(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
03 July 2025 (03.07.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/145196 A1

(51) International Patent Classification:
H04W 28/02 (2009.01) *H04W 84/12* (2009.01)
H04W 28/24 (2009.01) *H04L 47/2408* (2022.01)
H04W 76/14 (2018.01) *H04L 47/2441* (2022.01)
H04L 67/104 (2022.01)

(21) International Application Number:
PCT/US2024/062338

(22) International Filing Date:
30 December 2024 (30.12.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/616,560 30 December 2023 (30.12.2023) US
18/786,375 26 July 2024 (26.07.2024) US

(71) Applicant: **CISCO TECHNOLOGY, INC.** [US/US]; 170 West Tasman Drive, San Jose, California 95134-1706 (US).

(72) Inventors: **GUPTA, Binita**; 16208 Lone Way, San Diego, California 92127 (US). **SMITH, Malcolm M.**; 4601 Deer Valley Lane, Richardson, Texas 75082 (US). **HART, Brian D.**; 899 Lois Avenue, Sunnyvale, California 94087 (US).

(74) Agent: **STIER, D. Kent** et al.; Merchant & Gould P.C., P.O. BOX 2903, MINNEAPOLIS, Minnesota 55402-0903 (US).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

WO 2025/145196 A1

(54) Title: AUTHORIZATION FOR STREAM CLASSIFICATION SERVICE (SCS) REQUESTS FOR PEER-TO-PEER (P2P) TRAFFIC FLOWS

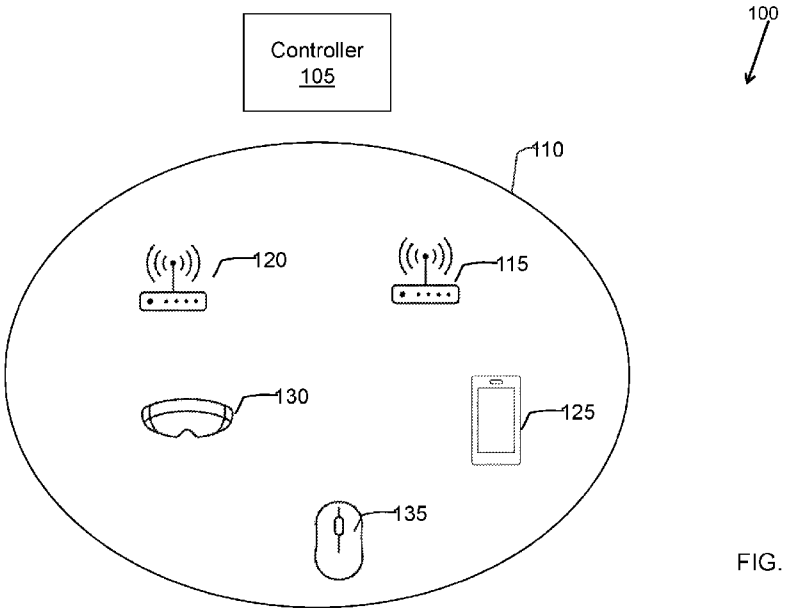

FIG. 1

(57) Abstract: Authorization for stream classification service requests for Peer-to-Peer (P2P) traffic flows may be provided. An Access Point (AP) may receive a Stream Classification Service (SCS) request from a station for a P2P traffic flow. The SCS request may include a flow identifier for the P2P traffic flow and Quality of Service (QoS) resource requested for the P2P traffic flow. The AP may determine whether to grant the SCS request. Determining whether to grant the SCS request may include determining that a network policy allows the P2P traffic flow based on the flow identifier and determining that the AP can support the QoS resource requested for the P2P traffic flow.

[Continued on next page]

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, 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))*

AUTHORIZATION FOR STREAM CLASSIFICATION SERVICE (SCS) REQUESTS FOR PEER-TO-PEER (P2P) TRAFFIC FLOWS

RELATED APPLICATION

[0001] This is being file as a PCT Application. Applicant claims the benefit of and priority to U.S. Provisional Application No. 63/616,560, filed December 30, 2023, and to U.S. Non-Provisional Application No. 18/786,375, filed July 26, 2024, which are incorporated herein by reference.

TECHNICAL FIELD

[0002] The present disclosure relates generally to authorization for stream classification service requests for peer-to-peer traffic flows.

BACKGROUND

[0003] In computer networking, a wireless Access Point (AP) is a networking hardware device that allows a Wi-Fi compatible client device to connect to a wired network and to other client devices. The AP usually connects to a router (directly or indirectly via a wired network) as a standalone device, but it can also be an integral component of the router itself. Several APs may also work in coordination, either through direct wired or wireless connections, or through a central system, commonly called a Wireless Local Area Network (WLAN) controller. An AP is differentiated from a hotspot, which is the physical location where Wi-Fi access to a WLAN is available.

[0004] Prior to wireless networks, setting up a computer network in a business, home, or school often required running many cables through walls and ceilings in order to deliver network access to all of the network-enabled devices in the

building. With the creation of the wireless AP, network users are able to add devices that access the network with few or no cables. An AP connects to a wired network, then provides radio frequency links for other radio devices to reach that wired network. Most APs support the connection of multiple wireless devices. APs are built to support a standard for sending and receiving data using these radio frequencies.

BRIEF DESCRIPTION OF THE FIGURES

[0005] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate various embodiments of the present disclosure. In the drawings:

[0006] FIG. 1 is a block diagram of an operating environment for authorization for stream classification service requests for peer-to-peer traffic flows;

[0007] FIG. 2 is a flow chart of a method for providing authorization for stream classification service requests for peer-to-peer traffic flows; and

[0008] FIG. 3 is a block diagram of a computing device.

DETAILED DESCRIPTION

OVERVIEW

[0009] Authorization for stream classification service requests for Peer-to-Peer (P2P) traffic flows may be provided. An Access Point (AP) may receive a Stream Classification Service (SCS) request from a station for a P2P traffic flow. The SCS request may include a flow identifier for the P2P traffic flow and Quality of Service (QoS) resource requested for the P2P traffic flow. The AP may determine whether to grant the SCS request. Determining whether to grant the SCS request may include determining

that a network policy allows the P2P traffic flow based on the flow identifier and determining that the AP can support the QoS resource requested for the P2P traffic flow.

[0010] Both the foregoing overview and the following example embodiments are examples and explanatory only and should not be considered to restrict the disclosure's scope, as described and claimed. Furthermore, features and/or variations may be provided in addition to those described. For example, embodiments of the disclosure may be directed to various feature combinations and sub-combinations described in the example embodiments.

EXAMPLE EMBODIMENTS

[0011] The following detailed description refers to the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the following description to refer to the same or similar elements. While embodiments of the disclosure may be described, modifications, adaptations, and other implementations are possible. For example, substitutions, additions, or modifications may be made to the elements illustrated in the drawings, and the methods described herein may be modified by substituting, reordering, or adding stages to the disclosed methods. Accordingly, the following detailed description does not limit the disclosure. Instead, the proper scope of the disclosure is defined by the appended claims.

[0012] Streaming traffic is among the largest and fastest growing traffic on the internet. Peer-to-Peer (P2P) streaming contributes substantially to this growth. P2P traffic is a decentralized network architecture that allows Stations (STAs) to interact directly with each other. When a STA sends a Stream Classification Service (SCS)

request with a Quality of Service (QoS) characteristics element to an Access Point (AP), the STA may provide Traffic Classification (TCLAS) information to identify a P2P traffic flow for that SCS request for Downlink (DL) flow. The QoS characteristics element may be used to indicate QoS resource requirements for the P2P traffic flow. However, for a P2P traffic flow, the Institute of Electrical and Electronics Engineers (IEEE) 802.11be amendment may not support sending the TCLAS information. In the absence of TCLAS information, an AP may not be able to identify a P2P traffic flow for which QoS resources are being requested.

[0013] P2P traffic may become more prevalent in enterprise deployments with Augmented Reality/Virtual Reality/Extended Reality (AR/VR/XR) applications on Head Mounted Devices (HMDs) being used for workplace productivity and collaboration. Therefore, it may become increasingly important for an AP to be able to identify P2P traffic flows for which QoS resources are being requested in a SCS request. The disclosure provides processes to enhance the SCS request to provide identification information for the P2P traffic flows. The disclosed enhancements to the SCS request may enable a STA to provide a flow identifier for the P2P traffic flow and QoS resources requested for the P2P traffic flow. The flow identifier may enable the AP to identify or distinguish the P2P traffic flows that are related to enterprise/workplace usage from other P2P traffic flows that are not related to the enterprise/business usage. The AP may use the flow identifier to apply a network policy to accept or reject the SCS request for the P2P traffic flows. For example, the AP may be configured with a network policy to accept SCS requests with the QoS characteristics for the P2P traffic

flows related to enterprise/workplace usage and reject SCS requests for the P2P traffic flows that are not related to the enterprise/business usage.

[0014] FIG. 1 shows an operating environment 100 for authorization for SCS requests for P2P traffic flows. As shown in FIG. 1, operating environment 100 may comprise a controller 105 and a coverage environment 110. Coverage environment 110 may comprise, but is not limited to, a Wireless Local Area Network (WLAN) comprising a plurality of APs that may provide wireless network access (e.g., access to the WLAN for client devices). The plurality of APs may comprise a first AP 115 and a second AP 120. The plurality of APs may provide wireless network access to a plurality of STAs as they move within coverage environment 110. The plurality of STAs may comprise, but are not limited to, a first STA 125, a second STA 130, and a third STA 135. Ones of the plurality of STAs may comprise, but are not limited to, a smart phone, a HMD, a mice, a keyboard, a personal computer, a tablet device, a mobile device, a telephone, a remote control device, a set-top box, a digital video recorder, an Internet-of-Things (IoT) device, a network computer, a router, AR/ VR/XR devices, or other similar microcomputer-based device. Each of the plurality of APs may be compatible with specification standards such as, but not limited to, the IEEE 802.11 specification standard for example.

[0015] The plurality of APs and the plurality of STAs may use Multi-Link Operation (MLO) where they simultaneously transmit and receive across different bands and channels by establishing two or more links to two or more AP radios. These bands may comprise, but are not limited the 2 GHz band, the 5 GHz band, the 6 GHz band, and the 60 GHz band.

[0016] Controller 105 may comprise a Wireless Local Area Network controller (WLC) and may provision and control coverage environment 110 (e.g., a WLAN). Controller 105 may allow first STA 125, second STA 130, and third STA 135 to join coverage environment 110. In some embodiments of the disclosure, controller 105 may be implemented by a Digital Network Architecture Center (DNAC) controller (i.e., a Software-Defined Network (SDN) controller) that may configure information for coverage environment 110 in order to provide authorization for SCS requests for P2P traffic flows.

[0017] The elements described above of operating environment 100 (e.g., controller 105, first AP 115, second AP 120, first STA 125, second STA 130, or third STA 135) may be practiced in hardware and/or in software (including firmware, resident software, micro-code, etc.) or in any other circuits or systems. The elements of operating environment 100 may be practiced in electrical circuits comprising discrete electronic elements, packaged or integrated electronic chips containing logic gates, a circuit utilizing a microprocessor, or on a single chip containing electronic elements or microprocessors. Furthermore, the elements of operating environment 100 may also be practiced using other technologies capable of performing logical operations such as, for example, AND, OR, and NOT, including but not limited to, mechanical, optical, fluidic, and quantum technologies. As described in greater detail below with respect to FIG. 3, the elements of operating environment 100 may be practiced in a computing device 300.

[0018] FIG. 2 is a flow chart setting forth the general stages involved in a method 200 consistent with embodiments of the disclosure for authorization for SCS

requests for P2P traffic flows. Method 200 may be implemented using first AP 115 and first STA 125 as described in more detail above with respect to FIG. 1. Ways to implement the stages of method 200 will be described in greater detail below.

[0019] Method 200 may begin at starting block 205 and proceed to stage 210 where first AP 115 may receive a SCS request from first STA 125 for a P2P traffic flow. The SCS request may comprise a flow identifier for the P2P traffic flow and QoS resources requested for the P2P flow. For example, first AP 115 may receive a SCS request from first STA 125 for a P2P traffic flow between first STA 125 and second STA 130 over a P2P link established between first STA 125 and second STA 130.

[0020] In one implementation, the flow identifier may include, but limited to, a TCLAS element for the P2P traffic flow. The TCLAS element may include Internet Protocol (IP) tuple information or a Fully Qualified Domain Name (FQDN) information for the P2P traffic flow for which the QoS resources are being requested. In another implementation, the flow identifier may include device identifiers of peer STAs involved in the P2P traffic flow. The device identifiers may include Media Access Control (MAC) addresses of the peer STAs, that is, a MAC addresses for each of first STA 125 and second STA 130. In yet another implementation, the flow identifier may include a category and type of the P2P traffic flow. The category and type may include, for example, an AR/VR flow, a non-Wireless Fidelity (non-WiFi) P2P flow, etc.. The non-WiFi flow may include a Bluetooth P2P traffic flow. In some implementation, the flow identifier may include an application name or an application identifier for an application that may be generating the P2P traffic flow. In some other implementations, the flow

identifier may include a Mobile Device Management (MDM) key for one or both of first STA 125 and second STA 130.

[0021] In some example SCS requests, first STA 125 may include a plurality of flow identifiers TCLAS elements. For example, if first STA 125 is combining QoS resources request for a plurality of P2P traffic flows in a single SCS request, such SCS request may include a plurality of flow identifiers (for example, TCLAS elements) for the multiple P2P traffic flows. First STA 125 may include a P2P Information Element (IE) in a SCS Descriptor Element of the SCS Request for the P2P traffic flow. The P2P IE may include TCLAS information, MAC addresses and MLD MAC addresses for a MLD STA for identification of P2P peers, and a category/type of the P2P traffic flow. In some examples, first STA 125 may be a group leader for multiple STAs and may send a SCS request on behalf of the group or on behalf of a member of the group.

[0022] Once having received the SCS request from first STA 125 for a P2P traffic flow at stage 210, method 200 may proceed to stage 220 where first AP 115 may determine whether to grant the SCS request. Determining whether to grant the SCS request may include determining that a network policy allows the P2P traffic flow based on the flow identifier and determining that first AP 115 can support the QoS resources requested for the P2P traffic flow.

[0023] First AP 115 upon receiving the SCS request for the P2P traffic flow, may use the flow identifier (for example, the TCLAS element) to identify the P2P traffic flow for which the SCS request is being made. In addition, first AP 115 may use the TCLAS element to verify a network policy configured for the P2P traffic flows. First AP 115 may have one or more network policies associated with P2P traffic flows stored

thereupon. The network policies may be configured for one or more of IP tuple, FQDN flow, MAC addresses, application identifiers, traffic type, device type, etc. or high-level P2P policy. Based on policy verification, first AP 115 may determine whether to authorize or accept the SCS request or reject the request for the P2P traffic flow.

[0024] In another implementation, first AP 115 may use fields from the P2P IE (for example, peer MAC addresses, peer MLD MAC addresses, flow category/type, application identifiers, MDM key,) by itself or along with the TCLAS information to verify the network policy to determine whether to authorize or accept or reject the SCS request for the P2P traffic flow. For example, first AP 115 may have a network policy that allows accepting a SCS request only for a P2P traffic flow between certain P2P peer MAC addresses and/or for certain category of flows (for example, AR/VR flows with known tethered devices).

[0025] First AP 115 may also use one or more of the TCLAS information, P2P IE, and QoS characteristics to authorize the QoS resource request for the P2P traffic flow. For example, first AP 115 may authorize an SCS request if the QoS resource requested is within a predetermined threshold. In one example, first AP 115 may authorize a SCS request when the QoS resource request (for example, a medium time) is below an AP defined threshold value for the P2P traffic flow. Similarly, first AP 115 may authorize a SCS request for an unrecognized TCLAS element between specific P2P peers identified based on MAC addresses, if the QoS resource requested is below a predetermined threshold (that is, a medium time requested is below another AP defined threshold value the P2P traffic flow).

[0026] Thus, first AP 115 may authorize the SCS request when both the network policy allows the P2P traffic flow and the QoS resource requested is within a predetermined threshold. If P2P traffic flow is not allowed by the network policy, then first AP 115 may not authorize the SCS request without even when or without determining whether the QoS resource requested is within a predetermined threshold. Similarly, if the QoS resource requested in the SCS request is not within a predetermined threshold, first AP 115 may not authorize the SCS request even when or without determining whether the P2P traffic flow is allowed by the network policy.

[0027] First AP 115 may send a SCS response to first STA 125 for the SCS request. The SCS response may notify first STA 125 whether the SCS request for the P2P traffic flow is authorized or not authorized. If the SCS response indicates that the SCS request was not authorized or rejected for the P2P traffic flow, the SCS response may include a reason for denial or rejection. The SCS response may further include a reason code or a status code. In an example, if the SCS request was rejected because the flow identifier (for example, a TCLAS element) associated with the SCS request is not authorized in the network policy, the SCS response for the SCS request may include the following code: SCS_REJECTED_P2P_TCLAS_NOT_AUTHORISED. In above example, the SCS response may include one or more suggested flow identifiers (that is, TCLAS elements) for P2P traffic flows that are allowed as per the network policy.

[0028] If first STA 125 included multiple P2P TCLAS elements in the SCS request, first AP 115 may authorize a subset of those P2P TCLAS traffic flows. In this example, first AP 115 may send a SCS response to first STA 125 with a status code

indicating a reason for accepting a subset and rejecting the remaining P2P traffic flows and suggested one or more TCLAS elements for P2P traffic flows that are allowed as per the network policy. The status code for the above example may include: SCS_REJECTED_NOT_ALL_P2P_TCLAS_AUTHORISED_SUGGESTED_P2P_TCLAS_INCLUDED. First STA 125 may then send another SCS request with QoS resource request for one or more authorized TCLAS elements.

[0029] If the network policy only supports authorizing P2P traffic flows from specific peer STAs and the SCS request for the P2P traffic flow from first STA 125 indicates peer addresses that are not authorized per network policy, then first AP 115 may reject the SCS request. In this example, the SCS response to first STA 125 may include the following status code indicating the reason: SCS_REJECTED_P2P_PEERS_NOT_ALLOWED_PER_POLICY. First AP 115 may, in the SCS response, include a P2P IE indicating peer MAC addresses and/or P2P traffic flow categories/types that are allowed for P2P resource request as per the network policy.

[0030] If the network policy only supports authorizing P2P traffic flows from certain applications the SCS request for the P2P traffic flow from first STA 125 indicates application identifiers that are not authorized per network policy, then first AP 115 may reject the SCS request. In this example, the SCS response to first STA 125 may include the following status code indicating the reason: SCS_REJECTED_APPLICATION_NOT_ALLOWED_PER_POLICY. First AP 115 may, in the SCS response, include one or more application identifiers that are allowed for

P2P resource request as per the network policy. Once first AP 115 determines whether to grant the SCS request at stage 220, method 200 may then end at stage 230.

[0031] FIG. 3 shows computing device 300. As shown in FIG. 3, computing device 300 may include a processing unit 310 and a memory unit 315. Memory unit 315 may include a software module 320 and a database 325. While executing on processing unit 310, software module 320 may perform, for example, processes for authorization for a SCS request for a P2P traffic flow as described above with respect to FIG. 2. Computing device 300, for example, may provide an operating environment for controller 105, first AP 115, second AP 120, first STA 125, second STA 130, or third STA 135. Controller 105, first AP 115, second AP 120, first STA 125, second STA 130, or third STA 135 may operate in other environments and are not limited to computing device 300.

[0032] Computing device 300 may be implemented using a Wi-Fi access point, a tablet device, a mobile device, a smart phone, a telephone, a remote control device, a set-top box, a digital video recorder, a cable modem, a personal computer, a network computer, a mainframe, a router, a switch, a server cluster, a smart TV-like device, a network storage device, a network relay device, or other similar microcomputer-based device. Computing device 300 may comprise any computer operating environment, such as hand-held devices, multiprocessor systems, microprocessor-based or programmable sender electronic devices, minicomputers, mainframe computers, and the like. Computing device 300 may also be practiced in distributed computing environments where tasks are performed by remote processing

devices. The aforementioned systems and devices are examples, and computing device 300 may comprise other systems or devices.

[0033] Embodiments of the disclosure, for example, may be implemented as a computer process (method), a computing system, or as an article of manufacture, such as a computer program product or computer readable media. The computer program product may be a computer storage media readable by a computer system and encoding a computer program of instructions for executing a computer process. The computer program product may also be a propagated signal on a carrier readable by a computing system and encoding a computer program of instructions for executing a computer process. Accordingly, the present disclosure may be embodied in hardware and/or in software (including firmware, resident software, micro-code, etc.). In other words, embodiments of the present disclosure may take the form of a computer program product on a computer-usable or computer-readable storage medium having computer-usable or computer-readable program code embodied in the medium for use by or in connection with an instruction execution system. A computer-usable or computer-readable medium may be any medium that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device.

[0034] The computer-usable or computer-readable medium may be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific computer-readable medium examples (a non-exhaustive list), the computer-readable medium may include the following: an electrical connection having one or more wires, a

portable computer diskette, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, and a portable compact disc read-only memory (CD-ROM). Note that the computer-usable or computer-readable medium could even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via, for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory.

[0035] While certain embodiments of the disclosure have been described, other embodiments may exist. Furthermore, although embodiments of the present disclosure have been described as being associated with data stored in memory and other storage mediums, data can also be stored on or read from other types of computer-readable media, such as secondary storage devices, like hard disks, floppy disks, or a CD-ROM, a carrier wave from the Internet, or other forms of RAM or ROM. Further, the disclosed methods' stages may be modified in any manner, including by reordering stages and/or inserting or deleting stages, without departing from the disclosure.

[0036] Furthermore, embodiments of the disclosure may be practiced in an electrical circuit comprising discrete electronic elements, packaged or integrated electronic chips containing logic gates, a circuit utilizing a microprocessor, or on a single chip containing electronic elements or microprocessors. Embodiments of the disclosure may also be practiced using other technologies capable of performing logical operations such as, for example, AND, OR, and NOT, including but not limited to, mechanical,

optical, fluidic, and quantum technologies. In addition, embodiments of the disclosure may be practiced within a general purpose computer or in any other circuits or systems.

[0037] Embodiments of the disclosure may be practiced via a system-on-a-chip (SOC) where each or many of the element illustrated in FIG. 1 may be integrated onto a single integrated circuit. Such an SOC device may include one or more processing units, graphics units, communications units, system virtualization units and various application functionality all of which may be integrated (or "burned") onto the chip substrate as a single integrated circuit. When operating via an SOC, the functionality described herein with respect to embodiments of the disclosure, may be performed via application-specific logic integrated with other components of computing device 300 on the single integrated circuit (chip).

[0038] Embodiments of the present disclosure, for example, are described above with reference to block diagrams and/or operational illustrations of methods, systems, and computer program products according to embodiments of the disclosure. The functions/acts noted in the blocks may occur out of the order as shown in any flowchart. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved.

[0039] While the specification includes examples, the disclosure's scope is indicated by the following claims. Furthermore, while the specification has been described in language specific to structural features and/or methodological acts, the claims are not limited to the features or acts described above. Rather, the specific

features and acts described above are disclosed as example for embodiments of the disclosure.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by an Access Point (AP), a Stream Classification Service (SCS) request from a station for a peer-to-peer traffic flow, the SCS request comprising a flow identifier for the peer-to-peer traffic flow and Quality of Service (QoS) resource requested for the peer-to-peer traffic flow; and

determining, by the AP, whether to grant the SCS request, wherein determining whether to grant the SCS request comprises:

determining that a network policy allows the peer-to-peer traffic flow based on the flow identifier, and

determining that the AP can support the QoS resource requested for the peer-to-peer traffic flow.

2. The method of claim 1, wherein the flow identifier comprises one or more of: a traffic classifier of the peer-to-peer traffic flow, a device identifier for each peers of the peer-to-peer traffic flow, a category of the peer-to-peer traffic flow, a type of the peer-to-peer traffic flow, an application identifier of an application associated with the peer-to-peer traffic flow.

3. The method of claim 1 or 2, wherein determining that the network policy allows the peer-to-peer traffic flow based on the flow identifier comprises:

determining the network policy associated with the flow identifier, and

verifying that the network policy associated with the flow identifier allows the peer-to-peer traffic flow.

4. The method of any preceding claim, wherein determining that the AP can support the QoS resource requested for the peer-to-peer traffic flow comprises determining that the QoS resource requested for the peer-to-peer traffic flow is below a predetermined threshold.

5. The method of any preceding claim, wherein determining whether to grant the SCS request comprises:

rejecting the SCS request in response to determining that the network policy does not allows the peer-to-peer traffic flow based on the flow identifier; and

providing a SCS response to the station, the SCS response comprising a reason code for rejection of the SCS request.

6. The method of any preceding claim, further comprising:

providing a suggested flow identifier that is allowed by the network policy for the peer-to-peer traffic flow.

7. The method of claim 6, further comprising:

receiving another SCS request from the station, the another SCS request comprising the suggested flow identifier.

8. The method of any preceding claim, wherein receiving the SCS request comprises receiving the SCS request comprising a plurality of flow identifiers corresponding to a plurality of peer-to-peer traffic flow, and wherein determining whether to grant the SCS request comprises:

determining to grant a subset of peer-to-peer traffic flows of the plurality of peer-to-peer traffic flows; and

determining to reject a remaining peer-to-peer traffic flows of the plurality of peer-to-peer traffic flows.

9. A system comprising:

a memory storage; and

a processing unit disposed in a first computing device and coupled to the memory storage, wherein the processing unit is operative to:

receive a Stream Classification Service (SCS) request from a station for a peer-to-peer traffic flow, the SCS request comprising a flow identifier for the peer-to-peer traffic flow and Quality of Service (QoS) resource requested for the peer-to-peer traffic flow; and

determine whether to grant the SCS request, wherein the processing unit being operative to determine whether to grant the SCS request comprises the processing unit being operative to:

determine that a network policy allows the peer-to-peer traffic flow based on the flow identifier, and

determine that an Access Point (AP) can support the QoS resource requested for the peer-to-peer traffic flow.

10. The system of claim 9, wherein the flow identifier comprises one or more of: a traffic classifier of the peer-to-peer traffic flow, a device identifier for each peers of the peer-to-peer traffic flow, a category of the peer-to-peer traffic flow, a type of the peer-to-peer traffic flow, an application identifier of an application associated with the peer-to-peer traffic flow.

11. The system of claim 10, wherein the device identifier comprises a media access control address or a mobile device management key.

12. The system of any of claims 9 to 11, wherein the SCS request comprises a plurality of flow identifiers corresponding to a plurality of peer-to-peer traffic flow, and wherein the processing unit being operative to determine whether to grant the SCS request comprises the processing unit being operative to:

determine to grant a subset of peer-to-peer traffic flows of the plurality of peer-to-peer traffic flows; and

determine to reject a remaining peer-to-peer traffic flows of the plurality of peer-to-peer traffic flows.

13. The system of claim 12, wherein the processing unit is further operative to:

provide a reason code for rejected peer-to-peer traffic flows of the plurality of peer-to-peer traffic flows.

14. The system of claim 13, wherein the processing unit is further operative to:

provide a suggested flow identifier that is allowed by the network policy for the peer-to-peer traffic flow.

15. The system of claim 14, wherein the processing unit is further operative to:

receive another SCS request from the station, the another SCS request comprising the suggested flow identifier.

16. The system of claim 14 or 15, wherein the processing unit being operative to determine that the network policy allows the peer-to-peer traffic flow based on the flow identifier comprises the processing unit being operative to:

determine the network policy associated with the flow identifier, and

verify that the network policy associated with the flow identifier allows the peer-to-peer traffic flow.

17. A non-transitory computer-readable medium that stores a set of instructions which when executed perform a method executed by the set of instructions comprising:

receiving, by an Access Point (AP), a Stream Classification Service (SCS) request from a station for a peer-to-peer traffic flow, the SCS request comprising a flow identifier for the peer-to-peer traffic flow and Quality of Service (QoS) resource requested for the peer-to-peer traffic flow; and

determining, by the AP, whether to grant the SCS request, wherein determining whether to grant the SCS request comprises:

determining that a network policy allows the peer-to-peer traffic flow based on the flow identifier, and

determining that the AP can support the QoS resource requested for the peer-to-peer traffic flow.

18. The non-transitory computer-readable medium of claim 17, wherein determining that the network policy allows the peer-to-peer traffic flow based on the flow identifier comprises:

determining the network policy associated with the flow identifier, and

verifying that the network policy associated with the flow identifier allows the peer-to-peer traffic flow.

19. The non-transitory computer-readable medium of claim 17 or 18, wherein receiving the SCS request comprises receiving the SCS request comprising a plurality of flow identifiers corresponding to a plurality of peer-to-peer traffic flow, and wherein determining whether to grant the SCS request comprises:

determining to grant a subset of peer-to-peer traffic flows of the plurality of peer-to-peer traffic flows; and

determining to reject a remaining peer-to-peer traffic flows of the plurality of peer-to-peer traffic flows.

20. The non-transitory computer-readable medium of any of claims 17 to 19, wherein determining whether to grant the SCS request comprises:

rejecting the SCS request in response to determining that the network policy does not allows the peer-to-peer traffic flow based on the flow identifier;

providing a SCS response to the station, the SCS response comprising a reason code for rejection of the SCS request; and

providing a suggested flow identifier that is allowed by the network policy for the peer-to-peer traffic flow.

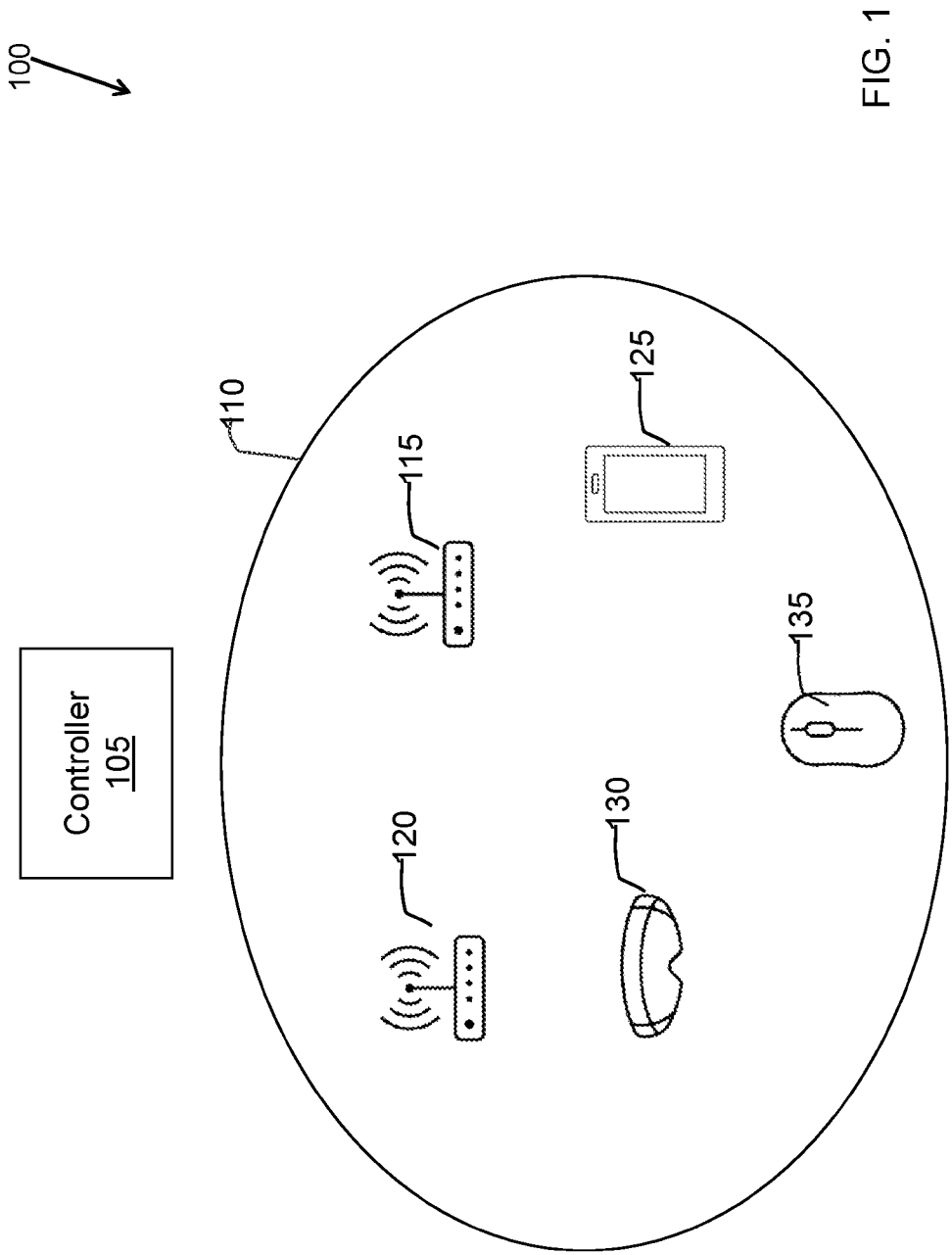

FIG. 1

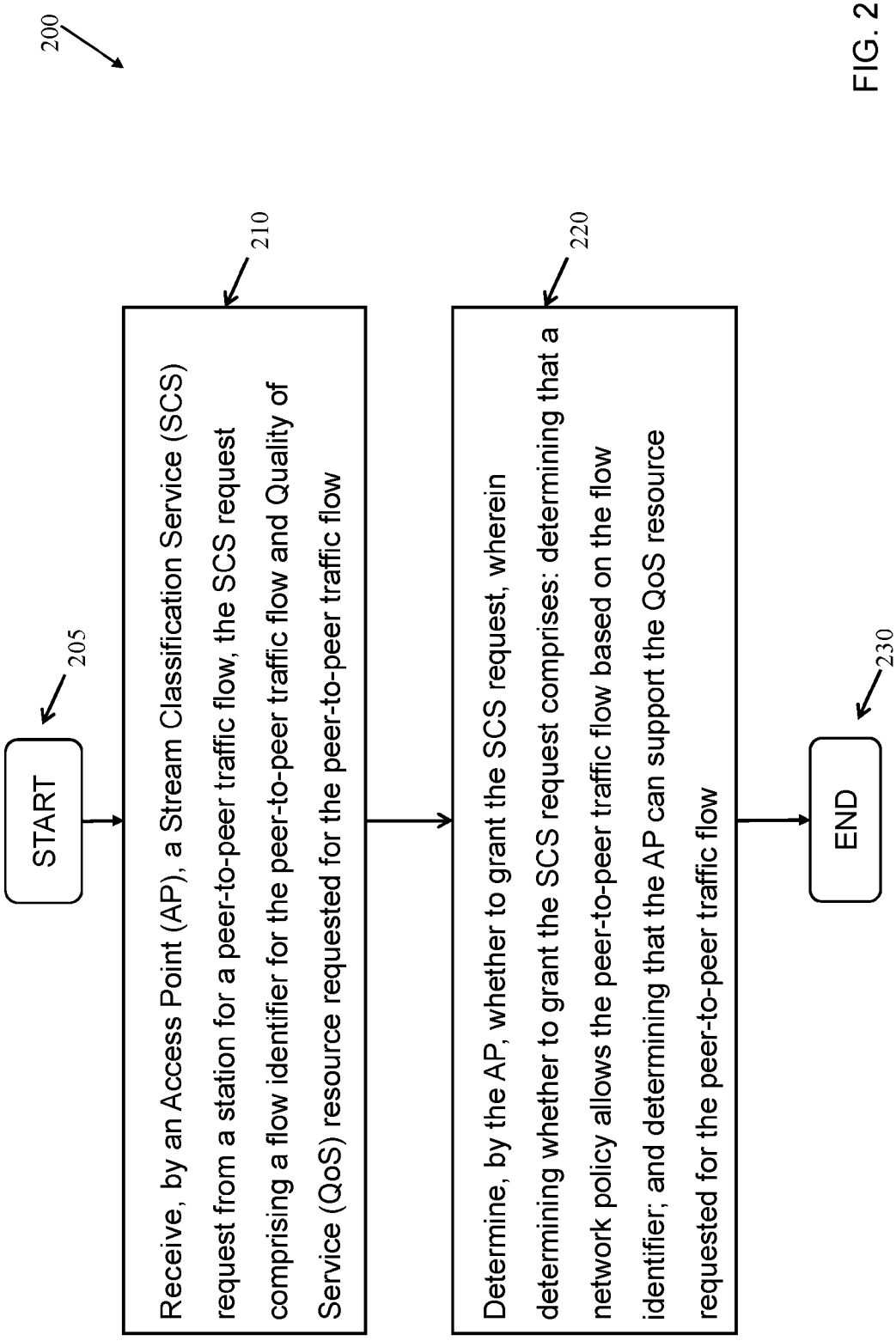
200
START
205
Receive, by an Access Point (AP), a Stream Classification Service (SCS) request from a station for a peer-to-peer traffic flow, the SCS request comprising a flow identifier for the peer-to-peer traffic flow and Quality of Service (QoS) resource requested for the peer-to-peer traffic flow
210
Determine, by the AP, whether to grant the SCS request, wherein determining whether to grant the SCS request comprises: determining that a network policy allows the peer-to-peer traffic flow based on the flow identifier; and determining that the AP can support the QoS resource requested for the peer-to-peer traffic flow
220
END
230

FIG. 2

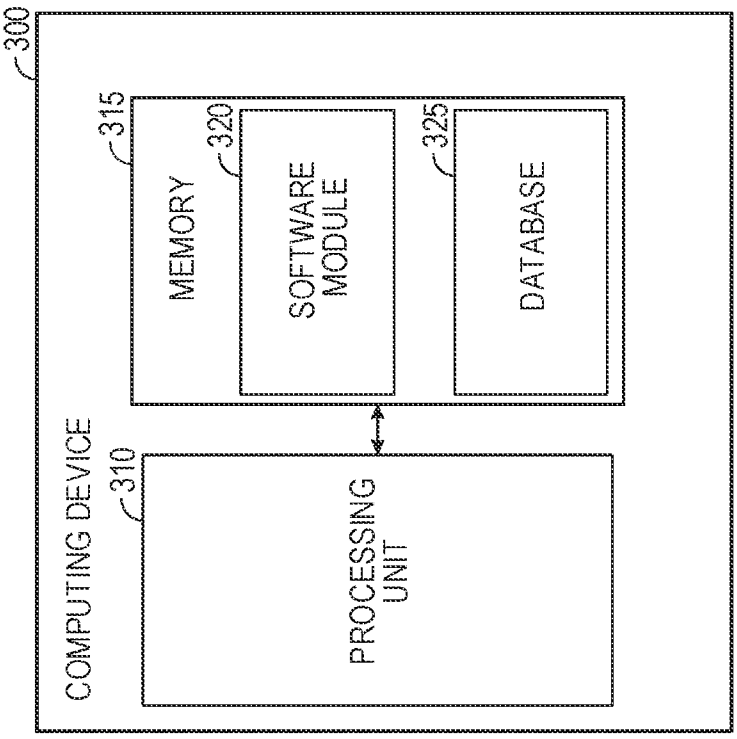
300
COMPUTING DEVICE
310
PROCESSING UNIT
315
MEMORY
320
SOFTWARE MODULE
325
DATABASE

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2024/062338

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W28/02 H04W28/24 H04W76/14 H04L67/104 H04W84/12
H04L47/2408 H04L47/2441

ADD.

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 H04L

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)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BINITA GUPTA (CISCO SYSTEMS): "LB275 CR for SCS TCLAS Counter Proposal", IEEE DRAFT; IEEE-SA MENTOR, PISCATAWAY, NJ USA , vol. 802.11 EHT; 802.11be, no. 2 28 October 2023 (2023-10-28), pages 1-9, XP068206774, Retrieved from the Internet: URL:https://mentor.ieee.org/802.11/dcn/23/11-23-1540-02-00be-lb275-cr-for-scs-tclas-counter-proposal.docx	1-7, 9-11,17, 18,20
Y	page 3 - page 7; tables 9-78	8,12-16, 19

-/--

[x] Further documents are listed in the continuation of Box C.

[x] 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	Date of mailing of the international search report
17 March 2025	24/03/2025

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Tortelli, Michele

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2024/062338

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2022/146635 A1 (INTEL CORP [US]) 7 July 2022 (2022-07-07)	1-4, 9-11,17, 18
A	paragraph [0019] - paragraph [0024] paragraph [0062] - paragraph [0067] paragraph [0101] - paragraph [0104] paragraph [0115]	5-8, 12-16, 19,20

Y	US 2023/156516 A1 (CHU LIWEN [US] ET AL) 18 May 2023 (2023-05-18)	8,12-16, 19
A	paragraph [0051] - paragraph [0061]; figures 2, 3	1-7, 9-11,17, 18,20

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2024/062338

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2022146635 A1	07-07-2022	EP 4272483 A1	08-11-2023
		US 2023379749 A1	23-11-2023
		WO 2022146635 A1	07-07-2022
US 2023156516 A1	18-05-2023	NONE	