IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh, et al.	
U.S. Patent No.:	9,271,184	Attorney Docket No.: 39843-0156IP1
Issue Date:	February 23, 2016	
Appl. Serial No.:	14/688,713	
Filing Date:	April 16, 2015	
Title:	WIRELESS END-USER DEVICE WITH PER-APPLICATION DATA LIMIT AND TRAFFIC CONTROL POLICY LIST LIMITING BACKGROUND APPLICATION TRAFFIC	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 9,271,184 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

I. REQUIREMENTS FOR IPR 1
- **A.** Grounds for Standing 1
- **B.** Challenge and Relief Requested 1
- **C.** Claim Construction 2
- **D.** Level of Ordinary Skill in the Art 3

II. THE '184 PATENT 3
- **A.** Brief Description 3
- **B.** Prosecution History 4

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE 4
- **A.** [GROUND 1] – Claims 1-6, 13, and 18 are rendered obvious by Rao, Oestvall, and Freund 4
  - 1. Overview of Rao 4
  - 2. Overview of Oestvall 8
  - 3. Combination of Rao and Oestvall 11
  - **(a)** Rao's system selectively allows and blocks network traffic from applications based on various criteria 11
  - **(b)** Like Rao, Oestvall's system selectively allows and blocks network traffic from applications based on various criteria, including whether the application is "trusted" or "untrusted" 14
  - **(c)** A POSITA would have been led to modify Rao's system to allow/block an application's network traffic based on the application's "trusted/untrusted" status as taught by Oestvall to thereby reduce battery drain 15
  - 4. Overview of Freund 19
  - 5. Combination of Rao-Oestvall and Freund 23
  - 6. Analysis 26
- **B.** [GROUND 2] – Claims 10-12, 14-17, and 19-20 are rendered obvious by Rao, Oestvall, Freund, and Araujo 58
  - 1. Overview of Araujo 58
  - 2. Combination of Rao-Oestvall-Freund and Araujo 62
  - 3. Analysis 66

IV. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION 79
- **A.** 35 U.S.C. §325(d) – *Discretionary Denial under 325(d) is not warranted* 79
- **B.** 35 U.S.C. §314(a) – Discretionary Denial is not Merited in view of Petitioner's *Sotera* Stipulation 80

Headwater Ex. 2004
Samsung v. Headwater
IPR2023-01362

V. CONCLUSION AND FEES 82

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....82
- **A.** Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....82
- **B.** Related Matters Under 37 C.F.R. § 42.8(b)(2).....82
- **C.** Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....83
- **D.** Service Information 83

Headwater Ex. 2004
Samsung v. Headwater
IPR2023-01362

EXHIBITS

SAMSUNG-1001 U.S. Patent No. 9,271,184 to Raleigh, et al. ("the '184 Patent")

SAMSUNG-1002 Excerpts from the Prosecution History of the '184 Patent ("the Prosecution History")

SAMSUNG-1003 Declaration and Curriculum Vitae of Dr. Kevin Butler

SAMSUNG-1004 Complaint, Headwater Research LLC v. Samsung Electronics Co., Ltd. et al., 2:22-cv-00422, E.D. Tex., October 26, 2022

SAMSUNG-1005 U.S. Patent Publication No. 2006/0039354 A1 ("Rao")

SAMSUNG-1006 U.S. Patent Publication No. 2007/0038763 A1 ("Oestvall")

SAMSUNG-1007 U.S. Patent No. 5,987,611 ("Freund")

SAMSUNG-1008 U.S. Patent Publication No. 2009/0217065 A1 ("Araujo")

SAMSUNG-1009 M. V. Pedersen, F. H. P. Fitzek, and T. Larsen, "Implementation and Performance Evaluation of Network Coding for Cooperative Mobile Devices," ICC Workshops - 2008 IEEE International Conference on Communications Workshops, Beijing, China: IEEE, May 2008, pp. 91–96. doi: 10.1109/ICCW.2008.22 ("Pedersen")

SAMSUNG-1010 U.S. Patent Publication No. No. 2008/0080458 ("Cole")

SAMSUNG-1011 U.S. Patent No. 8,381,127 ("Singh")

SAMSUNG-1012 W. R. Stevens, "TCP/IP Illustrated, Volume 1," 2003, ISBN: 0-13-141155-1 ("Stevens") (SAMSUNG-1013)

SAMSUNG-1013 TO SAMSUNG-1014 RESERVED

SAMSUNG-1015 Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (USPTO June 21, 2022) ("Director's Guidance")

SAMSUNG-1016 Samsung Stipulation letter regarding IPR grounds in District court litigation

Headwater Ex. 2004
Samsung v. Headwater
IPR2023-01362

SAMSUNG-1017 First Amended Complaint, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00422, E.D. Tex., November 30, 2022

SAMSUNG-1018 Amended Docket Control Order, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00422, E.D. Tex., April 21, 2023

Headwater Ex. 2004
Samsung v. Headwater
IPR2023-01362

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre]	A wireless end-user device, comprising:
[1a]	a wireless wide area network (WWAN) modem to communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the at least one WWAN; and
[1b]	one or more processors configured to, for a time when data communication for Internet service activities is provided by the WWAN modem,
[1c]	classify whether a particular application associated with an Internet service access request, and capable of both interacting with a user in a user interface foreground of the device, and at least some Internet service activities when not interacting with a user in the device user interface foreground, is interacting with the user in the device user interface foreground,
[1d]	apply a differential traffic control policy to the Internet service access request, based on

	(i) whether the application is classified as interacting with the user, and (ii) a differential traffic control policy list distinguishing between a first one or more applications resident on the device and a second one or more applications resident on the device,
[1e]	such that, the one or more processors are operable to, in a first state wherein the particular application is one of the first one or more applications, and the particular application is not classified as interacting with a user in the device user interface foreground, block the Internet service access request, and
[1f]	the one or more processors are operable to allow the Internet service access request in at least one other state, and
[1g]	for at least one of the first or second one or more applications, disallow Internet data communication for that application based on an application-specific amount of Internet data usage reaching a limit.
Claim 2	
[2]	The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is interacting with the user in the device user interface foreground

	when the user of the device is directly interacting with that application or perceiving any benefit from that application.
Claim 3	
[3]	The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is interacting with the user in the device user interface foreground based on a state of user interface priority for the application.
Claim 4	
[4]	The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is not interacting with the user in the device user interface foreground when the application is providing or utilizing a background data service.
Claim 5	
[5]	The wireless end-user device of claim 1, wherein the one or more processors are configured to, when the Internet service access request is blocked in the first state, delay network activity in association with the first Internet access request until a second Internet access request is received and allowed.

Claim 6	
[6]	The wireless end-user device of claim 1, further comprising a user interface, wherein the user interface is to inform the user of the device when there are options to set, control, override, or modify at least one aspect of the differential traffic control policy and/or the differential traffic control policy list.
Claim 10	
[10]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change a determination of whether to apply the differential traffic control policy based on a power state of the device.
Claim 11	
[11]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the determination of whether to apply the differential traffic control policy based on a device usage state.
Claim 12	

[12]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the determination of whether to apply the differential traffic control policy based on a device usage state.
Claim 13	
[13]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to update at least a portion of the differential traffic control policy and/or the differential traffic control policy list based on information received from a network element.
Claim 14	
[14]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to, when the Internet service access request is blocked, prevent the first Internet access request from causing a change to a power state of the modem.
Claim 15	
[15]	The wireless end-user device of claim 14, wherein the one or more processors are further configured to, when the power state of the modem is idle or sleeping, prevent power state changes to the modem until an Internet service access request is allowed.

Claim 16	
[16]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to, when the Internet service access request is blocked, instruct the first end-user application to transition to a different state.
Claim 17	
[17]	The wireless end-user device of claim 1, further comprising an agent to block, modify, remove, or replace user interface messages generated by the particular application based on the block of the Internet service access request.
Claim 18	
[18]	The wireless end-user device of claim 1, wherein the one or more processors operable to block the Internet service access request are configured to selectively block the Internet service access request by intercepting open, connect, and/or write requests by the particular application to a network stack.
Claim 19	

[19]	The wireless end-user device of claim 18, wherein the one or more processors are configured to respond to an intercepted request by the particular application by emulating network messaging.
Claim 20	
[20]	The wireless end-user device of claim 19, wherein emulating network messaging comprises responding to a network request from the particular application by blocking the request from passing to a network stack and returning to the particular application a message indicating the network request was not successful.

Samsung Electronics Co., Ltd. ("**Petitioner**" or "**Samsung**") petitions for *Inter Partes* Review ("**IPR**") of claims 1-6 and 10-20 ("**the Challenged Claims**") of U.S. Patent No. 9,271,184 ("**the '184 Patent**"). Compelling evidence presented in this Petition demonstrates at least a reasonable likelihood that Samsung will prevail with respect to at least one of the Challenged Claims.

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the '184 Patent is available for IPR. This petition is being filed within one year of service of a complaint against Samsung. SAMSUNG-1004. Samsung is not barred or estopped from requesting review of the Challenged Claims on the below-identified grounds.

B. Challenge and Relief Requested

Samsung requests an IPR of the Challenged Claims on the below grounds. Dr. Kevin Butler provides supporting testimony in his Declaration. SAMSUNG-1003, ¶¶1-262.

Ground	Claim(s)	35 U.S.C. § 103
1	1-6, 13, 18	Rao in view of Oestvall and Freund
2	10-12, 14-17, 19-20	Rao in view of Oestvall, Freund, and Araujo

The '184 Patent claims priority to a number of provisional applications, the

Headwater Ex. 2004
Samsung v. Headwater
IPR2023-01362

earliest of which was filed 1/28/2009. SAMSUNG-1001, Cover. While Samsung does not concede that 1/28/2009 is the priority date that should be afforded to the '184 Patent, for the purposes of this proceeding, each of the references asserted in this Petition qualifies as prior art under 35 USC § 102(b) and/or § 102(e) (as shown in the table below) even if the 1/28/2009 date of the provisional application is used as the priority date of the '184 Patent.

Reference	Filing Date	Publication Date
Rao	7/22/2005	2/23/2006
Oestvall	7/2/2004	2/15/2007
Freund	5/6/1997	11/16/1999
Araujo	2/26/2008	8/27/2009

C. Claim Construction

Petitioner submits that no formal claim constructions are necessary because "claim terms need only be construed to the extent necessary to resolve the controversy." *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); SAMSUNG-1003, ¶38. Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by the Board. Petitioner is not conceding that each challenged claim satisfies all statutory requirements, nor is Petitioner waiving any arguments concerning claim scope or grounds that can only be

raised in district court. For this petition, Petitioner applies prior art in a manner consistent with Patent Owner's allegations of infringement before the district court.

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art ("POSITA") relating to the subject matter of the '184 Patent as of 1/28/2009 would have had (1) at least a bachelor's degree in computer science, electrical engineering, or a related field, and (2) three to five years of experience with networking, power consumption of networked computing devices, and/or wireless digital communications systems. SAMSUNG-1003, ¶¶15-17. Additional graduate education could substitute for professional experience, and *vice versa*. *Id*.

II. THE '184 PATENT

A. Brief Description

The '184 Patent is directed to selectively "apply[ing] a differential traffic control policy to an application requesting Internet service access" through a "system 2700 for application-specific differential network access control." SAMSUNG-1001, Abstract, 100:28-102:56, FIG. 27; SAMSUNG-1003, ¶¶32-34.

The system "analyzes traffic from [a] network service consuming application," and "uses one or more policies to "determine an appropriate prioritization for traffic to and/or from the network service consuming application." *Id.*, 100:45-101:57. For example, the system can selectively (i) "cause[] the network service consuming application ... traffic to be queued in [an] application traffic cache" for

transmission over a network (*id.*, 101:63-102:11), or (ii) "restrict network access of a particular service usage activity" (*id.*, 102:12-37).

B. Prosecution History

The '184 Patent was allowed on the first action. SAMSUNG-1002, 46-54. In allowing the claims, the Examiner noted that the references cited during prosecution do not render obvious the [1c]-[1g] limitations. *Id.* SAMSUNG-1003, ¶36.

During prosecution, the Examiner did not consider any of Rao, Oestvall, Freund, and Araujo. *Id.* As discussed below, these references render obvious the Challenged Claims, including the [1c]-[1g] limitations. SAMSUNG-1003, ¶37.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. [GROUND 1] – Claims 1-6, 13, and 18 are rendered obvious by Rao, Oestvall, and Freund

1. Overview of Rao [1]

Rao describes a system for performing "intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application." SAMSUNG-1005, [0179], FIG. 5A; SAMSUNG-1003,

[1] Descriptions of the references and combinations thereof are incorporated into each mapping that includes citations to these references. All emphasis is added unless otherwise indicated.

¶¶39-53. Rao's system is used to prioritize "data communications" of some applications over others, and "compliment Quality of Service (QOS) networks." SAMSUNG-1005, [0184].

An example of this system is shown in FIG. 5A (reproduced below).

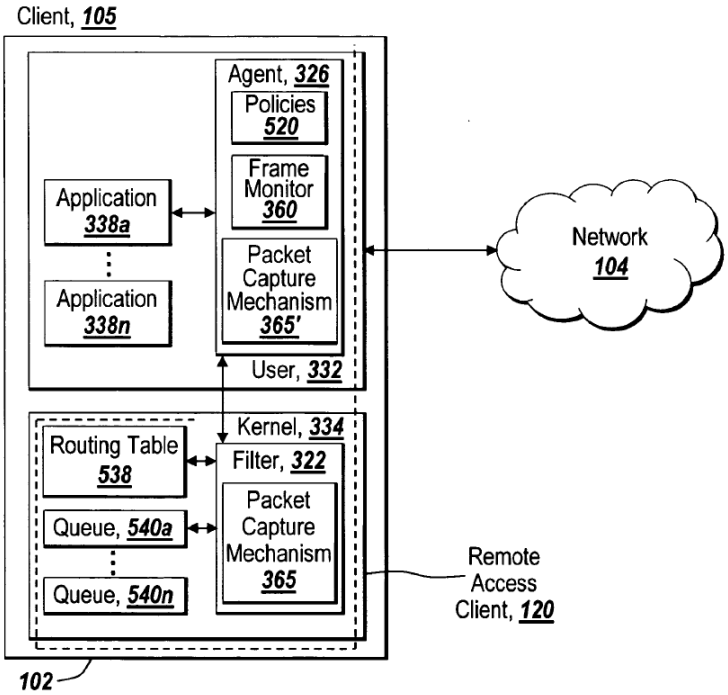


Fig. 5A

SAMSUNG-1005, FIG. 5A[2]

A "remote access client 105 of computing device 102 is connected to net-

[2] Annotations to the figures throughout this Petition are shown in color.

work 104" through one or more "LAN or WAN links" and/or "wireless connections," and "may execute one or more applications 338 a-338 n, which access the network 104 via the agent 326 and filter 322 of the remote access client 120." *Id*. Rao's applications can communicate with one or more servers on the network 104, such as "an application server providing email services such as Microsoft Exchange," "a web or Internet server," "a desktop sharing server," or "a collaboration server." *Id.*, [0090].

Further, Rao's system implements "one or more policies 520 for specifying client-side prioritization of network communications related to applications 338 a-338 n." *Id.*, [0182]. Rao deploys these policies by intercepting packets of network traffic by the applications (e.g., using a "packet capture mechanism 365, 365′"), determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. *Id.,* [0080], [0184]-[0190], FIGS. 5A-5B.

In some cases, Rao's system prioritizes the captured packets by allowing certain packets to be transmitted to the network. For example, Rao's system can use "[a] filter 322 [to] place, arrange, or coordinate network packets into queues 540 a-540 n in support of the priorities" (e.g., queues included on a network driver). *Id.*, [0143], [0180], [0191]. "[T]he network packets of the highest priority queue 540 a-540 n are communicated first, and then the next highest priority

queue 540 a-540 n second, and so on." *Id.*, [0194].

In some cases, Rao's system prioritizes the captured packets by blocking network packets from being transmitted to the network, either permanently or temporarily. *Id.*, [0102], [0207], [0040], [0194]; SAMSUNG-1003, ¶¶50-53.

As an example, based on the policies, Rao's system can block network packets from being transmitted to the network permanently, such as by "drop[ping] or accept[ing] the network packets depending on their content" (e.g., effectively deprioritizing those packets entirely). SAMSUNG-1005, [0102], [0207]. For instance, the "filter 322" can be used to "discard[] packets" having the lowest priority (e.g., "unwanted packets"), such that the packets are not transmitted to the network. *Id.*

As another example, Rao's system can block network packets from being transmitted to the network temporarily, by "preventing ... at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application" (e.g., by "holding" a packet in a queue, "releasing" the packet upon communication of packets from higher priority applications). *Id.*, [0040], [0194].

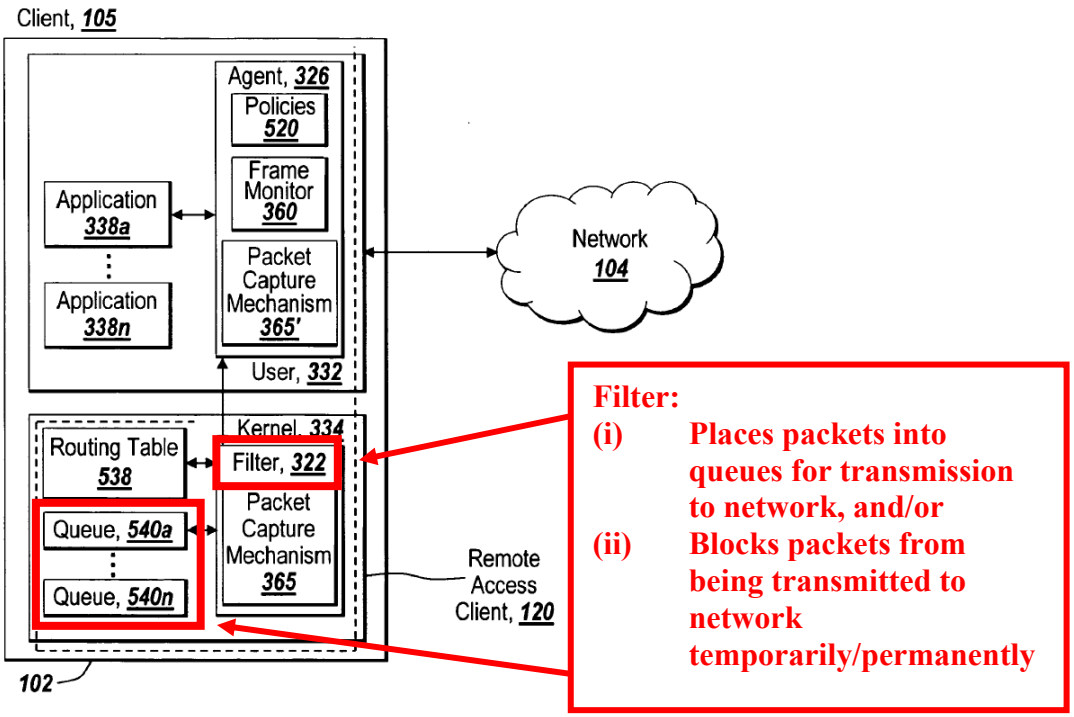


Fig. 5A

SAMSUNG-1005, FIG. 5A (annotated)

2. Overview of Oestvall

Oestvall describes "a method of enabling a multitasking computing device to preserve or conserve resources, such as battery power." SAMSUNG-1006, [0002]; SAMSUNG-1003, ¶¶54-61. According to Oestvall's method, a device classifies applications with respect to various criteria, and selectively provides resources to the applications based on their classifications. SAMSUNG-1006, [0008]-[0017], [0019]-[0025].

As an example, applications can be classified with respect to "'trust' or certi-

fication criteria—i.e. criteria which define the level of trustworthiness of the application." *Id.*, [0010]. Specifically, applications can be classified as (i) "untrusted" applications and (ii) "trusted" applications. *Id.*, [0015], FIG. 1.

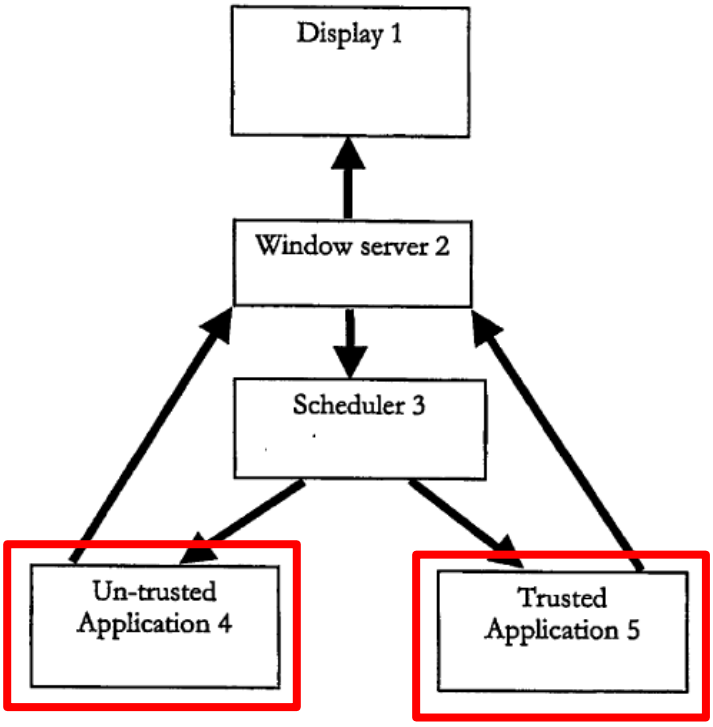


Figure 1

SAMSUNG-1006, FIG. 1 (annotated)

As another example, applications can be classified as "in the background or foreground on [a] display." *Id.*, [0023]. Further, applications may switch between being in the background or the foreground of the display. *Id.*, [0014], [0021], [0025].

Further, the device can provide resources to the applications differently, based on these classifications. *Id*., [0010]-[0017], [0021]-[0025]. For example, the device can selectively:

(i) Prevent an "untrusted" application in the background from running (*e.g.,* by preventing the application from "being given any services or consuming any resources") (*id*., [0023]),

(ii) Allow an "untrusted" application in the foreground to run (*id*., [0021], [0025]), and

(iii) Allow a "trusted" application to run, regardless of whether it is in the foreground or background (*id*., [0015]).

That is, Oestvall's device selectively provides resources to applications that it deems sufficiently important to consume resources (e.g., "trusted" applications and "untrusted" applications in the foreground), while selectively denying resources to applications that it deems not sufficiently important to consume resources (e.g., "untrusted" applications in the background). SAMSUNG-1003, ¶60.

As Oestvall describes, this method "is a valuable addition to power conservation strategies, especially (although without limitation) to battery operated devices." SAMSUNG-1006, [0024]. For example, the method can be performed to "prevent background untrusted applications from 'polling' for data over a wireless network, an activity that can potentially drain a battery quickly." *Id.* Accordingly,

the "battery life" of the device is "increased." *Id*., [0009].

3. Combination of Rao and Oestvall

A POSITA would have found it obvious to modify Rao's system of prioritizing network packets based on the specific application classification criteria taught by Oestvall. SAMSUNG-1003, ¶¶62-82; §III.A.1, §III.A.2. Combining Rao and Oestvall would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way. *See KSR Int'l Co. v. Teleflex Inc.,* 550 U.S. 398, 415-421, 82 USPQ2d 1385, 1395-97 (2007)*; MPEP 2143*; SAMSUNG-1003, ¶¶62-82.

Specifically, a POSITA would have recognized (i) that Rao and Oestvall are both directed to similar operations having similar purposes (e.g., controlling an application's access to a network in order to preserve limited system resources), and (ii) that Oestvall provides specific classification criteria for achieving a specific technical benefit (e.g., reducing battery consumption in a network-enabled device). SAMSUNG-1003, ¶62.

(a) Rao's system selectively allows and blocks network traffic from applications based on various criteria

Rao's system includes several applications configured to transmit network packets to a network (e.g., the Internet via one or more wireless connections).

SAMSUNG-1005, [0095],[0125], [0179]; §III.A.1. Rao's system controls each of the applications' access to the network by intercepting packets of network traffic by the applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. SAMSUNG-1005, [0184]-[0190], FIG. 5B; SAMSUNG-1003, ¶¶64-69.

Specifically, Rao's system prioritizes network packets by implementing one or more policies 520 for controlling network traffic. SAMSUNG-1005, [0182]. These policies can "define prioritization" based on various criteria, including:

(i) "the name of the application,"

(ii) "<u>the type of application,"</u>

(iii) "the type of one or more protocols used by the application[s],"

(iv) "the size of the payload of the network packet"

(v) <u>"whether an application is running in the foreground or the back-ground of the client,"</u> and/or

(vi) "the destination network address, such as host name or IP address, and/or destination port number." SAMSUNG-1005, [0182].

Based on these policies, Rao's system can selectively use a filter to (i) <u>allow</u> network packets to be transmitted to the network or (ii) <u>block</u> the network packets

from being transmitted to the network, either permanently or temporarily. SAMSUNG-1005, [0191], [0194], [0207]; SAMSUNG-1003, ¶¶65-68; §III.A.1. Although Rao's description regarding the use of "policies 520" in this context is set forth in the context of "a network disruption shielding technique" (*see, e.g.,* SAMSUNG-1005, [0199]), a POSITA would have found it obvious to also use "policies 520" to discard low priority packets in other circumstances where the network is not disrupted but there nevertheless exists a similar desire to reduce communications over the network (e.g., due to reductions in the network's bandwidth, or a surge in higher priority packets to be sent over the network). SAMSUNG-1003, ¶68. Doing so would have achieved the benefit of ensuring that communication or system resources (e.g., memory) are selectively freed up for higher priority packets/communications. SAMSUNG-1003, ¶68.

For instance, a POSITA would have understood or found it obvious to configure Rao's system to prioritize the captured packets by selectively "drop[ping] or accept[ing] the network packets depending on their content" (e.g., effectively deprioritizing those packets entirely). SAMSUNG-1005, [0102]; SAMSUNG-1003, ¶69. As an example, the "filter 322" can be used to "discard[] packets" having the lowest priority (e.g., "unwanted packets"), such that the packets are permanently blocked from being transmitted to the network. SAMSUNG-1005, [0102]; SAMSUNG-1003, ¶69.

(b) Like Rao, Oestvall's system selectively allows and blocks network traffic from applications based on various criteria, including whether the application is "trusted" or "untrusted"

Like Rao, Oestvall describes an application-based priority system for controlling access to resources. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]; SAMSUNG-1003, ¶70. Further, Oestvall contemplates similar criteria as Rao, and teaches that specific combinations of these criteria can be selected to achieve a specific technical benefit. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]; SAMSUNG-1003, ¶70.

Specifically, Oestvall teaches that certain types of applications (e.g., "untrusted" applications) that are running in the background of the client should be assigned a low priority, such that they cannot access a network. SAMSUNG-1006, [0008], [0014]-[0017], [0021], [0023], [0024]; SAMSUNG-1003, ¶71.
Further, Oestvall teaches that certain other types of applications (e.g., "trusted" applications) should be assigned a high priority, such that they can continue to access a network. SAMSUNG-1006, [0008], [0014]-[0017], [0021], [0023], [0024]; SAMSUNG-1003, ¶72.

As Oestvall describes, these combinations of criteria can be used to "prevent background untrusted applications from 'polling' for data over a wireless network, an activity that can potentially drain a battery quickly." SAMSUNG-1006,[0024]; SAMSUNG-1003, ¶73.

(c) A POSITA would have been led to modify Rao's system to allow/block an application's network traffic based on the application's "trusted/untrusted" status as taught by Oestvall to thereby reduce battery drain

A POSITA would have readily recognized that Rao's remote access client 120 could use a filter to discard packets from background untrusted applications (e.g., effectively deprioritizing those packets entirely) to thereby prevent them from being communicated over network 104. SAMSUNG-1003, ¶74. As a consequence, the battery life of a mobile device client 105 would be increased, as taught by Oestvall. SAMSUNG-1003, ¶74. Indeed, while Oestvall teaches increasing battery life by preventing such applications from running and thereby engaging in any network communications, a POSITA would have recognized that the power usage associated with using a wireless modem to transmit network packets to a network far exceeds the power usage associated with an application generating those network packets. SAMSUNG-1003, ¶74. *Also see, generally,* SAMSUNG-1009. Accordingly, a POSITA would have readily recognized that Rao's system could be used to enable a similar increase in battery life by specifically preventing the battery draining activity identified by Oestvall (i.e., preventing the network/packet communications that result in excessive battery drain). SAMSUNG-1003, ¶74.

That is, a POSITA would have recognized (i) that Rao's system is ready for

improvement in this way based on Oestvall's teachings and (ii) that such an improvement would enable the system to not only provide the benefits identified by Rao but also provide the additional benefit taught by Oestvall of increased battery life when client 105 is a wireless mobile device. SAMSUNG-1003, ¶74. Moreover, this increase in battery life would be obtained without having to completely shut down the application as disclosed by Oestvall. SAMSUNG-1003, ¶75. In particular, a POSITA would have recognized that, based on Rao, the combined Rao-Oestvall system can reduce battery drain while controlling the network activities of applications to a much greater degree of granularity than offered by Oestvall's relatively blunt approach of completely shutting down applications to achieve this benefit. SAMSUNG-1003, ¶75.

As an example of this modification, a POSITA would have configured Rao's "filter 322" to selectively block network packets and/or transmit network packets to the network, specifically based on the criteria specified by Oestvall. SAMSUNG-1003, ¶76. Specifically, the "filter 322" would selectively "discard[]" network packets from applications that are "untrusted" and running in the background (e.g., a classification of applications that should be assigned a low priority, as taught by Oestvall). SAMSUNG-1003, ¶76. Accordingly, these applications can no longer poll for data over a wireless network (i.e., an activity that Oestvall teaches as being particularly burdensome on a battery). SAMSUNG-1003, ¶76.

Further, the "filter 322" would selectively allow the transmission of network packets from applications that are either (i) "untrusted" and running in the foreground or (ii) "trusted," regardless of whether they are running in the foreground or the background (e.g., classifications of applications that should be assigned a high priority, as taught by Oestvall). SAMSUNG-1003, ¶77. Accordingly, applications that are sufficiently important can continue to exchange data in accordance with one or more Internet services. SAMSUNG-1003, ¶77.

An example modification to Rao's system in view of Oestvall's teachings ("Rao-Oestvall system") is shown below.

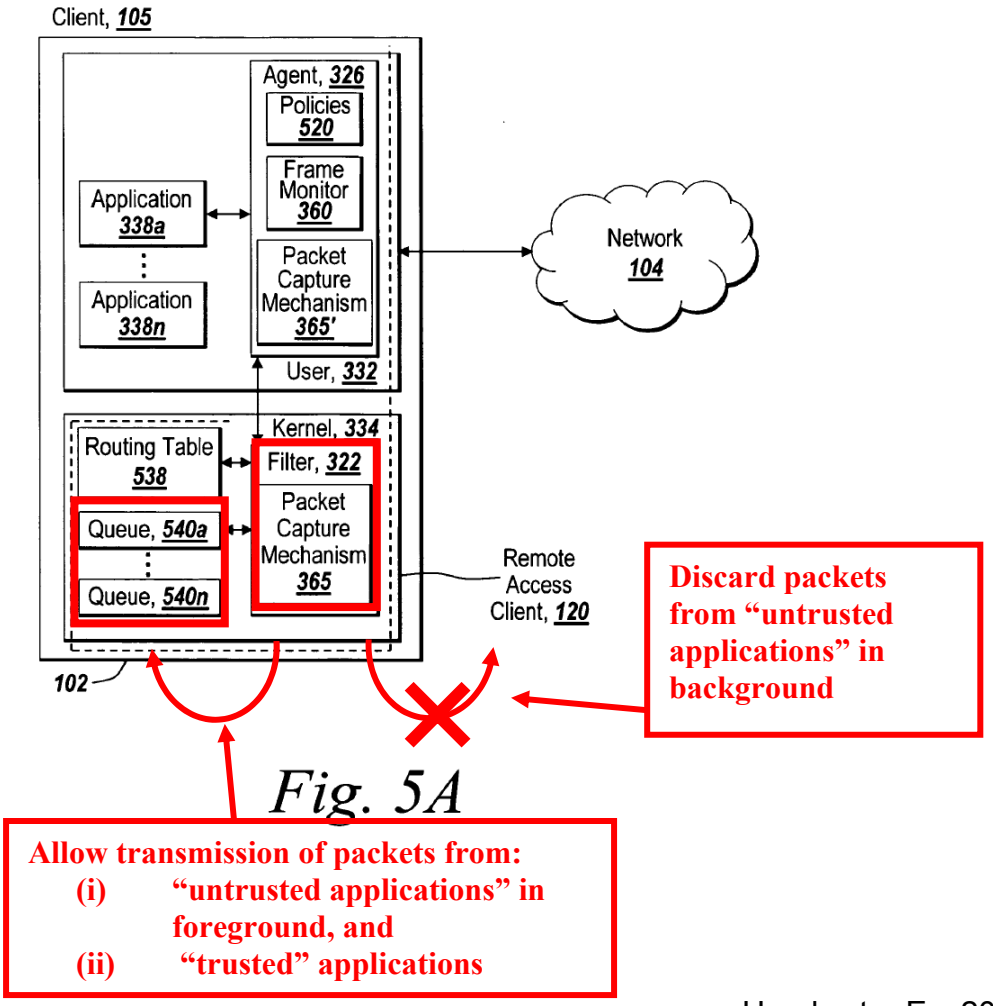


Fig. 5A

SAMSUNG-1005, FIG. 5A (annotated)

While the Rao-Oestvall system reduces battery drain by blocking an application's transmission of network packets permanently as taught by Rao (as distinguished from shutting down the application entirely to reduce battery drain as taught by Oestvall), a POSITA also would have found it obvious to configure the Rao-Oestvall system to additionally or alternatively selectively block network packets temporarily as taught by Rao, in at least some situations where more granular control of battery draining activities is desired. SAMSUNG-1003, ¶79.

For example, Rao describes that its system can block network packets from being transmitted to the network temporarily, by "preventing ... at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application" (e.g., by "holding" a packet in a queue, "releasing" the packet upon communication of packets from higher priority applications). SAMSUNG-1005, [0040], [0149]; §III.A.1; SAMSUNG-1003, ¶80. As Rao explains, this "holding" technique can be beneficial in "provid[ing] a packet by packet prioritization across all applications ... and intercepted network packets" and to implement prioritization according to different levels of "granularity." SAMSUNG-1005, [0191].

A POSITA would have recognized that "holding" of network packets of

lower priority applications until the packets of higher priority applications have been transmitted would increase the likelihood that the battery will have sufficient remaining energy to successfully transmit the packets of the higher priority applications, thereby preferentially allocating the limited battery energy resource to those higher priority applications over the lower priority applications. This enables lower priority applications (e.g., "untrusted" applications in the background) to still be able to communicate over the network but to do so in accordance with their lower level of priority and without interfering with the activities of other applications having higher priorities (e.g., "untrusted" applications in the foreground or "trusted" applications). SAMSUNG-1003, ¶81.

Accordingly, consistent with Rao's teachings, the Rao-Oestvall system can control the battery draining activities of applications according to a greater degree of granularity than offered by Oestvall alone and, in doing so, achieve a similar reduction in battery drain while also minimizing disruption to the operation of the applications. SAMSUNG-1003, ¶82.

4. Overview of Freund

Freund describes "[a] computing environment with methods for monitoring access to an open network, such as WAN or the Internet." SAMSUNG-1007, Abstract; SAMSUNG-1003, ¶¶83-87. In an exemplary configuration, Freund's sys-

tem includes several client devices, each having "a client-side monitoring component for monitoring Internet access" by that client device. SAMSUNG-1007, 14:51-62, FIG. 3A, 310a-310c. Further, Freund's system includes "a server 321 (or another client) having a "supervisor 323 [that] directs runtime monitoring operations" by "maintain[ing] the access rules for the client based filter and verif[ying] the existence and proper operation of the client-based filter application"). *Id.*, 3:50-4:4, 14:62-67.

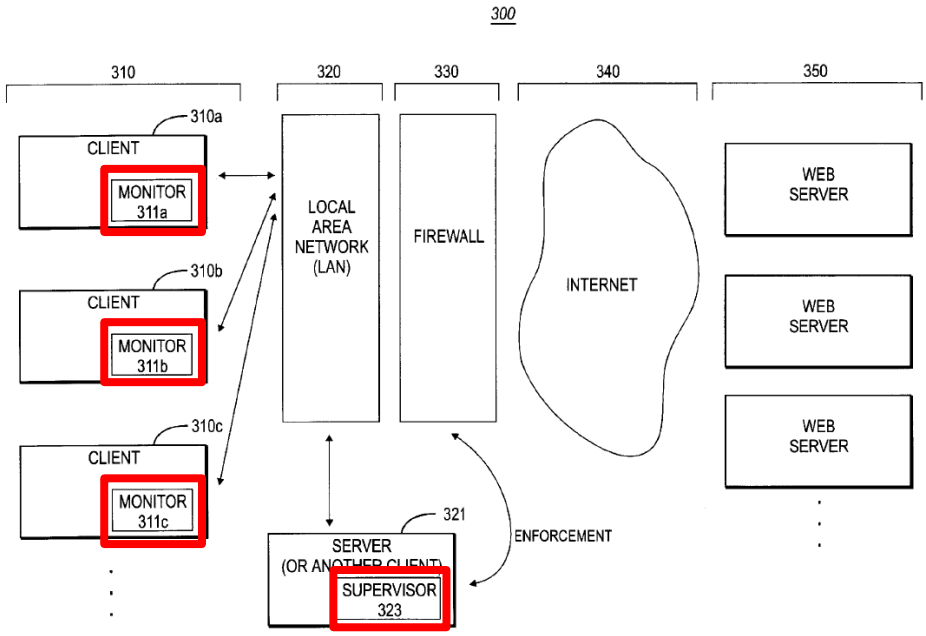


FIG. 3A

SAMSUNG-1007, FIG. 3A (annotated)

Freund's system "monitor[s] and regulate[s] Internet access on a per application basis," and "specif[ies] which applications can (and cannot) access the Inter-

net." *Id.,* 10:44-50. For instance, Freund's system can "monitor[] access to the Internet by individual applications ... to not only track Internet traffic but also [to] determine in many cases data exchanged on a per application basis." *Id.,* 11:10-15. As Freund teaches, "per application monitoring simplifies the task of tracking bandwidth utilization for a network, including providing detailed review on how the Internet access is being used," and can "greatly ease[] planning of hardware and connection requirements." Further, this system can "avert ... [i]nadvertent disruptions of the network by individual users, such as bandwidth hording [sic] by a user using RealAudio for listening to a Web audio 'broadcast.'" *Id.,* 11:21-28.

In an exemplary monitoring process, Freund's system performs "bandwidth and interactive use monitoring" in which a "Client Monitor maintains a list of active Applications (processes) with various fields to track activities and a global activity record." *Id.,* 30:10-29, FIGS. 13A-13B. For each of the applications on a device, Freund's "Client Monitor" intercepts the application's requests to access the Internet (e.g., "Winsock ... calls" to a "communications driver"). *Id.,* 29:17-30:9, FIG. 13A (1301). Further Freund's "Client Monitor" determines the amount of Internet data that is transmitted and/or received by the application (e.g., "data lengths"), and tracks the amount of data (e.g., by "[a]dd[ing] the data lengths to a DataIn or DataOut accumulator or counter"). *Id.*, 30:24-29, FIG. 13A (1302(D)).

Further, Fruend's system selectively allows or prevents the application from

accessing the Internet based on the amount of data used by that application. *Id.* For example, "[i]f [an] application is not allowed to access the Internet ... then [the] client monitor can stop [that] application from accessing the Internet and/or warn user." *Id.,* 5:61-64. In particular, with respect to bandwidth monitoring, "[i]f the DataIn or DataOut fields exceed rule-based quantity either for the specific Application or the user/workstation, the Client Monitor disables future Internet access and/or warns the user." *Id.*, 30:24-29, FIG. 13A (1302(E)).

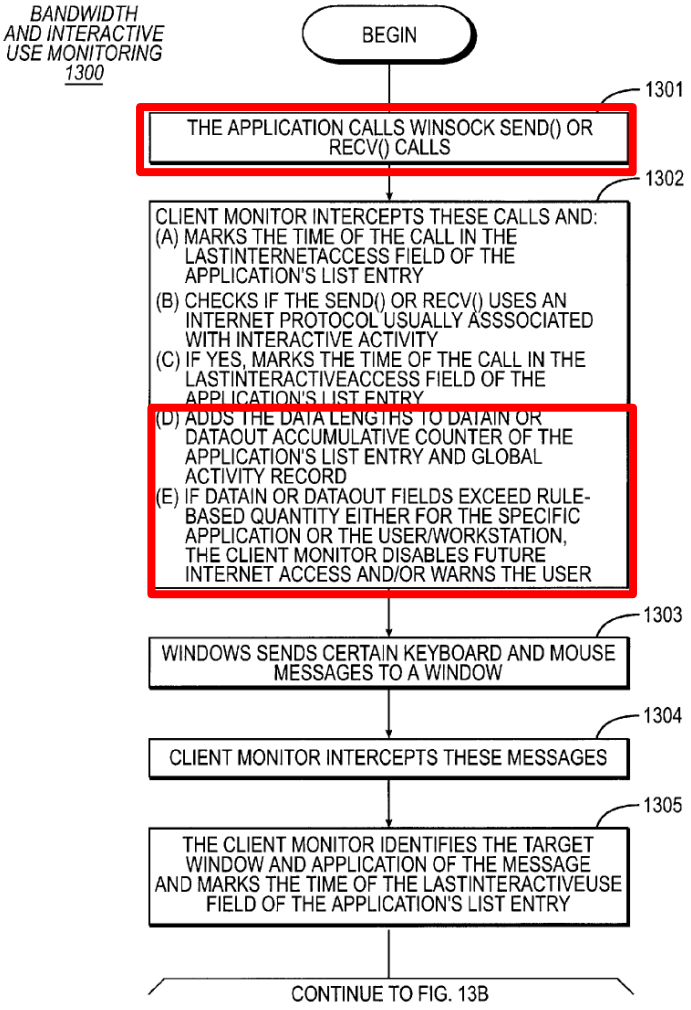


FIG. 13A

SAMSUNG-1007, FIG. 3A (annotated)

5. Combination of Rao-Oestvall and Freund

In view of Freund, a POSITA would have found it obvious to modify the Rao-Oestvall system to selectively enable an application to access a network (e.g., the Internet) based on the amount of network data that has been used by that application. SAMSUNG-1003, ¶¶88-93; §III.A.3, §III.A.4. Combining Rao-Oestvall with Freund would have involved (1) combining prior art elements according to

known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421, 82 USPQ2d 1385, 1395-97 (2007); MPEP 2143; SAMSUNG-1003, ¶¶88-93.

In particular, a POSITA would have recognized that, like the Rao-Oestvall system, Freund's system is configured to control an application's access to a network in order to preserve limited system resources. SAMSUNG-1007, 11:19-28; SAMSUNG-1003, ¶89. Further, a POSITA would have recognized that Freund provides a specific "bandwidth and interactive use monitoring" technique for selectively blocking an application's request to access a network in order to achieve a specific technical benefit (e.g., to "avert ... [i]nadvertent disruptions of the network by individual users, such as bandwidth hording [sic] by a user"). SAMSUNG-1007, 11: 19-28; SAMSUNG-1003, ¶¶89-90.

In view of Freund, a POSITA would have found it obvious to modify the Rao-Oestvall system to additionally include Freund's "bandwidth and interactive use monitoring" in order to prevent an application from hoarding the bandwidth of a network. SAMSUNG-1007, 11: 19-28; SAMSUNG-1003, ¶91. Further, a POSITA would have recognized that Freund's "bandwidth and interactive use monitoring" enhances the Rao-Oestvall system's ability to control an application's access to a network and to preserve limited system resources by accounting for the

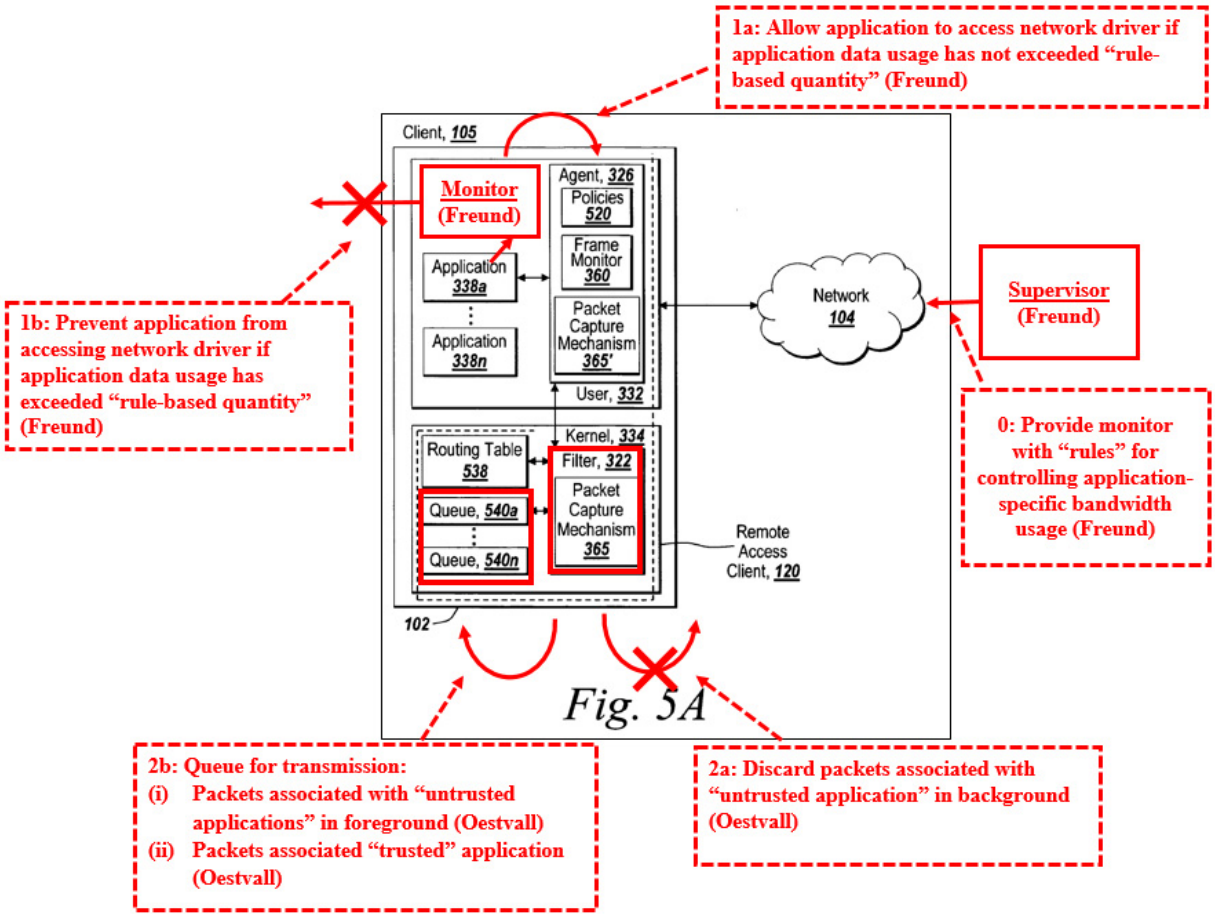
aggregate amount of data transmitted by an application over the network. SAMSUNG-1003, ¶91.

As an example of this modification, a POSITA would have modified the Rao-Oestvall system to additionally include (i) Freund's "Client Monitor" in Rao's client device, and (ii) Freund's "Supervisor" on a server remote from Rao's client device. SAMSUNG-1003, ¶¶91-93. Specifically, a POSITA would have configured the "Supervisor" to instruct the "Client Monitor" to perform Freund's "bandwidth and interactive use monitoring" in accordance with a set of filter rules. SAMSUNG-1003, ¶91. According to these rules, the "Client Monitor" would (i) intercept an application's requests to access the Internet, (ii) determine and track the amount of Internet data that is transmitted and/or received by that application, and (iii) disable future Internet access by that application if the amount of data exceeds a particular application-specific data limitation (see step 1b below). SAMSUNG-1003, ¶91.

If an application is permitted to access the Internet (e.g., the amount of data used by the application does not yet exceed the application-specific data limitation), the network packets generated by that application would be filtered in accordance with the Rao-Oestvall combination, as described above (see steps 1a, 2a, and 2b below). SAMSUNG-1003, ¶92.

An example modification to the Rao-Oestvall system in view of Freund's

teachings ("Rao-Oestvall-Freund combination" or "ROFC") is shown below.



Rao's FIG. 5A (revised and annotated)

6. Analysis

[1pre]

ROFC renders obvious [1pre]. SAMSUNG-1003, ¶¶94-95.

Rao describes a device that is configured to communicate data wirelessly with a WAN and the Internet, such as to obtain email services, access a web or Internet service, access a desktop sharing server, and/or access a collaboration server

(***wireless end-user device***). SAMSUNG-1005, [0090], [0125]; §III.A.1.

[1a]

ROFC renders obvious [1a]. SAMSUNG-1003, ¶¶96-99.

Rao describes a device that is configured to communicate data wirelessly with a WAN and the Internet (e.g., using a "wireless network adapter" and/or a "modem") (***WWAN modem***). SAMSUNG-1005, [0125].

Further, Rao describes that the device is configured to communicate data for Internet service activities, such as to obtain email services, access a web or Internet service, access a desktop sharing server, and/or access a collaboration server **(*communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the at least one WWAN*).** SAMSUNG-1005, [0090].

To the extent that Rao does not expressly describe a "WWAN modem," a POSITA would have understood or found it obvious to implement a WWAN modem in Rao's system in view of Rao's teaching that (i) a device can access a WAN or the Internet wirelessly, and (ii) a "modem" can be used to interface the device with "any type of network." SAMSUNG-1005, [0125]. SAMSUNG-1003, ¶99. Further, network configurations for mobile devices that enabled WWAN connectivity via modems were conventional by the Critical Date. SAMSUNG-1003, ¶99; SAMSUNG-1010, [0035], FIG. 2.

[1b]

ROFC renders obvious [1b]. SAMSUNG-1003, ¶¶100-104.

Rao describes "a computing device useful for practicing an embodiment of the [subject matter described by Rao]." SAMSUNG-1005, [0118], FIG. 1D.

As Rao describes, "[e]ach computing device 102 includes a central processing unit [121]"[3] (***one or more processors***) that includes "any logic circuitry that responds to and processes instructions fetched from the main memory unit 104." SAMSUNG-1005, [0118]. *See also* SAMSUNG-1005, [0121] ("main processor 100"), FIG. 1E.

[3] Rao's [0118] erroneously refers to the "central processing unit" as "102," rather than "121" as depicted in FIG. 1D.

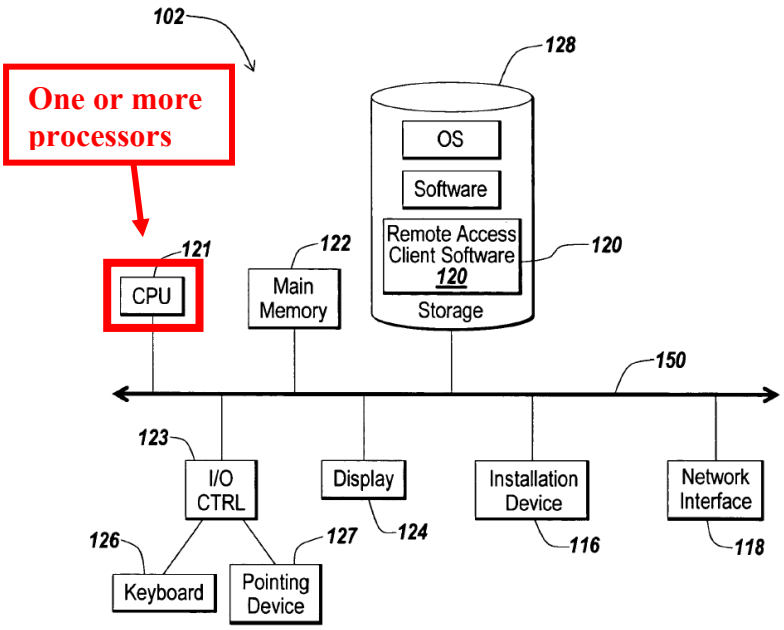


Fig. 1D

SAMSUNG-1005, FIG. 1D (annotated)

Further, as described in more detail below, Rao describes performing various operations using the processors for a time ***when data communication for Internet service activities is provided by the WWAN modem.*** *See* [1c]-[1g].

[1c]

ROFC renders obvious [1c], which includes features [1c(i)], [1c(ii)] and [1c(iii)]. SAMSUNG-1003, ¶¶105-118.

Regarding [1c(i)], Rao describes that an application can communicate with one or more servers on the network 104, an example of which is the Internet.

SAMSUNG-1005, [0090], [0095], [0125]. Further, Rao describes that an application can access services provided by a server 102e connected to the network 104 (i.e., the Internet), such as those provided by "an application server providing email services such as Microsoft Exchange," "a web or Internet server," "a desktop sharing server," or "a collaboration server" (***a particular application associated with an Internet service access request***). SAMSUNG-1005, [0090], FIG. 1A.

In particular, in Rao, an application may attempt to access an Internet service by transmitting packets to that Internet service (***Internet service access request***). *See, e.g.,* SAMSUNG-1005, [0179], [0184]. SAMSUNG-1003, ¶107.

A POSITA would have understood or found it obvious that Rao contemplates its applications being "associated with an Internet service access request" based on Rao's teachings of its applications communicating over the Internet and receiving service from servers. SAMSUNG-1005, [0090]; SAMSUNG-1003, ¶108. That is, based on these teachings, a POSITA would have understood or found it obvious that Rao's applications would be configured to send packetized communications over the Internet to such servers requesting access to their corresponding services ***(an Internet service access request***) to enable such applications to receive mail, Web, and/or other data content. SAMSUNG-1005, [0090]; SAMSUNG-1003, ¶108.

Regarding [1c(ii)], as discussed above, Rao describes that applications can

request access to Internet services." SAMSUNG-1005, [0090]. Further, Rao describes that an application may be "running in the foreground or the background of the client." SAMSUNG-1005, [0182]. *See also* SAMSUNG-1005, [0188]-[0189]. A POSITA would have understood or found it obvious that Rao's applications envision interactions with users in the foreground (e.g., such that the user can engage in email, web, desktop sharing, and/or collaboration activities) ***(interacting with a user in a user interface foreground of the device***). SAMSUNG-1003, ¶109.

Further, Rao contemplates that applications that are running in the background may perform at least some Internet service activities, such as by generating network packets (***capable of ... at least some Internet service activities when not interacting with a user in the device user interface foreground***). SAMSUNG-1005, [0003]. For example, a POSITA would have understood or found it obvious that Rao's email application can perform Internet service activities in the background (e.g., polling an email server for updates and/or retrieving emails in the background). SAMSUNG-1005, [0003], [0090]; SAMSUNG-1003, ¶110.

To the extent that Rao does not expressly describe that an application would be capable of both (i) interacting with a user in a user interface foreground of the device, and (ii) at least some Internet service activities when not interacting with a user in the device user interface foreground, this feature would have been obvious in view of Oestvall. SAMSUNG-1003, ¶111. For example, Oestvall describes that

a device includes applications that are capable of both:

(i) Running the "foreground" and "present[ing] a user interface with which a user can interact" (***interacting with a user in a user interface foreground of the device***), and

(ii) Running in the "background" and "not being interacted with by an end-user and ... present[ing] no user interface with which a user could interact (but it could for example present an icon indicating its presence and the fact that it was still active)" (***not interacting with a user in the device user interface foreground)***. SAMSUNG-1006, [0006], [0015].

Further, Oestvall describes that an application can perform network activities, and that applications may be capable of consuming "resources" (e.g., by performing network service activities such as "'polling' for data over a wireless network") when in the background (***capable of ... at least some ... activities when not interacting with a user in the device user interface foreground***). SAMSUNG-1006, [0023]-[0024].

In view of Oestvall, a POSITA would have understood or found it obvious that Rao's applications can interact with users in the foreground by "present[ing] a user interface with which a user can interact" in order to allow users to engage in activities such as email, web, desktop sharing, and/or collaboration) ***("interacting***

with a user in a user interface foreground of the device"). SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶¶114-115.

Further, in view of Oestvall, a POSITA would have understood or found it obvious that Rao's applications can perform Internet service activities (e.g., an email application polling an email server for updates and/or retrieving emails), even if the user is not interacting with the application and/or the application is not presenting a user interface with which a user could interact ***(capable of ... at least some Internet service activities when not interacting with a user in the device user interface foreground)***. SAMSUNG-1006, [0024]; SAMSUNG-1003, ¶116.

Regarding [1c(iii)], Rao describes that the device classifies "whether an application is running in the foreground or the background of the client 105" (***classify whether a particular application ... is interacting with the user in the device user interface foreground***). SAMSUNG-1005, [0182], [0188]-[0189]; SAMSUNG-1003, ¶117.

Oestvall also describes that the device uses a "window server component 2 ... to determine if an application is in the background or foreground on display" (***classify whether a particular application ... is interacting with the user in the device user interface foreground***). SAMSUNG-1006, [0008], [0016]-[0017], [0022]-[0023]; ; SAMSUNG-1003, ¶118.

[1d]

ROFC renders obvious [1d]. SAMSUNG-1003, ¶¶119-139.

A discussed in [1c], Rao describes an application is associated with an ***Internet service access request***. [1c], SAMSUNG-1003, ¶120.

Rao's system controls each of the applications' Internet service access requests by intercepting packets of network traffic by the applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. SAMSUNG-1005, [0184]-[0190], FIG. 5B. SAMSUNG-1003, ¶121.

Specifically, Rao's system includes "a packet capture mechanism 365, 365′ ... for intercepting network traffic of any of the applications 338 a-338 n of the client 105." SAMSUNG-1005, [0080], [0184]-[0186], FIG. 5A.

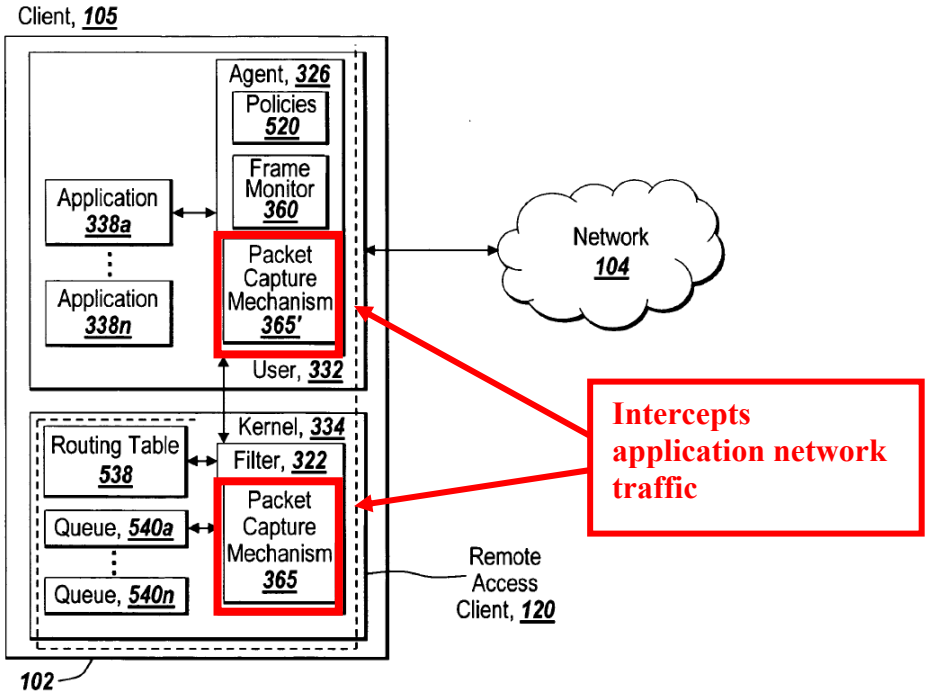


Fig. 5A

SAMSUNG-1005, FIG. 5A (annotated)

Further, Rao's system prioritizes the intercepted network packets by implementing one or more policies for controlling network traffic (***applying a differential traffic control policy to the Internet service access request***). SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶¶122-123. These policies can "define prioritization" based on various criteria, including:

(i) "the name of the application,"

(ii) "the type of application,"

(iii) "the type of one or more protocols used by the application[s],"

(iv) "the size of the payload of the network packet"

(v) "whether an application is running in the foreground or the background of the client," and/or

(vi) "the destination network address, such as host name or IP address, and/or destination port number." SAMSUNG-1005, [0182].

Specifically, in applying Rao's policies to differentially distinguish how the network traffic of distinct applications will be handled, Rao's system considers any one or more of the above criteria, including "whether an application is running in the foreground or the background of the client" (***applying*** … ***based on*** … ***whether the application is classified as interacting with the user)***. SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶124.

Further, by also considering the "type[s]" of applications and/or differently named applications, among other criteria, the application of Rao's policies for handling application traffic is further based on ***distinguishing between a first one or more applications resident on the device and a second one or more applications resident on the device.*** SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶125.

Rao describes that "[t]he policies ... may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium," which a POSITA would have understood would encompass one or more lists (***a differential traffic control policy list***). SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶126.

However, to the extent that Rao does not expressly describe representing these applications in the form of a list, a POSITA nevertheless would have found it obvious to implement such a list, as they would have recognized that a list is a commonplace "format of syntax and/or language" for enumerating data. SAMSUNG-1003, ¶127.

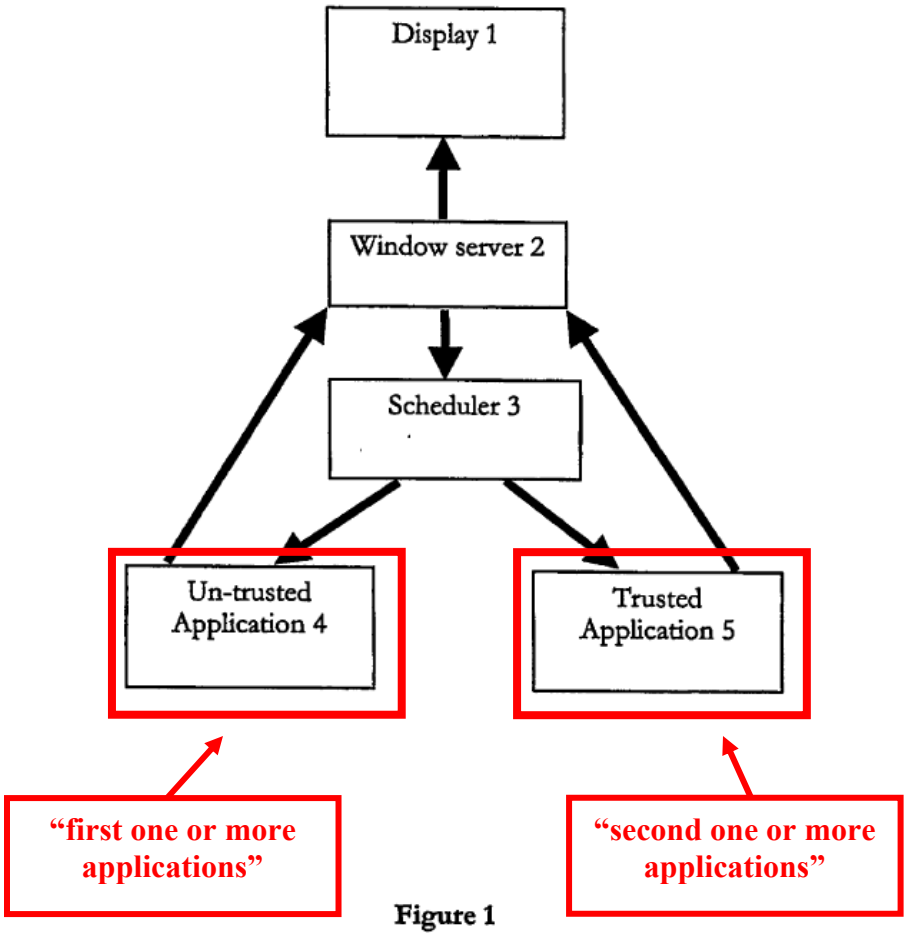
Further, in accordance with its policies, Rao's system selectively uses a filter to (i) allow network packets to be transmitted to the network or (ii) block the network packets from being transmitted to the network, either permanently or temporarily, thereby applying the polices to the Internet service access request embodied by those network packets. SAMSUNG-1005, [0191], [0194], [0207]; SAMSUNG-1003, ¶128. *See also* [1c]; §III.A.3. In at least some implementations, the filter also selectively determines which "types of packets to filter" based on "configuration settings" provided by the "agent 326." SAMSUNG-1004, [0104]; SAMSUNG-1003, ¶128.

To the extent that Rao does not expressly describe one or more of the features of [1d], these features nevertheless would have been obvious in view of Oestvall. SAMSUNG-1003, ¶129.

Like Rao, Oestvall describes an application-based priority system for controlling access to resources. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]; SAMSUNG-1003, ¶130. Further, Oestvall contemplates at least some of the same

criteria as Rao, and teaches that specific combinations of these criteria can be selected to achieve a specific technical benefit. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]; SAMSUNG-1003, ¶130.

Specifically, like Rao, Oestvall describes classifying applications into different types. SAMSUNG-1003, ¶131. In particular, Oestvall describes that applications can be classified with respect to "'trust' or certification criteria—i.e. criteria which define the level of trustworthiness of the application" (***a differential traffic control policy list***). SAMSUNG-1006, [0010]. For instance, applications can be classified as (i) "untrusted" applications (***distinguishing between a first one or more applications resident on the device***) and (ii) "trusted" applications (***... and a second one or more applications resident on the device***). SAMSUNG-1006, [0015], FIG. 1.



SAMSUNG-1006, FIG. 1 (annotated)

To the extent that Oestvall does not expressly describe representing these applications in the form of a list, a POSITA nevertheless would have found it obvious to implement such a list, as they would have recognized that a list is a commonplace format of syntax and/or language for enumerating data. SAMSUNG-1003, ¶132.

Further, like Rao, Oestvall describes that applications can be classified as "in

the background or foreground on [a] display" (***whether the application is classified as interacting with the user***). SAMSUNG-1006, [0023]; SAMSUNG-1003, ¶133 . *See also* [1c].

In addition, Oestvall describes applying a traffic control policy to an application differently, depending on these classifications. SAMSUNG-1003, ¶134. Specifically, Oestvall teaches selectively denying resources to applications based on these classifications ***(apply a differential traffic control policy to the Internet service access request***). SAMSUNG-1003, ¶134. For example, Oestvall's system denies resources to applications that are <u>not</u> sufficiently important to consume resources (e.g., such that those applications cannot "'poll[]' for data over a wireless network"), and provides resources to applications that <u>are</u> sufficiently important to consume resources (e.g., such that those applications can "'poll[]' for data over a wireless network"). SAMSUNG-1006, [0008], [0010], [0015]-[0017], [0022]-[0025].

As discussed in §III.A.3, a POSITA would have found it obvious to modify Rao's system of prioritizing network packets based on the specific application classification criteria taught by Oestvall, in order to achieve the specific technical benefit taught by Oestvall (e.g., reducing battery consumption in a network-enabled device). SAMSUNG-1003, ¶135.

As discussed in §III.A.3, according to this combination, Rao's "filter 322"

would selectively "discard" network packets from applications that are "untrusted" and running in the background (e.g., a classification of applications that should be assigned a low priority, as taught by Oestvall) (***apply a differential traffic control policy to the Internet service access request based on (i) the application being classified as not interacting with the user, and (ii) the application being a first one or more applications resident on the device).*** SAMSUNG-1003, ¶¶136-137. Thus, the network packets—and its corresponding Internet service access request—would be blocked permanently. SAMSUNG-1003, ¶137; §III.A.3 Accordingly, these applications can no longer poll for data over a wireless network (i.e., an activity that Oestvall teaches as being particularly burdensome on a battery). SAMSUNG-1006, [0024]; SAMSUNG-1003, ¶137.

Further, the "filter 322" would selectively allow the transmission of network packets from applications that are "trusted" (e.g., a classification of applications that should be assigned a high priority, as taught by Oestvall) (***apply a differential traffic control policy to the Internet service access request based on the application being a second one or more applications resident on the device***). SAMSUNG-1003, ¶138. Specifically, these network packets would be placed into a "highest priority queue," such that the network packets are immediately transmitted to the network (e.g., prior to the transmission of network packets placed into lower priority queues). SAMSUNG-1005, [0194]; SAMSUNG-1003, ¶138;

§III.A.3. Accordingly, applications that are sufficiently important can continue to exchange data in accordance with one or more Internet services. SAMSUNG-1003, ¶138.

An example implementation of the Rao-Oestvall system is shown in §III.A.3.c.

[1e]

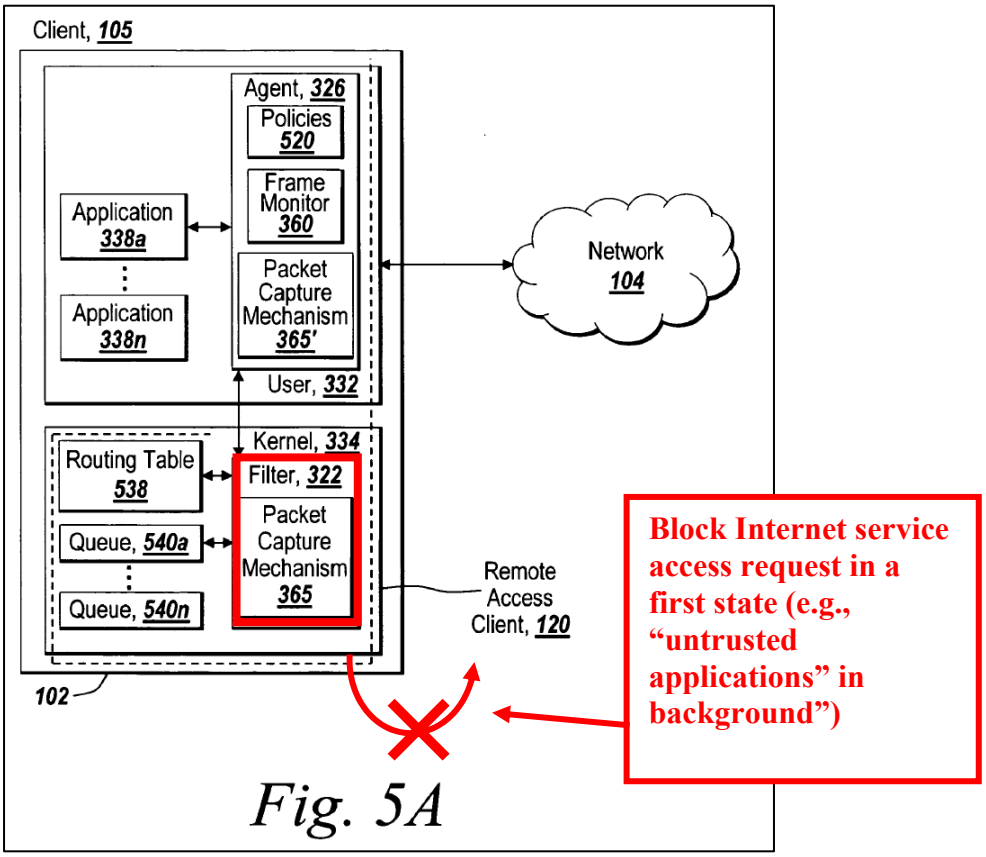
ROFC renders obvious [1e]. SAMSUNG-1003, ¶¶140-143.

As discussed in §III.A.3 and [1d], a POSITA would have found it obvious to modify Rao's system of prioritizing network packets based on the specific application classification criteria taught by Oestvall.

In particular, the "filter 322" would selectively "discard" network packets (***block the Internet service access request***) from applications that are "untrusted" (***in a first state wherein the particular application is one of the first one or more applications)*** and running in the background (***the particular application is not classified as interacting with a user in the device user interface foreground***) (e.g., a classification of applications that should be assigned a low priority, as taught by Oestvall). *See* §III.A.3; [1d]; SAMSUNG-1003, ¶142.

Thus, the network packets—and its corresponding Internet service access request—would be blocked permanently. SAMSUNG-1003, ¶143; §III.A.3. Accordingly, these applications can no longer poll for data over a wireless network

(i.e., an activity that Oestvall teaches as being particularly burdensome on a battery). *See* §III.A.3; [1d]; SAMSUNG-1006, [0024]; SAMSUNG-1003, ¶143.



SAMSUNG-1005, FIG. 5A (annotated)

[1f]

ROFC renders obvious [1f]. SAMSUNG-1003, ¶¶144-147.

As discussed with in §III.A.3 and [1d], a POSITA would have found it obvious to modify Rao's system of prioritizing network packets based on the specific application classification criteria taught by Oestvall. SAMSUNG-1003, ¶145.

Specifically, the "filter 322" would selectively allow the transmission of network packets from applications that are "untrusted" and running in the foreground

(***at least one other state in which the application is classified as interacting with the user in the device user interface foreground***) (e.g., a classification of applications that should be assigned a high priority, as taught by Oestvall). *See* §III.A.3; [1d]; SAMSUNG-1003, ¶146.

In particular, by virtue of the application now being in the foreground, these network packets would be placed into a "highest priority queue," thereby having their communication be unfettered as taught by Oestvall such that the network packets are immediately transmitted to the network (e.g., prior to the transmission of network packets placed into lower priority queues). SAMSUNG-1005, [0194]; SAMSUNG-1003, ¶147; §III.A.3. Indeed, in view of Oestvall, a POSITA would have found it obvious to treat untrusted application that are running in the background identically as trusted application (regardless if they are running in the foreground or the background), and would have treated network packets from each of these applications similarly. Accordingly, applications that are sufficiently important can continue to exchange data in accordance with one or more Internet services. *See* §III.A.3; [1d]; SAMSUNG-1003, ¶147.

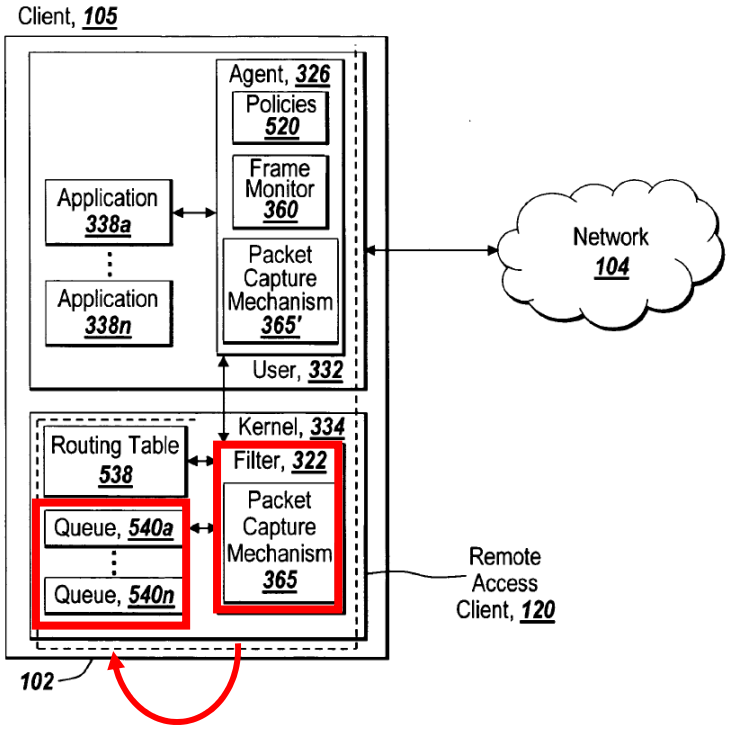


Fig. 5A

Allow Internet service access request in at least one other state (e.g., "untrusted applications" in foreground)

SAMSUNG-1005, FIG. 5A (annotated)

[1g]

ROFC renders obvious [1g]. SAMSUNG-1003, ¶¶148-152.

As discussed in §III.A.5, in view of Freund, a POSITA would have found it obvious to modify the Rao-Oestvall system to selectively enable an application to access a network (e.g., the Internet) based on the amount of network data that has been used by that application. §III.A.5; SAMSUNG-1003, ¶149.

An example implementation of the Rao-Oestvall-Freund system is shown in

§III.A.5.

As discussed in §III.A.5, according to this combination, a POSITA would have configured the "Supervisor" to instruct the "Client Monitor" to perform Freund's "bandwidth and interactive use monitoring" in accordance with a set of filter rules. SAMSUNG-1003, ¶¶150-152. According to these rules, the "Client Monitor" would:

(i) Intercept an application's requests to access the Internet (e.g., "Winsock ... calls" to a "communications driver") (SAMSUNG-1007, 29:17-30:9, FIG. 13A (1301)),

(ii) Determine the amount of Internet data that is transmitted and/or received by that application (e.g., "data lengths"), and tracks that amount of data (e.g., by "[a]dd[ing] the data lengths to a DataIn or DataOut accumulator or counter of the Application's list entry and global activity record") (***application-specific amount of Internet data usage***) (SAMSUNG-1007, 30:24-29, FIG. 13A (1302(D)), and

(iii) "[D]isable[] future Internet access" by that application if the amount of data exceeds a particular application-specific limitation (e.g., "[i]f the DataIn or DataOut fields exceed rule-based quantity either for the specific Application") (***disallow Internet data communication for that application based on an application-specific amount of Internet***

data usage reaching a limit) (SAMSUNG-1007, 30:24-29, FIG. 13A).

[2]

ROFC renders obvious [2]. SAMSUNG-1003, ¶¶[153]-[161].

As discussed in [1c], in ROFC, a device classifies "whether an application is running in the foreground or the background of the client 105," as taught by Rao. SAMSUNG-1005, [0182], [0188]-[0189]; [1c]; SAMSUNG-1003, ¶154. Further, Rao describes that, in at least some cases, "an application [that] is running in the foreground [is] currently in active use by the user." SAMSUNG-1005, [0003].

As also discussed in [1c]-[1d], in ROFC, the device performs this classification upon generating and intercepting a network packet by the application, in order to determine the priority of that network packet. *See* [1c]-[1d]; SAMSUNG-1003, ¶155].

Accordingly, a POSITA would have understood or found it obvious that, when the ROFC device classifies that "an application is running in the foreground ... of the client 105," this classification would be performed based on the *current state* of the application (e.g., at the time that the packet was generated and intercepted by the ROFC system, such that the network packet can be accurately prioritized). SAMSUNG-1003, ¶¶156-157. Specifically, this classification would be performed ***when a user of the device is directly interacting with that application***

(e.g., by engaging in "active use" of the application, as taught by Rao) and/or is ***perceiving any benefit from that application*** (e.g., by viewing the application as it is running in the foreground and/or perceiving that the application is ready for input by the user, as also taught by Rao). SAMSUNG-1005, [0003]; SAMSUNG-1003, ¶¶156-157.

As also discussed in [1c], Oestvall describes that the device uses a "window server component 2 ... to determine if an application is in the background or foreground on display." SAMSUNG-1005, [0008], [0016]-[0017], [0022]-[0023]; [1c]. Further, the device performs this classification upon an application requesting access to an Internet service. [1c]; SAMSUNG-1003, ¶158. Oestvall additionally describes that "[a] foreground application ... present[s] a user interface with which a user can interact." SAMSUNG-1006, [0006].

A POSITA would have understood or found it obvious that, when the ROFC device classifies that "an application is in the ... foreground on display," this classification would be performed based on the *current state* of the application. SAMSUNG-1003, ¶159. Specifically, this classification would be performed ***when a user of the device is directly interacting with that application*** (e.g., by interacting with a user interface of the application, as taught by Oestvall) and/or is ***perceiving any benefit from that application*** (e.g., by viewing the user interface as it is running in the foreground and/or perceiving that the application is ready for input by

the user via a presented user interface, as also taught by Oestvall). SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶159.

Further, techniques for adapting the prioritization for an application or otherwise impacts its operation based on the application's direct user interaction were well-known by the Critical Date. SAMSUNG-1003 ¶¶160-161; SAMSUNG-1011, 9:33-35; SAMSUNG-1007, 10:16-44.

[3]

ROFC renders obvious [3]. SAMSUNG-1003, ¶¶162-168.

As discussed in [1c], in ROFC, the device classifies "whether an application is running in the foreground or the background of the client 105," as taught by Rao. SAMSUNG-1005, [0182], 0188]-[0189]; [1c]; SAMSUNG-1003, ¶163.

Further, Oestvall describes that an application's user interface can have different ***states of user interface priority***, depending on whether it is in the foreground or the background. SAMSUNG-1006, [0006]. For instance, when the application is in the background, the user interface has a low state of priority, such that the user interface is relegated to an icon (e.g., "[a]n application is in the background if it is not being interacted with by an end-user and it presents no user interface with which a user could interact (but it could for example present an icon indicating its presence and the fact that it was still active)"). SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶¶164-165.

Further, when the application is in the foreground, the user interface has a high state of priority, such that the user interface is presented to the user for interaction (e.g., "A foreground application conversely does present a user interface with which a user can interact."). SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶166.

A POSITA would have understood or found it obvious that, when the ROFC device classifies "whether an application is running in the foreground or the background of the client 105," this classification could be efficiently implemented ***based on a state of a user interface priority of that application*** (e.g., by assessing the state of the user interface priority for the application, such as whether the application's user interface is visible, is available for interaction with a user, and/or is represented by a mere icon, as taught by Oestvall). SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶167. Moreover, the use of states of user interface priority in coordinating application operation was well known before the Critical Date and a POSITA would have found obvious the use of states of user interface priority for classification in Rao-Oestvall. SAMSUNG-1003, ¶[168]; SAMSUNG-1011, 9:19-35).

[16]

[4]

ROFC renders obvious [4]. SAMSUNG-1003, ¶¶169-177.

As discussed in [1c], in ROFC, the device classifies "whether an application is running in the foreground or the background of the client 105," as taught by Rao. SAMSUNG-1005, [0182], [0188]-[0189]; 1[c]; SAMSUNG-1003, ¶¶170-171.

Further, as discussed in [1c], Rao contemplates that applications that are running in the background may perform at least some Internet service activities, such as by generating network packets while running in the background ("***providing or utilizing a background data service***"). [1c]; SAMSUNG-1003, ¶173. For example, a POSITA would have understood or found it obvious that Rao's email application can use a background data service of the device (e.g., a network stack of the device) in order to poll an email server for updates and/or retrieve emails in the background. SAMSUNG-1005, [0003], [0090]; [1c]; SAMSUNG-1003, ¶173.

As discussed in [1c] and [2] POSITA would have understood or found it obvious that, when the ROFC device classifies that "an application is running in... the background of the client 105," this classification would be performed based on the *current state* of the application. SAMSUNG-1003, ¶¶172-174. Specifically, this classification would be performed ***when the application is providing or utilizing a background data service*** (e.g., by generating network packets in the background, as taught by Rao). SAMSUNG-1005, [0003], [0090]; [1c]; SAMSUNG-1003, ¶174.

As also discussed in [1c], Oestvall describes that the device uses a "window

server component 2 ... to determine if an application is in the background or foreground on display." SAMSUNG-1006, [0008], [0016]-[0017], [0022]-[0023]; [1c]; SAMSUNG-1003, ¶175. Further, in ROFC, the device performs this classification upon an application requesting access to an Internet service. [1c]; SAMSUNG-1003, ¶175.

Further, as also discussed in [1c], Oestvall describes that an application can perform network activities, and that applications may be capable of consuming "resources" when in the background (***providing or utilizing a background data service***). SAMSUNG-1006, [0023]-0024]; [1c]; SAMSUNG-1003, ¶176.

A POSITA would have understood or found it obvious that, when the ROFC device classifies that "an application is in the background," this classification would be performed based on the *current state* of the application (e.g., at the time that the packet was generated and intercepted by the ROFC device). SAMSUNG-1003, ¶177. Specifically, this classification would be performed ***when the application is providing or utilizing a background data service*** (e.g., by performing network activities and/or consuming resources when in the background, as taught by Oestvall). SAMSUNG-1006, [0023]-0024]; [1c]; SAMSUNG-1003, ¶177.

[5]

ROFC renders obvious [5]. SAMSUNG-1003, ¶¶178-182.

As discussed in §III.A.3, [1d], and [1e], the ROFC device can prioritize the

captured packets by blocking network packets from being transmitted to the network, either permanently or temporarily. §III.A.3; [1d]; [1e]; SAMSUNG-1003, ¶179. In particular, as discussed in §III.A.3, a POSITA would have found it obvious to configure the Rao-Oestvall system to selectively block network packets temporarily, in at least some situations where more granular control of battery draining activities is desired. §III.A.3; SAMSUNG-1003, ¶¶179-182.

For example, Rao describes that its system can block network packets from being transmitted to the network temporarily, by "preventing ... at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application." SAMSUNG-1005, [0040]. In particular, a client can "hold[] ... in the queue a network packet associated with the second application" (***delay network activity in associate with the first Internet access request***), and "releas[e] the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet" (***until a second Internet access request is received and allowed***). SAMSUNG-1005, [0040], [0194]. As Rao explains, "holding" network packets in this manner can be beneficial in "provid[ing] a packet by packet prioritization across all applications ... and intercepted network packets" and to implement prioritization according to different levels of "granularity." SAMSUNG-1005, [0191].

[6]

ROFC renders obvious [6]. SAMSUNG-1003, ¶¶183-189.

As described in [1d], in ROFC, a device would apply a differential traffic control policy to the Internet service access request. [1d]; SAMSUNG-1003, ¶184. For example, Rao contemplates prioritizing network packets by implementing one or more policies for controlling network traffic (***a differential traffic control policy***). SAMSUNG-1005, ¶[0182]; [1d]; SAMSUNG-1003, ¶185.

Further, Rao describes that a system can "provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies" (***a user interface ... to inform the user of the device when there are options to set, control, override, or modify at least one aspect of the differential traffic control policy and/or the differential traffic control policy list***). SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶186.

A POSITA would have understood or found it obvious that the ROFC device provides a user interface that enables a user to set, control, override, and/or modify one or more aspects of Rao's policies, in order to provide a user with a greater degree of control over the manner in which network packets are prioritized. SAMSUNG-1003, ¶187. Indeed, user interfaces for configuring the types of policies described in Rao were well-known before the Critical Date. SAMSUNG, ¶¶188-189; SAMSUNG-1007, FIG. 7A, 24:16-20, 25:1-13.

[13]

ROFC renders obvious [13]. SAMSUNG-1003, ¶¶190-194.

As described in [1d], in ROFC, a device would apply a differential traffic control policy to the Internet service access request. [1d]; SAMSUNG-1003, ¶191. For example, Rao contemplates prioritizing network packets by implementing one or more policies for controlling network traffic (***a differential traffic control policy***). SAMSUNG-1005, [0182]; [1d]; SAMSUNG-1003, ¶192.

Further, Rao describes that these policies "may be provided by or downloaded via a gateway." SAMSUNG-1005, [0183]. For example, "[t]he policies 520 may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium, such as electronically by one or more network packets or via a file, such as an XML file." SAMSUNG-1005, [0183].

In view of Rao, POSITA would have understood or found it obvious that a device can specify at least some of its policies, such as adding new policies (***update at least a portion of the differential traffic control policy and/or the differential traffic control policy list***), by downloading and implementing policies from a gateway, such as in the form of a network packet or file (***information received from a network element***). SAMSUNG-1003, ¶¶193-194. For example, a POSITA

would have recognized that such a configuration would allow for centralized control and/or remote administration of multiple devices in prioritizing network packets, and/or would allow devices to maintain up-to-date policies with which to prioritize network packets. SAMSUNG-1003, ¶194.

[18]

ROFC renders obvious [18]. SAMSUNG-1003, ¶¶195-201.

As discussed in [1d] and [1e], the ROFC device ***blocks the Internet service access request*** in a first state in which the particular application is one of the first one or more applications, and the particular application is not classified as interacting with a user in the device user interface foreground. [1d]-[1e]; SAMSUNG-1003, ¶¶196-198.

Further, Rao describes that the device includes a "network stack 310" that "include[s] one or more network drivers." SAMSUNG-1005, [0100], FIG. 1C. Further, Rao describes that network packets can be communicated "via a secure socket layer." SAMSUNG-1005, [0035].

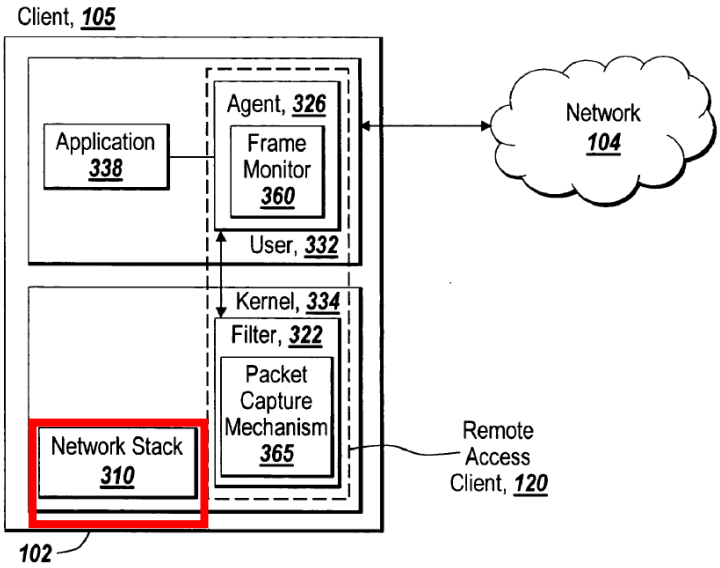


Fig. 1C

SAMSUNG-1005, FIG. 5A (annotated)

Rao teaches that the device "may intercept network packets of one or more applications 338 a-338 n transparently to the application 338 a-338 n ... and any of the network layers of a network stack." SAMSUNG-1005, [0185]. Rao teaches that such a blocking technique is beneficial in that it allows the prioritization technique to "support any type of application 338 a-338 n on the client 105." SAMSUNG-1005, [0185].

In view of Rao, a POSITA would have understood or found it obvious that the ROFC device enables applications to transmit network packets to a remote server on the Internet by transmitting requests to a network stack. SAMSUNG-1003, ¶¶199-201. Further, a POSITA would have understood or found it obvious

that such requests could include requests to the network stack to open, connect to, and/or write data to a socket (e.g., using the "secure socket layer") (***open, connect, and/or write requests by the particular application to a network stack***). SAMSUNG-1003, ¶201. Further, in view of Rao, a POSITA would have understood or found it obvious to selectively block such requests to the network stack (***selectively block the Internet service access request by intercepting open, connect, and/or write requests by the particular application to a network stack)***, as performing such an operation would allowing Rao's prioritization technique to "support any type of application" on a device, as taught by Rao. SAMSUNG-1003, ¶201.

B. [GROUND 2] – Claims 10-12, 14-17, and 19-20 are rendered obvious by Rao, Oestvall, Freund, and Araujo

1. Overview of Araujo

Araujo describes "a power-management policy" for managing a "machine's power usage." SAMSUNG-1008, Abstract; SAMSUNG-1003, ¶¶202-209. Araujo's device classifies programs with respect to various criteria, and selectively provides resources to the programs based on their classifications. SAMSUNG-1008, [0027]. In particular, the device determines "[w]hether a program is permitted to consume power ... based on a finding as to whether the program's status justifies the consumption of power under the circumstances that are present." *Id.* For example, programs "may have a status that reflects its worthiness to consume

power," such as a "'VIP' status that allows them to consume power in situations where other programs would not." *Id.*

Further, the device provides resources to the applications differently, based on whether the applications are "worthy" to consume power. *Id.,* [0024]. For example, a program can generate "a request to perform an action using a particular device," such as "a request to send data over a wireless network" using a "wireless network card." *Id.,* [0020], [0024]. In response, the device selectively performs various operations with respect to the request, including "[a]llowing" or "[b]locking" the request based on a power management policy. *Id.*, [0035], [0050], FIG. 3 (302), FIG. 4 (406).

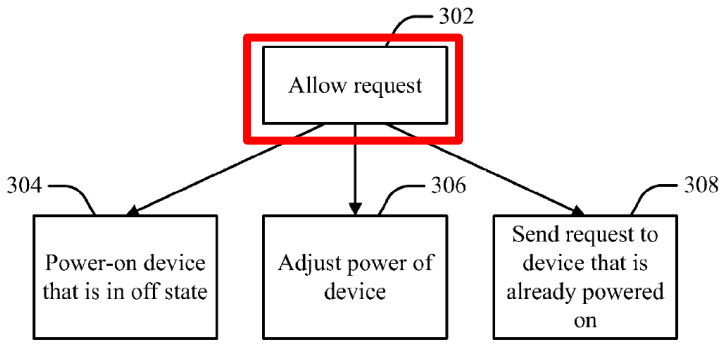


FIG. 3

SAMSUNG-1008, FIG. 3 (annotated)

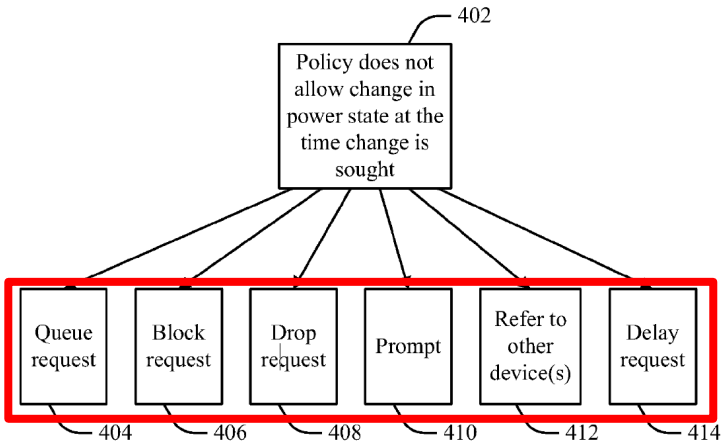
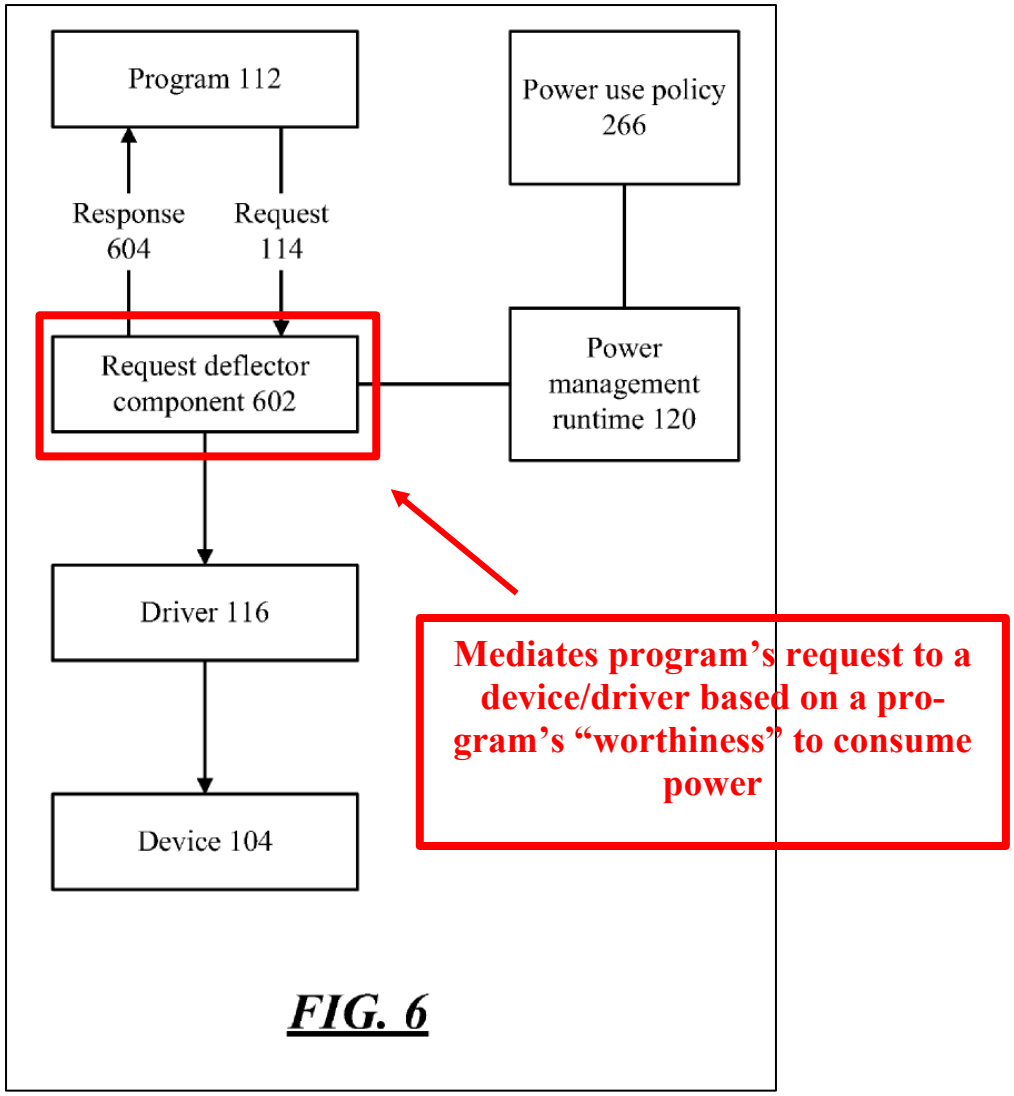


FIG. 4

SAMSUNG-1008, FIG. 4 (annotated)

Specifically, Araujo describes selectively allowing or blocking a request using a "request deflector component" that is "interposed" between a "program" and a "driver" of a "device," and configured to "intercept[] requests and respond[] to the requests based on power management considerations before the request reach a device driver." *Id.,* [0024], [0050]. In particular, if "[a] request 114 may be carried out under [a] power policy, then request deflector component 602 passes the request along to driver 116. Otherwise, request deflector component may permanently or temporarily deflect the request from reaching driver 116." *Id.*



SAMSUNG-1008, FIG. 6 (annotated)

That is, Araujo's device selectively allows a program's request when it deems that the program is sufficiently important to consume resources (e.g., "worthy" programs, such as "VIP" programs), while selectively denying the program's request when it deems that the program is not sufficiently important to consume resources (e.g., programs that are not "worthy," such as non-"VIP" programs). SAMSUNG-1003, ¶208.

Araujo's "power-management policy" can be used to "justify [a program] consuming power, depending on what the program is doing." SAMSUNG-1008, [0004]. Accordingly, a device implementing Araujo's policy can better "use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge." *Id.,* [0001].

2. Combination of Rao-Oestvall-Freund and Araujo

A POSITA would have found it obvious to modify the ROFC system to include Araujo's "request deflector component" in order to allow the ROFC system to better "use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge." SAMSUNG-1008, [0001]; SAMSUNG-1003, ¶¶210-215; §III.B.1. This modification would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way. *See KSR Int'l Co. v. Teleflex Inc.,* 550 U.S. 398, 415-421, 82 USPQ2d 1385, 1395-97 (2007)*; MPEP 2143*; SAMSUNG-1003, ¶¶210-215.

As discussed in §III.A.3, the ROFC system controls each of the applications' access to the network by intercepting packets of network traffic by the applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network

based on the determined priority. §III.A.3. As taught by Rao, these operations can be performed, at least in part, by one or more "network drivers of a network stack 310" (e.g., by "customiz[ing], modifi[ng] or adapt[ing]" the network drivers "to provide a custom or modified portion of the network stack 310 in support of any of the techniques" described in Rao). SAMSUNG-1005, [0100]. As an example, the ROFC system can include "[a] filter 322 [to] place, arrange, or coordinate network packets into queues 540 a-540 n in support of the priorities," and these "queues 540 a-540 n may be included in a network driver, such as an NDIS driver for the filter 322." *Id.*, [0143], [0180], [0191].

In view of Araujo, a POSITA would have understood that an application's request to the network driver (e.g., including network packets for transmission to a network) can be intercepted and mediated by a "request deflector component" that is "interposed" between each application and the network driver, in order to selectively allow or block an application from transmitting data to the network. SAMSUNG-1008, ¶[0050]; SAMSUNG-1003, ¶¶211-212. In particular, a POSITA would have understood or recognized that incorporating Araujo's "request deflector component" into the ROFC system would allow the ROFC system to determine whether each of the applications has a "status [that] justifies the consumption of power under the circumstances that are present," and selectively block or allow requests by those applications based on the determination. SAMSUNG-1008,

[0027]; SAMSUNG-1003, ¶212. Accordingly, the ROFC system can better "use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge." SAMSUNG-1008, [0001].

As an example of this modification, a POSITA would have "interposed" Araujo's "request deflector component" between the ROFC's applications and the network driver that implements Rao's packet prioritization functionality (e.g., a network driver implementing the packet capture mechanism 364, filter 322, and queues 540a-540n). SAMSUNG-1003, ¶213. As one example, a POSITA would have arranged the Araujo's "request deflector component" to process network packets after an application's requests has otherwise been allowed by Freund's "Client Monitor" to perform a further assessment of whether the application can access the network (e.g., in addition to considering whether an application has exceeded application-specific data limitations) in order to further enhance the efficiency of the ROFC system. SAMSUNG-1003, ¶213.

Further, a POSITA would have configured to the "request deflector component" to determine whether each of the applications has a "status [that] justifies the consumption of power under the circumstances that are present," and selectively allow or block the request and, hence, the network packets from proceeding to the network driver based on the determination. SAMSUNG-1003, ¶214. Upon deter-

mining that the application's status justifies the consumption of power, the "request deflector component" can allow the request, and hence, the network packets to proceed to the network driver for prioritization (see step 1.5a below). SAMSUNG-1003, ¶214. Alternatively, upon determining that the application's status does not justify the consumption of power, the "request deflector component" can block the request and, hence, the network packets from reaching the network driver, either permanently or temporarily (see step 1.5b below). SAMSUNG-1003, ¶214. Accordingly, the "request deflector component" would provide an additional layer of control for regulating each of the applications' access to the network (e.g., to supplement the functionality taught by Rao, Oestvall, and Freund). SAMSUNG-1003, ¶214.

An example modification to the Rao-Oestvall-Freund system in view of Araujo's teachings ("Rao-Oestvall-Freund-Araujo system") is shown below.

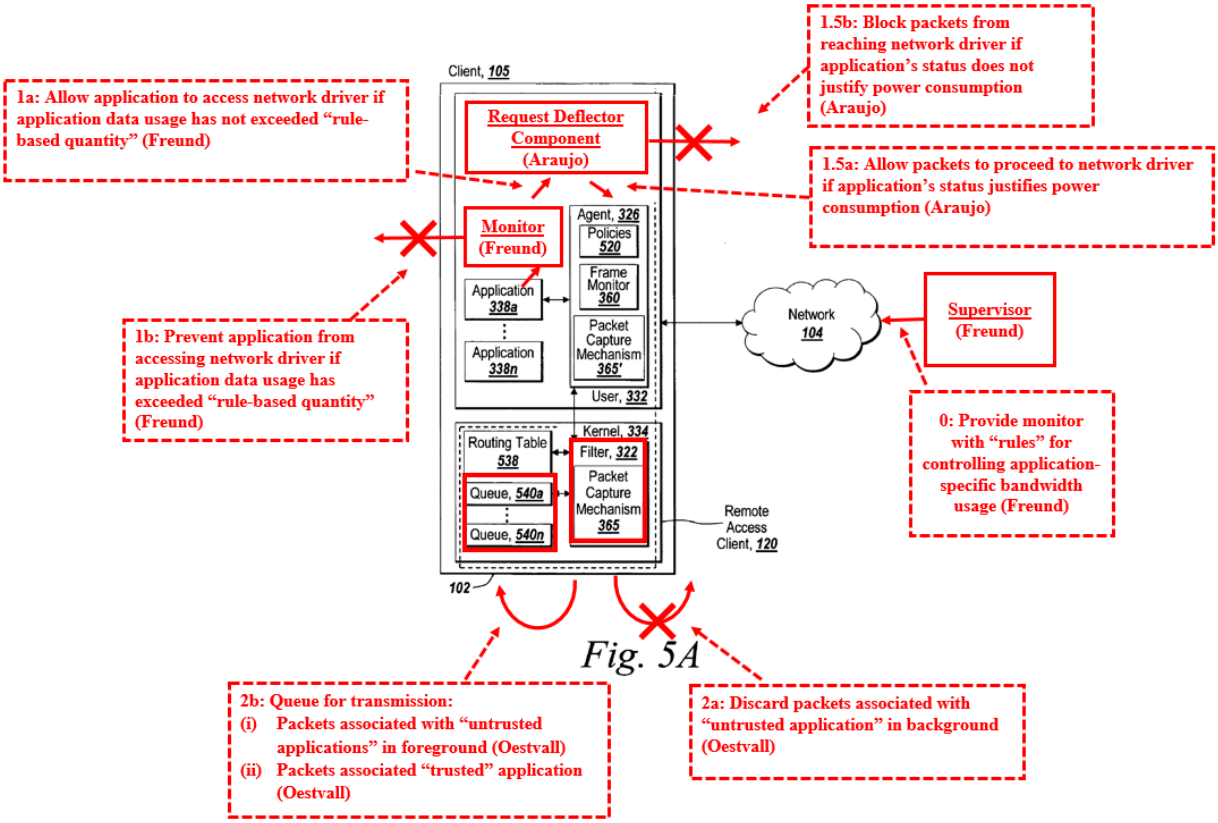


Fig. 5A

Rao's FIG. 5A (revised and annotated)

3. Analysis

[10], [12]

ROFAC renders obvious [10], [12]. SAMSUNG-1003, ¶¶216-221, ¶¶227-231.

As discussed in [1d] and §III.B.2, the ROFAC system would use a network driver to apply ***a differential traffic control policy*** to the Internet service access request.

Further, as modified by Araujo, the ROFAC system would selectively allow network packets to proceed to the network driver for prioritization (***dynamically***

change a determination of whether to apply the differential traffic control policy). §III.B.2; SAMSUNG-1003, ¶¶218-229. As Araujo teaches, this configuration allows the ROFAC system to determine whether each of the applications has a "status [that] justifies the consumption of power under the circumstances that are present." SAMSUNG-1008, [0027].

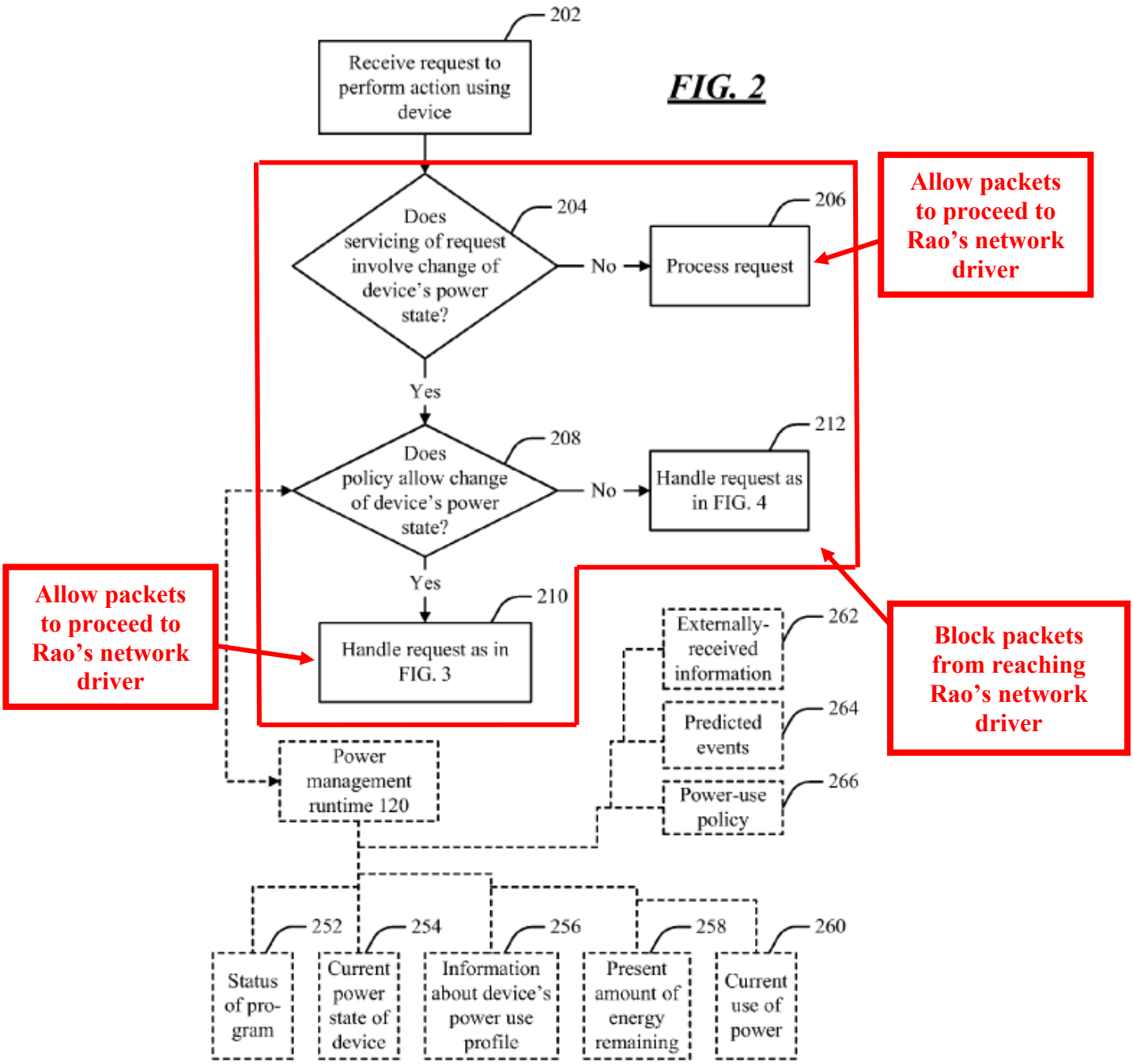
An example configuration of the ROFAC system is shown in §III.B.2 above. Specifically, in the ROFAC system, Araujo's "request deflector component" would be "interposed" between the applications and the network driver that implements Rao's packet prioritization functionality. §III.B.2; SAMSUNG-1003, ¶219. Further, the "request deflector component" would selectively allow or block an application's network packets—representing an Internet service access request by that application—from reaching the network driver based on whether that application is considered sufficiently important to consume power. §III.B.2; SAMSUNG-1003, ¶219.

A modified by Araujo, the ROFAC system would determine whether to allow an application's request to proceed to the network driver based on a device's power state, such as the power state of the device's network card or WWAN modem (***...based on a power state of the device [10]***). SAMSUNG-1008, FIG. 2 (204), [0025]; SAMSUNG-1003, ¶¶[229]-[221]. Specifically, this configuration would enable the ROFAC system to account for whether a device's components

"may already be powered on and/or in an appropriate power state" in order to better regulate power consumption by the device. SAMSUNG-1008, [0037]. For example, if a device's network card or WWAN modem are already powered on and/or is "in an appropriate power state," the ROFAC system determines that an application's use of those components "does not affect power management," and selectively allows the application's network packets to proceed to the network driver in order to service the application's request. *Id*; SAMSUNG-1003, ¶¶220-221.

In particular, the ROFAC system would determine whether to allow an application's request to proceed to the network driver based on power control state changes for a device, such as a network card or WWAN modem (***...based on power control state changes for the WWAN modem, [12]***). SAMSUNG-1003, ¶¶ 230-231. For example, as shown in FIG. 2, if servicing the application's request would not involve a change in the power state of the device's components, the ROFAC system would process the request and "proceed[s] as normal." SAMSUNG-1008, FIG. 2 (206), [0025]. Accordingly, the network packets representing the request would be forwarded to the network driver for prioritization. SAMSUNG-1003, ¶221. In contrast, if servicing the request would involve a change in the power state of the device's components, the ROFAC system determines whether a policy would allow a change of the device's power state, and selectively

(i) allows the request and transmits the network packets to the network driver (e.g., as shown in FIG. 3) (SAMSUNG-1008, FIG. 2 (210), FIG. 3, ¶[0035]), or (ii) queues the request, blocks the request, drops the request, delays the request, and/or refers the request to another device, thereby blocking the network packets from reaching the network driver, either permanently or temporarily (e.g., as shown in FIG. 4) (*id.*, FIG. 2 ((212), FIG. 3; ¶[0035]; SAMSUNG-1003, ¶231).



SAMSUNG-1008, FIG. 2 (annotated)

[11]

ROFAC renders obvious [11]. SAMSUNG-1003, ¶¶222-226.

As discussed in [1d] and §III.B.2, the ROFC system would use a network driver to ***apply a differential traffic control policy*** to the Internet service access request. Further, as modified by Araujo, the ROFAC system would selectively allow network packets to proceed to the network driver for prioritization (***dynamically change a determination of whether to apply the differential traffic control policy***). §III.B.2; SAMSUNG-1003, ¶¶224. *See also* [10].

As modified by Araujo, the ROFAC system would determine whether to allow an application's request to proceed to the network driver based on ***the state of usage of the device***, such as:

(i) the "[s]tatus of program" that is being used by a user (SAMSUNG-1008, [0027], FIG. 2),

(ii) the "[c]urrent power state of the device" (*id.*, [0028], FIG. 2), and/or

(iii) "[p]resent use of power" by the device (*id.*, [0031], FIG 2).

As Araujo explains, each of these factors reflects an application's "worthiness to consume power" in a given situation. *Id.,* [0027]. Accordingly, by mediating an application's request based on factors that reflect the use of the device and/or the "programs" stored thereon, the ROFAC system can better "use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge." *Id.*, [0001]; SAMSUNG-1003, ¶226.

[14]

ROFAC renders obvious [14]. SAMSUNG-1003, ¶¶232-234.

As discussed in [10], if servicing a request would involve a change in a device's power state (e.g., the power state of a network card or WWAN modem), the ROFAC system determines whether a policy would allow a change of the device's power state. SAMSUNG-1008, FIG. 2 (210), FIG. 3, [0035]. If the policy would not allow such a change, the ROFAC system would block the network packets from reaching the network driver, either permanently or temporarily (e.g., as shown in FIG. 4). *Id.,* FIG. 2 (212, FIG. 3, [0035]; SAMSUNG-1003, ¶234. Accordingly, the power state of the network card or WWAN modem would remain unchanged (***when the Internet service access request is blocked, prevent the first Internet access request from causing a change to a power state of the modem***). SAMSUNG-1003, ¶234.

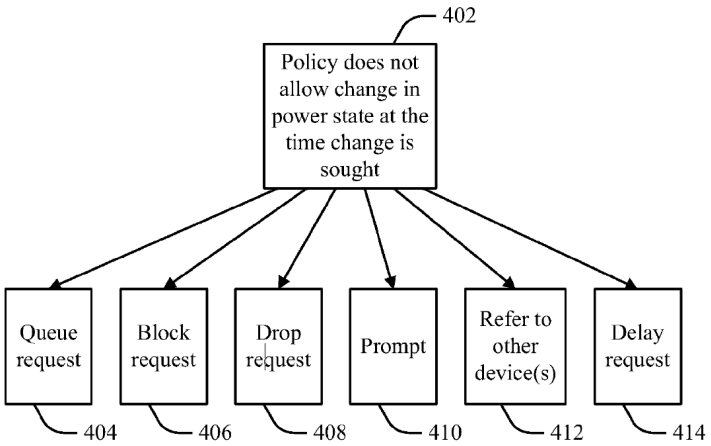


FIG. 4

SAMSUNG-1008, FIG. 4

[15]

ROFAC renders obvious [15]. SAMSUNG-1003, ¶¶235-238.

Araujo describes that a device (e.g., a network card or WWAN modem) can operate according to an "idle" mode (***power state of the modem is idle or sleeping***). SAMSUNG-1008, [0021]. Further, as discussed in [10], if servicing a request would involve a change in the device's power state (e.g., from "idle" to an actively used state), the ROFAC system determines whether a policy would allow a change of the device's power state. *Id.*, FIG. 2 (210), FIG. 3, [0035]. If the policy would not allow such a change, the ROFAC system can "queue" the request, such that is "processed at some later time." *Id.,* [0039], FIG. 4, block 404. "[I]f at some later time the power management policy allows the device to be turned on, then the program's request may be dequeued and processed." *Id.,*

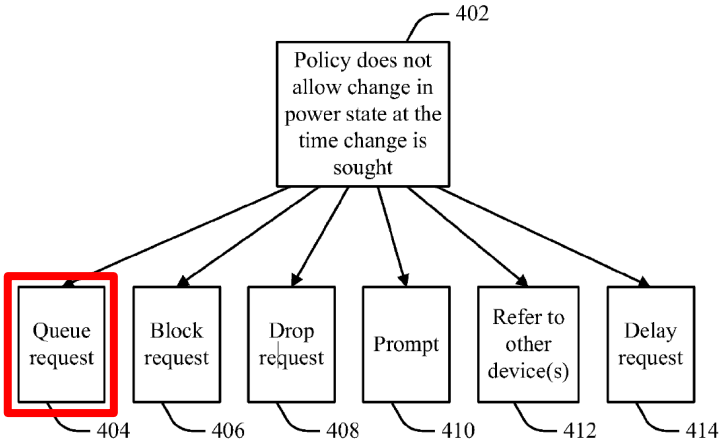


FIG. 4

SAMSUNG-1008, FIG. 4 (annotated)

A POSITA would have recognized that, a queued request would be delayed until the request to use the device (or another subsequent request) is allowed. SAMSUNG-1003, ¶238. Upon allowance of such a request, the device's power state would change from "idle" to an actively used state (***when the power state of the modem is idle or sleeping, prevent power state changes to the modem until an Internet service access request is allowed***). SAMSUNG-1003, ¶238.

[16]

ROFAC renders obvious [16]. SAMSUNG-1003, ¶¶239-242.

As discussed in [10], Araujo explains that "if the power state change is not allowable under the policy," the device can "block the request" and "notif[y] [the program] that the request will not be processed." SAMSUNG-1008, [0038], [0041]. Further, "[t]he program may also be notified that the reason for the request is that the device is off. For example, the program may receive an error code or result code indicating that the request calls for a device that is not turned on" (***when the Internet service access request is blocked, instruct the first end-user application to transition to a different state***). *Id., See also id.*, [0017] ("a program could be notified that a request to use a device is not being put through to the device because the request would be contrary to power-usage policy.")

In view of Araujo, a POSITA would have understood or found it obvious that, when the request is blocked, the ROFAC system instructs an application to

transition to a different state (e.g., from a state in which the application is making a request to a state in which the application's request is blocked either permanently or temporarily, as taught by Araujo). SAMSUNG-1003, ¶¶241-242. In particular, a POSITA would have understood or found it obvious that a device can provide an application with instructions to transition to a different state (e.g., a state in which the application is idle or is waiting for a request to be allowed) by transmitting an error code or result code indicating that the request calls for a device that is not turned on, as taught by Araujo. SAMSUNG-1003, ¶242. Such a configuration would allow a system to control the manner in which power is consumed by a device according to a greater degree of granularity (e.g., by selectively controlling the manner in which an application's request is denied), as taught by Araujo. SAMSUNG-1003, ¶242.

[17]

ROFAC renders obvious [17]. SAMSUNG-1003, ¶¶243-247.

As discussed in [10], Araujo explains that "if a power state change is not allowable under a policy," the system can generate "a dialog box ... on a display that informs the person in front of the display that the card is off." SAMSUNG-1008, [0041].

In view of Araujo, a POSITA would have understood or found it obvious that a system can present information to a user regarding a blocked Internet service

access request, thereby modifying and/or replacing what was previously displayed on the user interface (***block, modify, remove, or replace user interface messages generated by the particular application based on the block of the Internet service access request***). SAMSUNG-1003, ¶¶244-246. For instance, this would allow the system to alert the user to changes in the operation of the device and/or to provide the user with a greater degree of control over the device, as taught by Araujo. SAMSUNG-1003, ¶246.

Further, in view of Araujo, a POSITA would have understood that this functionality can be provided, at least in part, using "[s]oftware ... stored in [a] data remembrance component(s) 704)" and "execute[d] on ... one or more processor(s) 702) (***agent***). SAMSUNG-1008, ¶[0055]; SAMSUNG-1003, ¶247.

[19]

ROFAC renders obvious [19]. SAMSUNG-1003, ¶¶248-254.

As discussed in §III.B.2, the ROFAC system would include Araujo "request deflector component" to "intercept[] requests and respond[] to the requests based on power management considerations before the request reach a device driver." SAMSUNG-1008, [0024], [0050].

Specifically, Araujo explains that "if the power state change is not allowable under the policy," the device can "block the request" and "notif[y] [the program]

that the request will not be processed." SAMSUNG-1008, [0038], [0041]. Further, "[t]he program may also be notified that the reason for the request is that the device is off. For example, the program may receive an error code or result code indicating that the request calls for a device that is not turned on." *Id., See also id.*, [0017].

In view of Araujo, a POSITA would have understood or found it obvious that a system can respond to an intercepted request by the particular application by notifying the application that the request will not be processed and/or transmitting an error code or result code to the application (***respond to an intercepted request by the particular application***). SAMSUNG-1003, ¶¶248-251. In doing so, the system would provide an application with a greater degree of information regarding its attempt to access a network, as taught by Araujo. SAMSUNG-1003, ¶251.

Further, a POSITA would have found it obvious to notify the application by emulating conventional network messages, such as those generated by an Application Programming Interface (API) for facilitating network access for applications (***...by emulating network messaging)***, as doing so would provide functionality in a manner that is transparent to the application, thereby providing support for any type of application (e.g., as taught by Rao). SAMSUNG-1003, ¶¶252-255. *See also* SAMSUNG-1012, 1-20.

Araujo's use of an "error code or result code" is also consistent with the

specification of the '184 Patent, which describes that "an emulated network API" can block an application's connection attempt and send "a message ... back to the application" regarding the blocking, such as a "message that the application will understand and can interpret to indicate that the network access attempt was not allowed/blocked, that the network is not available, and/or to try again later for the requested network access." SAMSUNG-1001, 91:25-49; SAMSUNG-1003, ¶256.

[20]

ROFAC renders obvious [20]. SAMSUNG-1003, ¶¶257-260.

As discussed in §III.B.2, the ROFAC system would include Araujo's "request deflector component" to "intercept[] requests and respond[] to the requests based on power management considerations before the requests reach a device driver." SAMSUNG-1008, [0024], [0050]. Further, as discussed in [19], the ROFAC system would notify an application that a request will not be processed and/or transmit an error code or result code to the application by emulating conventional network messages (***emulating network messaging***).

A POSITA would have understood or recognized that, in blocking the request from reaching the network driver, the ROFAC system would block the request from passing to Rao's "network stack" (which includes "one or more network drivers supporting the one or more layers" of the network stack) (***responding to a network request from the particular application by blocking the request from***

passing to a network stack). SAMSUNG-1005, ¶[0100]; SAMSUNG-1003, ¶¶258-259.

Further, A POSITA would have understood or recognized that, in notifying an application that a request will not be processed and/or transmitting an error code or result code to the application, the ROFAC would ***return to the particular application a message indicating the network request was not successful***. SAMSUNG-1008, [0038], [0041]; SAMSUNG-1003, ¶260. *See also* SAMSUNG-1008, [0017].

IV. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. 35 U.S.C. §325(d) – *Discretionary Denial under 325(d) is not warranted*

Discretionary denial under the Board's §325(d) *Advanced Bionics* analysis is not warranted. *See Advanced Bionics, LLC v. Med-El Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, 8-9 (PTAB Feb. 13, 2020) (precedential) ("*Advanced Bionics"*).

None of the prior art references advanced in this Petition was previously before the Office. While a relative of Rao (PCT application WO 2006/012610A2 ("Rao-2") was cited on the face of the '184 Patent, there is no evidence that the Office substantively considered this reference among the references listed on the first 11 pages of the '184 Patent. *See, generally,* SAMSUNG-1002. Moreover, the

Headwater Ex. 2004
Samsung v. Headwater
IPR2023-01362

same or substantially the same arguments were not previously presented to the Office. *Id.* Indeed, there could be no overlap between the arguments made before the Office because the Examiner issued no prior art rejections during prosecution.

To the extent it is argued that the same or substantially the same art or arguments were previously presented to the Office, the second prong is not met. *Advanced Bionics*, 8-10. The Examiner issued no prior art rejections and included no substantive discussion of any prior art reference. *See, generally,* SAMSUNG-1002. Therefore, although Rao-2 was cited on the face of the '184 Patent, neither Rao nor Rao-2 nor the obviousness of the Challenged Claims in view of those references was ever addressed during prosecution. As highlighted in Grounds 1 and 2, the Examiner clearly did not appreciate Rao's disclosures and how those references in combination and in combination with other prior art references not previously before the Office (Oestvall, Freund, and Araujo) render the Challenged Claims obvious. Moreover, Petitioner has shown a reasonable likelihood that it would prevail that at least one of the Challenged Claims is unpatentable over the applied art based on the current record. *Supra* §IIIA-E; *see Tokyo Ohka Kogyo Co., Ltd. v. Fujifilm Elec. Materials U.S.A., Inc.*, PGR2022-00010, Paper 9, 8-9 (PTAB June 6, 2022). As such, Petitioner has demonstrated material error by the Office, and discretionary denial is not warranted.

B. 35 U.S.C. §314(a) – Discretionary Denial is not Merited in view of Petitioner's *Sotera* Stipulation

In *Apple Inc. v. Fintiv, Inc.*, the Board enumerated six factors to determine whether a petition should be discretionarily denied institution under §314(a). IPR2020-00019, Paper 11 at 2-3 (PTAB "precedential" Mar. 20, 2020) ("*Fintiv*"). In June 2022, the USPTO issued updated discretionary denial guidance in view of the *Fintiv* factors and expressly noted that ***the PTAB will not discretionarily deny institution if Petitioner presents a Sotera stipulation***. SAMSUNG-1015, 3, 7-8. Here, Petitioner has eliminated any risk of duplicated effort by voluntarily presenting a *Sotera* stipulation to Patent Owner. SAMSUNG-1016; *Sotera Wireless, Inc. v. Masimo Corp.,* Case IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020). For at least this reason, the Board should not discretionarily deny this petition.

Although the Board need not address additional *Fintiv* factor considerations in light of Samsung's *Sotera* stipulation, indeed, the *Fintiv* factors do not favor denial.

Factor 1 is neutral because neither party has requested a stay in co-pending litigation.

Factor 2 is neutral because the Court's trial date is speculative at this point and subject to change. The Board will likely issue its Final Written Decision around March 2025, approximately five months after the currently scheduled trial date (August 5, 2024). SAMSUNG-1017, 1. However, as the Board and Director have previously recognized, "scheduled trial dates are unreliable and often [subject

to] change." SAMSUNG-1015, 8.

Factor 3 also favors institution because Petitioner has diligently filed this Petition months ahead of the one-year time bar, while the EDTX Litigation is still in its early stages. Beyond exchanging preliminary infringement/invalidity contentions, the parties and the District Court have yet to expend significant resources on invalidity. SAMSUNG-1017, 5.

Factor 4 also favors institution because Petitioner has provided a *Sotera* stipulation. SAMSUNG-1016.

Factor 5: The parties in the parallel EDTX litigation are the same.

Factor 6 favors institution because the merits of this Petition are compelling.

V. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung") are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '184 Patent is the subject of a civil action, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00422, E.D. Tex., filed October 26, 2022 (SAMSUNG-1004). Petitioner and Headwater are also involved in case nos.

2:22-cv-00467 and 2:23-cv-00103, also in E.D. Tex.

Petitioner is not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the '184 Patent.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email:IPR39843-0156IP1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Roberto Devoto, Reg. No. 55,108 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above. Petitioner consents to electronic service by email at IPR39843-0156IP1@fr.com (referencing No. 39843-0156IP1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, jjm@fr.com, and devoto@fr.com).

Respectfully submitted,

Dated 9-8-23

/Roberto J. Devoto/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Roberto Devoto Reg. No. 55,108
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2023-01361)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,993 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated 9-8-23

/Roberto J. Devoto/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Roberto Devoto Reg. No. 55,108
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on September 8, 2023, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

/Kristyn Waldhauser/
Kristyn Waldhauser
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(612) 638-5731