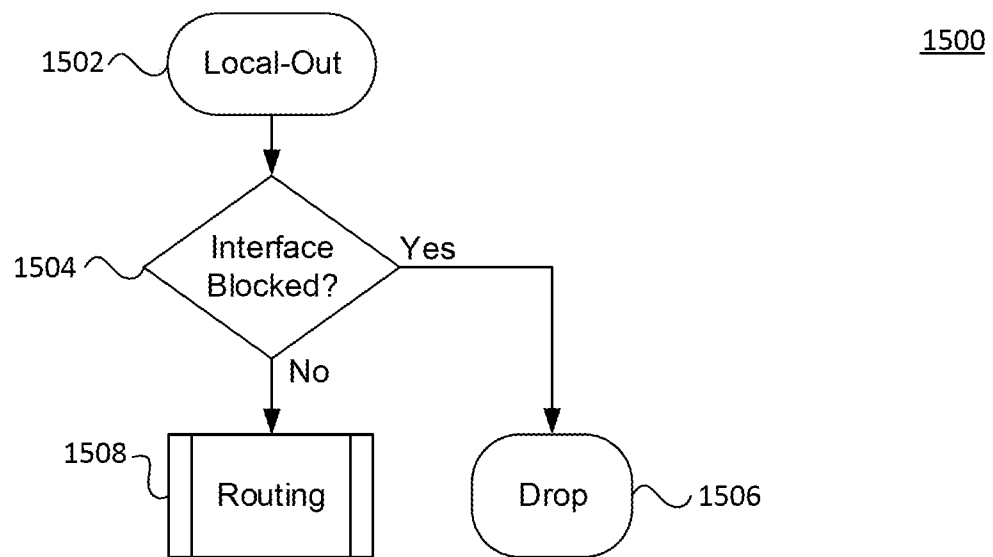


FIG. 15

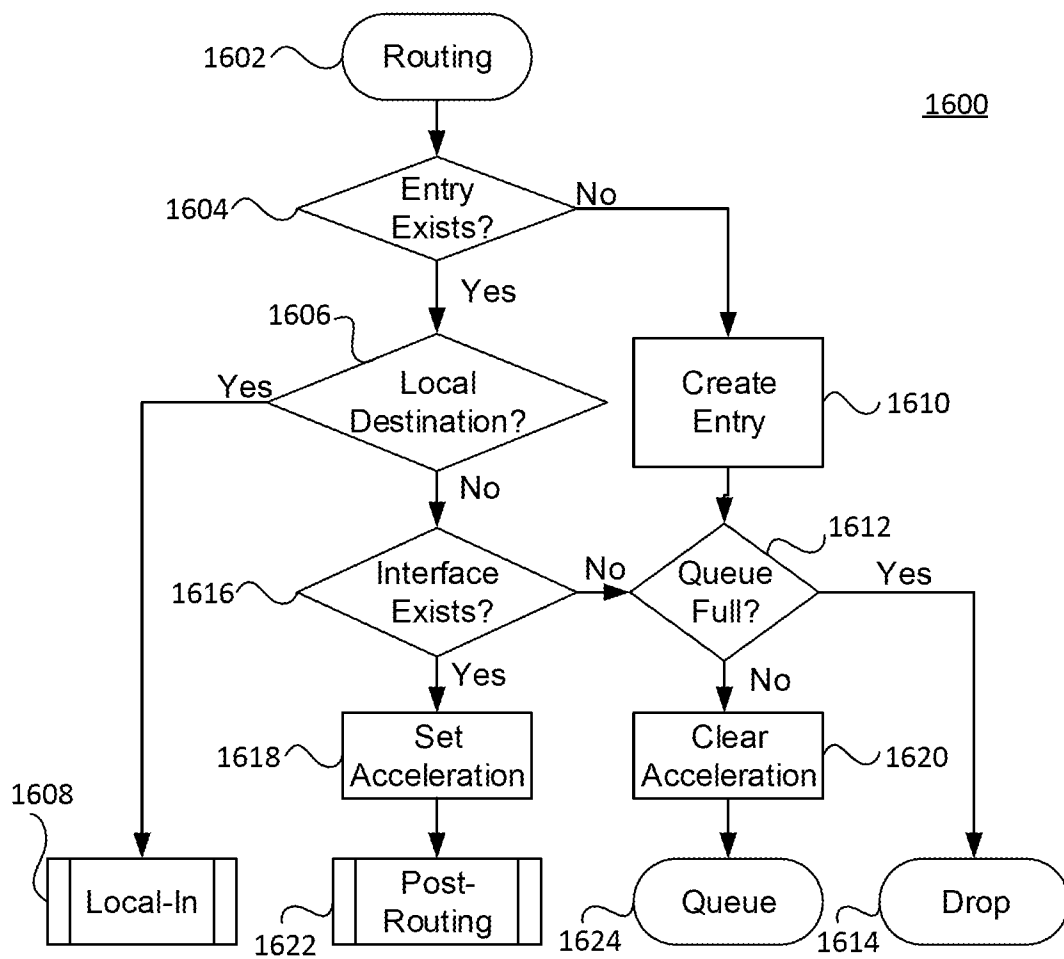


FIG. 16

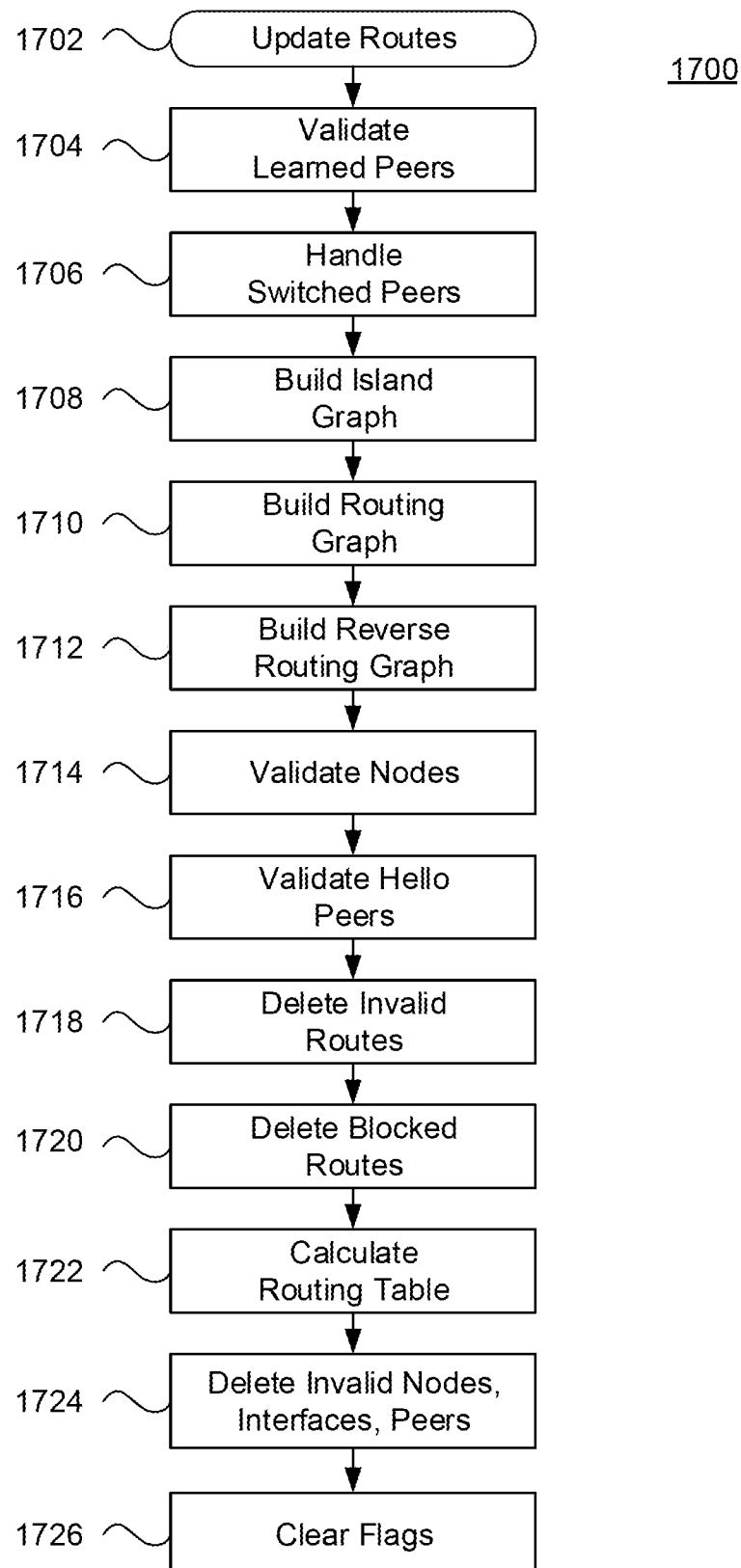


FIG. 17

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2018/000075

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W40/24
ADD. H04W84/18

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EP0-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	YAIR AMIR ET AL: "The SMesh wireless mesh network", ACM TRANSACTIONS ON COMPUTER SYSTEMS (TOCS), ASSOCIATION FOR COMPUTING MACHINERY, INC, US, vol. 28, no. 3, 30 September 2008 (2008-09-30), pages 1-49, XP058355434, ISSN: 0734-2071, DOI: 10.1145/1841313.1841314 chapter 4.1.1; page 10 - page 11 page 8; figure 1 chapter 4.1.2; page 11 chapter 4.1; page 9 ----- -/--	1-18



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

15 May 2018

Date of mailing of the international search report

23/05/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Bos, Jürgen

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2018/000075

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Azzedine Boukerche ET AL: "A Taxonomy of Routing Protocols for Mobile Ad Hoc Networks : Boukerche/Mobile" In: "Distributed Channel Access Scheduling for Ad Hoc Networks", 24 October 2008 (2008-10-24), Wiley, Hoboken, NJ, XP055474809, ISBN: 978-0-470-38358-2 pages 129-163, DOI: 10.1002/9780470396384.ch5, chapter 5.4.2; page 144 - page 145 page 145 - page 146 -----	1-18