

VASU HOLDINGS, LLC, a Texas Corporation,
Plaintiff,
v.
SAMSUNG ELECTRONICS CO., LTD., a Korean Corporation, and SAMSUNG ELECTRONICS AMERICA, INC., a New York Corporation,
Defendants.

Samsung Ex. 1012
Samsung v. Vasu
IPR2025-00450
Page 00001

Pursuant to Local Patent Rules 3-1 and 3-2, Plaintiff Vasu Holdings, LLC (“Vasu”) makes the following Disclosure of Asserted Claims and Preliminary Infringement Contentions to Samsung Electronics Co., Ltd., and Samsung Electronics America, Inc., (“Defendants”), including the claim charts attached hereto as Appendix A-1, Appendices B-1 through B-4, Appendix C-1, Appendices D-1 through D-4, Appendices E-1 through E-4, and Appendices F-1 through F-4 (the “Appendices”) for each of the Accused Products of U.S. Patent Nos. 8,520,605, (the “’605 Patent”), 8,886,181 (the “’181 Patent”), 8,958,434 (the “’434 Patent”), 10,206,154 (the “’154 Patent”), 10,368,281 (the “’281 Patent”), and 10,419,996 (the “’996 Patent”) (collectively, the “Asserted Patents”), and accompanying document production.

Vasu makes this disclosure based upon information presently known and reasonably available to it as of the date hereof. This Disclosure of Asserted Claims and Preliminary Infringement Contentions, and the accompanying Appendices, are preliminary, as discovery has not yet commenced in this action, such that Defendants have not produced any technical documents. As Vasu’s investigation is ongoing, Vasu reserves the right to amend, modify, supplement, and/or narrow any portion of this Disclosure of Asserted Claims and Preliminary Infringement Contentions, including, but not limited to, the identification of asserted claims, the products and/or services accused of infringement, and the bases and manner of infringement.

To the maximum degree allowed by the Federal Rules of Civil Procedure, the Court’s Local Rules, and any scheduling orders entered in this action, Vasu reserves its right to amend, modify, supplement, and/or narrow this Disclosure of Asserted Claims and Preliminary Infringement Contentions as appropriate, as the case develops.

I. 3-1(a). Identification of Each Claim in Suit

Based on the information presently known to Vasu, and without the benefit of relevant discovery or the Court's claim construction, Vasu provides the following contentions pursuant to Patent Local Rules 3-1(a): Defendant has infringed and continues to infringe Claims 1, 12, 24, 28, 29, and 30 of the '605 Patent, Claims 1, 3, 4, 8, and 9 of the '181 Patent, Claims 1, 2, 10, 12, and 19 of the '434 Patent, Claims 1, 2, 4, 43, and 47 of the '154 Patent, Claims 1, 12, 23, 31, 37, and 45 of the '281 Patent, and Claims 1, 12, 23, 25, 34, 35, 39, and 41 of the '996 Patent (collectively, the "Asserted Claims"). Defendants have directly infringed and continues to directly and indirectly infringe the Asserted Claims pursuant to 35 U.S.C. § 271(a).

Due to the early stage of this litigation, the lack of discovery to date (including discovery concerning Defendants' products and services, and actions taken with respect to its products and services), and the absence of a claim construction order, the above identification is necessarily limited and preliminary in nature. Vasu reserves the right to amend, modify, supplement, or narrow these contentions pursuant to Patent Local Rule 3-6, including identifying additional asserted claims, as it obtains additional information over the course of discovery and in light of the Court's claim construction order.

II. 3-1(b). Identification of Accused Instrumentalities

Based on the information presently known to Vasu, and without the benefit of relevant discovery or the Court's claim construction, Vasu provides the following contentions pursuant to Patent Local Rule 3-1(b):

U.S. Pat. No. 8,520,605

The “Accused Products” are devices released in the following product ranges:

- Samsung 300 Series (“300 Series”) WLAN Access Point: WEA302i, WEA303i, WEA303e
- Samsung 400 Series (“400 Series”) WLAN Access Points: WEA403i, WEA403Si, WEA403e, WEA412h, WEA412i, WEA453e, and WEA463e
- Samsung 500 Series (“500 Series”) WLAN Access Point: WEA504i, WEA512i, WEA514i, and WEA524i
- WEA Access Point Controllers: WEC8500 and WEC8050
- Wireless Enterprise Manager: WDS-LM500

Defendants infringe the asserted claims (claims 1, 12, 24, 28, 29, and 30) of the ’605 Patent through direct infringement, inducement of infringement, and contributory infringement. The Accused Products all include technology that operates the same with respect to the claims asserted.

U.S. Pat. No. 8,886,181

The “Accused Products” are devices released in the following product ranges:

- Galaxy A Series (“A Series”): A02s, A03s, A10e, A11, A12, A13, A13 5G, A14 5G, A20, A21, A23 5G, A23 5G UW, A34 5G, A51, A51 5G, A51 5G UW, A52 5G, A53 5G, A53 5G UW, A54 5G, A71 5G, A71 5G UW, A73 5G
- Galaxy Note Series (“Note”): Note II, Note 5, Note 8, Note 9, Note 10, Note 10 5G, Note 10+, Note 10+ 5G, Note 20 5G, Note 20 Ultra 5G, Note Edge
- Galaxy S Series (“S Series”): SIII, S4, S5, S5 Active, S5 Mini, S5 Sport, S6, S6 Active, S6 Edge, S6 Edge+, S7, S7 Active, S7 Edge, S8, S8 Active, S8+, S9, S9+, S10, S10e, S10 Lite, S10+, S20, S20 5G, S20 Ultra 5G, S20 FE 5G, S20 Ultra 5G, S20+, S20+ 5G, S21 5G, S21 FE 5G, S21 Ultra 5G, S21+ 5G, S22, S22 Ultra, S22+, S23, S23+, S23 Ultra, S24, S24+, S24 Ultra
- Galaxy Z Series (“Z Series”): Z Fold, Z Fold5, Z Flip, Z Fold2 5G, Z Fold3 5G, Z Flip3 5G, Z Fold4, Z Fold4 5G, Z Flip4, Z Flip4 5G, Z Flip5, Z Flip 5G
- Galaxy XCover Series (“XCover”): XCover FieldPro, XCover Pro, XCover 5, XCover 6 Pro
- Galaxy J Series (“J Series”): Amp Prime, Amp Prime 3, J2, J2 Pure, J3, J7, J7 V, J7 Prime, J7 Star
- Galaxy Tab S Series (“Tab S”): Tab S3, Tab S7, Tab S7 5G, Tab S7 FE 5G, Tab S7+, Tab S7+ 5G, Tab S8, Tab S8 Ultra, Tab S8+, Tab S8+ 5G, Tab S9, Tab S9 FE, Tab S9 FE+, Tab S9 Ultra, Tab S9+, Tab S9+ 5G
- Galaxy Tab A Series (“Tab A”): Tab A, Tab A7 Lite, Tab A8.0, Tab A8.4, Tab A10.5
- Galaxy Tab View Series (“View”): View, View 2
- Galaxy Tab E Series (“Tab E”): Tab E8.0

Defendants infringe the asserted claims (claims 1, 3, 4, 8, 9) of the '181 Patent through direct infringement, inducement of infringement, and contributory infringement. The Accused Products all include technology that operates the same with respect to the claims asserted.

U.S. Pat. No. 8,958,434

The “Accused Products” are devices released in the following product ranges:

- Samsung 300 Series (“300 Series”) WLAN Access Point: WEA302i, WEA303i, WEA303e
- Samsung 400 Series (“400 Series”) WLAN Access Points: WEA403i, WEA403Si, WEA403e, WEA412h, WEA412i, WEA453e, and WEA463e
- Samsung 500 Series (“500 Series”) WLAN Access Point: WEA504i, WEA512i, WEA514i, and WEA524i
- WEA Access Point Controllers: WEC8500 and WEC8050
- Wireless Enterprise Manager: WDS-LM500

Defendants infringe the asserted claims (claims 1, 2, 10, 12, and 19) of the '434 Patent through direct infringement, inducement of infringement, and contributory infringement. The Accused Products all include technology that operates the same with respect to the claims asserted.

The “Accused Products” are devices released in the following product ranges:

- Galaxy A Series (“A Series”): A02s, A03s, A10e, A11, A12, A13, A13 5G, A14 5G, A20, A21, A23 5G, A23 5G UW, A34 5G, A51, A51 5G, A51 5G UW, A52 5G, A53 5G, A53 5G UW, A54 5G, A71 5G, A71 5G UW, A73 5G
- Galaxy Note Series (“Note”): Note II, Note 5, Note 8, Note 9, Note 10, Note 10 5G, Note 10+, Note 10+ 5G, Note 20 5G, Note 20 Ultra 5G, Note Edge
- Galaxy S Series (“S Series”): SIII, S4, S5, S5 Active, S5 Mini, S5 Sport, S6, S6 Active, S6 Edge, S6 Edge+, S7, S7 Active, S7 Edge, S8, S8 Active, S8+, S9, S9+, S10, S10e, S10 Lite, S10+, S20, S20 5G, S20 Ultra 5G, S20 FE 5G, S20 Ultra 5G, S20+, S20+ 5G, S21 5G, S21 FE 5G, S21 Ultra 5G, S21+ 5G, S22, S22 Ultra, S22+, S23, S23+, S23 Ultra, S24, S24+, S24 Ultra
- Galaxy Z Series (“Z Series”): Z Fold, Z Fold5, Z Flip, Z Fold2 5G, Z Fold3 5G, Z Flip3 5G, Z Fold4, Z Fold4 5G, Z Flip4, Z Flip4 5G, Z Flip5, Z Flip 5G
- Galaxy XCover Series (“XCover”): XCover FieldPro, XCover Pro, XCover 5, XCover 6 Pro
- Galaxy J Series (“J Series”): Amp Prime, Amp Prime 3, J2, J2 Pure, J3, J7, J7 V, J7 Prime, J7 Star
- Galaxy Tab S Series (“Tab S”): Tab S3, Tab S7, Tab S7 5G, Tab S7 FE 5G, Tab S7+, Tab S7+ 5G, Tab S8, Tab S8 Ultra, Tab S8+, Tab S8+ 5G, Tab S9, Tab S9 FE, Tab S9 FE+, Tab S9 Ultra, Tab S9+, Tab S9+ 5G
- Galaxy Tab A Series (“Tab A”): Tab A, Tab A7 Lite, Tab A8.0, Tab A8.4, Tab A10.5
- Galaxy Tab View Series (“View”): View, View 2
- Galaxy Tab E Series (“Tab E”): Tab E8.0

Defendants infringe the asserted claims (claims 1, 2, 4, 43, 47) of the ’154 Patent through direct infringement, inducement of infringement, and contributory infringement. The Accused Products all include technology that operates the same with respect to the claims asserted.

U.S. Pat. No. 10,368,281

The “Accused Products” are devices released in the following product ranges:

- Galaxy A Series (“A Series”): A02s, A03s, A10e, A11, A12, A13, A13 5G, A14 5G, A20, A21, A23 5G, A23 5G UW, A34 5G, A51, A51 5G, A51 5G UW, A52 5G, A53 5G, A53 5G UW, A54 5G, A71 5G, A71 5G UW, A73 5G
- Galaxy Note Series (“Note”): Note II, Note 5, Note 8, Note 9, Note 10, Note 10 5G, Note 10+, Note 10+ 5G, Note 20 5G, Note 20 Ultra 5G, Note Edge
- Galaxy S Series (“S Series”): SIII, S4, S5, S5 Active, S5 Mini, S5 Sport, S6, S6 Active, S6 Edge, S6 Edge+, S7, S7 Active, S7 Edge, S8, S8 Active, S8+, S9, S9+, S10, S10e, S10 Lite, S10+, S20, S20 5G, S20 Ultra 5G, S20 FE 5G, S20 Ultra 5G, S20+, S20+ 5G, S21 5G, S21 FE 5G, S21 Ultra 5G, S21+ 5G, S22, S22 Ultra, S22+, S23, S23+, S23 Ultra, S24, S24+, S24 Ultra
- Galaxy Z Series (“Z Series”): Z Fold, Z Fold5, Z Flip, Z Fold2 5G, Z Fold3 5G, Z Flip3 5G, Z Fold4, Z Fold4 5G, Z Flip4, Z Flip4 5G, Z Flip5, Z Flip 5G
- Galaxy XCover Series (“XCover”): XCover FieldPro, XCover Pro, XCover 5, XCover 6 Pro
- Galaxy J Series (“J Series”): Amp Prime, Amp Prime 3, J2, J2 Pure, J3, J7, J7 V, J7 Prime, J7 Star
- Galaxy Tab S Series (“Tab S”): Tab S3, Tab S7, Tab S7 5G, Tab S7 FE 5G, Tab S7+, Tab S7+ 5G, Tab S8, Tab S8 Ultra, Tab S8+, Tab S8+ 5G, Tab S9, Tab S9 FE, Tab S9 FE+, Tab S9 Ultra, Tab S9+, Tab S9+ 5G
- Galaxy Tab A Series (“Tab A”): Tab A, Tab A7 Lite, Tab A8.0, Tab A8.4, Tab A10.5
- Galaxy Tab View Series (“View”): View, View 2
- Galaxy Tab E Series (“Tab E”): Tab E8.0

Defendants infringe the asserted claims (claims 1, 12, 23, 31, 37, and 45) of the ’281 Patent through direct infringement, inducement of infringement, and contributory infringement. The Accused Products all include technology that operates the same with respect to the claims asserted.

U.S. Pat. No. 10,419,996

The “Accused Products” are devices released in the following product ranges:

- Galaxy A Series (“A Series”): A02s, A03s, A10e, A11, A12, A13, A13 5G, A14 5G, A20, A21, A23 5G, A23 5G UW, A34 5G, A51, A51 5G, A51 5G UW, A52 5G, A53 5G, A53 5G UW, A54 5G, A71 5G, A71 5G UW, A73 5G
- Galaxy Note Series (“Note”): Note II, Note 5, Note 8, Note 9, Note 10, Note 10 5G, Note 10+, Note 10+ 5G, Note 20 5G, Note 20 Ultra 5G, Note Edge
- Galaxy S Series (“S Series”): SIII, S4, S5, S5 Active, S5 Mini, S5 Sport, S6, S6 Active, S6 Edge, S6 Edge+, S7, S7 Active, S7 Edge, S8, S8 Active, S8+, S9, S9+, S10, S10e, S10 Lite, S10+, S20, S20 5G, S20 Ultra 5G, S20 FE 5G, S20 Ultra 5G, S20+, S20+ 5G, S21 5G, S21 FE 5G, S21 Ultra 5G, S21+ 5G, S22, S22 Ultra, S22+, S23, S23+, S23 Ultra, S24, S24+, S24 Ultra
- Galaxy Z Series (“Z Series”): Z Fold, Z Fold5, Z Flip, Z Fold2 5G, Z Fold3 5G, Z Flip3 5G, Z Fold4, Z Fold4 5G, Z Flip4, Z Flip4 5G, Z Flip5, Z Flip 5G
- Galaxy XCover Series (“XCover”): XCover FieldPro, XCover Pro, XCover 5, XCover 6 Pro
- Galaxy J Series (“J Series”): Amp Prime, Amp Prime 3, J2, J2 Pure, J3, J7, J7 V, J7 Prime, J7 Star
- Galaxy Tab S Series (“Tab S”): Tab S3, Tab S7, Tab S7 5G, Tab S7 FE 5G, Tab S7+, Tab S7+ 5G, Tab S8, Tab S8 Ultra, Tab S8+, Tab S8+ 5G, Tab S9, Tab S9 FE, Tab S9 FE+, Tab S9 Ultra, Tab S9+, Tab S9+ 5G
- Galaxy Tab A Series (“Tab A”): Tab A, Tab A7 Lite, Tab A8.0, Tab A8.4, Tab A10.5
- Galaxy Tab View Series (“View”): View, View 2
- Galaxy Tab E Series (“Tab E”): Tab E8.0

Defendants infringe the asserted claims (claims 1, 12, 23, 25, 34, 35, 39, and 41) of the ’996 Patent through direct infringement, inducement of infringement, and contributory infringement. The Accused Products all include technology that operates the same with respect to the claims asserted.

Due to the early stage of this litigation, the lack of discovery to date (including discovery concerning Defendants’ products and services), and the absence of a claim construction order, the above identification is necessarily limited and preliminary in nature. Vasu anticipates that discovery will reveal additional Accused Products and/or products, features and/or services that infringe the patents-in-suit. Vasu reserves the right to amend, modify, supplement, or narrow these contentions pursuant to Patent Local Rule 3-6, including identifying additional Accused Products, products, features and/or services, as it obtains

additional information over the course of discovery and in light of the Court's claim construction order.

III. 3-1(c)-(d). Claim Charts

Based on the information presently known to Vasu, Vasu provides the following Charts:

- Appendix A-1: showing how the WLAN 300 Series, 400 Series, and 500 Series Access Points, WEC8500/8050, and WDS-LM500 infringe the Asserted Claims 1, 12, 24, 28, 29, and 30 of the '605 Patent;
- Appendix B-1: showing how the Accused Galaxy A Series, S Series, Z Series, XCover, Note, J Series phones infringe the Asserted Claims 1, 3, 4, 8, and 9 of the '181 Patent;
- Appendix B-2: showing how the Accused Galaxy S Series, Note, Z Series, and J Series phones infringe the Asserted Claims 1, 3, 4, 8, and 9 of the '181 Patent;
- Appendix B-3 showing how the Accused Galaxy S Series, A Series, and View Series tablets infringe the Asserted Claims 1, 3, 4, 8, and 9 of the '181 Patent;
- Appendix B-4: showing how the Accused Galaxy View and E Series tablets infringe the Asserted Claims 1, 3, 4, 8, and 9 of the '181 Patent;
- Appendix C-1: showing how the WLAN 300 Series, 400 Series, and 500 Series Access Points, WEC8500/8050, and WDS-LM500 infringe the Asserted Claims 1, 2, 10, 12, and 19 of the '434 Patent;
- Appendix D-1: showing how the Accused Galaxy A Series, S Series, Z Series, XCover, Note, and J Series phones infringe the Asserted Claims 1, 2, 4, 43, and 47 of the '154 Patent;

- Appendix D-2: showing how the Accused Galaxy S Series, Note, Z Series, and J Series phones infringe the Asserted Claims 1, 2, 4, 43, and 47 of the '154 Patent;
- Appendix D-3: showing how the Accused Galaxy S Series, A Series, and View Series tablets infringe the Asserted Claims 1, 2, 4, 43, and 47 of the '154 Patent;
- Appendix D-4: showing how the Accused Galaxy View and E Series tablets infringe the Asserted Claims 1, 2, 4, 43, and 47 of the '154 Patent;
- Appendix E-1: showing how the Accused Galaxy A Series, S Series, Z Series, XCover, Note, and J Series phones infringe the Asserted Claims 1, 12, 23, 31, 37, and 45 of the '281 Patent;
- Appendix E-2: showing how the Accused Galaxy S Series, Note, Z Series, and J Series phones infringe the Asserted Claims 1, 12, 23, 31, 37, and 45 of the '281 Patent;
- Appendix E-3: showing how the Accused Galaxy S Series, A Series, and View Series tablets infringe the Asserted Claims 1, 12, 23, 31, 37, and 45 of the '281 Patent;
- Appendix E-4: showing how the Accused Galaxy View and E Series tablets infringe the Asserted Claims 1, 12, 23, 31, 37, and 45 of the '281 Patent;
- Appendix F-1: showing how the Accused Galaxy A Series, S Series, Z Series, XCover, Note, and J Series phones infringe the Asserted Claims 1, 12, 23, 25, 34, 35, 39, and 41 of the '996 Patent;

- Appendix F-2: showing how the Accused Galaxy S Series, Note, Z Series, and J Series phones infringe the Asserted Claims 1, 12, 23, 25, 34, 35, 39, and 41 of the '996 Patent;
- Appendix F-3: showing how the Accused Galaxy S Series, A Series, and View Series tablets infringe the Asserted Claims 1, 12, 23, 25, 34, 35, 39, and 41 of the '996 Patent; and
- Appendix F-4: showing how the Accused Galaxy View and E Series tablets infringe the Asserted Claims 1, 12, 23, 25, 34, 35, 39, and 41 of the '996 Patent.

The Appendices identify each element that is governed by 35 U.S.C. 112 (6) and the structure meeting this element. The Appendices also identify the elements governed under the doctrine of equivalents.

Vasu makes this disclosure based upon information presently known and reasonably available to it as of the date hereof. This Disclosure of Asserted Claims and Preliminary Infringement Contentions, and the accompanying Appendices, are preliminary, as discovery has not yet commenced in this action, such that Defendants have not produced any technical documents.

Vasu has subdivided the Asserted Claims in the Charts to explain where the Accused Products meet each claim element. These subdivisions are not to be taken as an indication of the boundaries of claim elements with respect to the doctrine of equivalents, or any other issue. In addition, the Accused Products may infringe the Asserted Claims in multiple ways. Vasu reserves the right to provide an alternative claim mapping or infringement contentions for such Accused Products or other products and services. Vasu further reserves the right to rely upon

the opinions of one or more experts in support of its infringement contentions in accordance with the Court's Scheduling Order.

As Vasu's investigation is ongoing, Vasu reserves the right to amend, modify, supplement, and/or narrow any portion of this Disclosure of Asserted Claims and Preliminary Infringement Contentions, including, but not limited to, the identification of Asserted Claims, the products and/or services accused of infringement, and the bases and manner of infringement.

The Asserted Claims cover a variety of inventions for mobile switch between cellular and Wi-Fi seamless roaming and broadband content access. Vasu's Preliminary Infringement Contentions set forth exemplary arrangement of features in the Accused Products illustrating why the Asserted Claims are infringed. As described in the specifications of the Asserted patents and as recited in the claims, Vasu's invention provides seamless roaming, seamless session continuity, and broadband access distribution. As such, there are multiple ways that the Asserted Claims are infringed, including as set forth in the Preliminary Infringement Contentions as well as by other arrangements of features in the Accused Products, such as by components which have multiple different functions such as Intelligent Wi-Fi and Smart Network Switch.

To the maximum degree allowed by the Federal Rules of Civil Procedure, the Court's Local Rules, and any scheduling orders entered in this action, Vasu reserves its right to amend, modify, supplement, and/or narrow this Disclosure of Asserted Claims and Preliminary Infringement Contentions as appropriate, as the case develops.

IV. Priority Date of Asserted Claims

Pursuant to Local Patent Rule 3-1(e), Vasu hereby identifies the priority date of asserted claims (identified in the accompanying Appendices) of the Asserted Patents as January 6, 2004.

V. 3-1(f). Identification of Own Practicing Products

Based on the information presently known to Vasu and Vasu's present understanding, Vasu provides the following contentions pursuant to Patent Local Rule 3-1 (f): Vasu does not identify any of its own products as practicing the patents. Vasu reserves the right to amend, modify, supplement, or narrow these contentions pursuant to Patent Local Rule 3-6.

VI. 3-2. Accompanying Document Production

Pursuant to the Patent Local Rule 3-2, Vasu provides herewith a document production which includes, *inter alia*, a copy of the file history for each of the Asserted Patents. Vasu makes this production based upon information presently known and reasonably available to it as of the date hereof. Vasu reserves the right to supplement its document production as the case develops over the course of discovery and as additional information becomes known or available to it.

Vasu has also provided documents identified in the table below. Specifically, each of the accompanying Appendices identifies and relies upon documents and support which are identified below and available in the document production as noted by the Bates range provided herein.

Bates Range	Reference
VASU 000010-10	U.S. Pat. No. 8,520,605
VASU 000011-829	U.S. Pat. No. 8,520,605 File History

VASU 000830-843	U.S. Pat. No. 8,886,181
VASU 000844-1567	U.S. Pat. No. 8,886,181 File History
VASU 001568-76	U.S. Pat. No. 8,958,434
VASU 001577-997	U.S. Pat. No. 8,958,434 File History
VASU 001998-2011	U.S. Pat. No. 10,206,154
VASU 002012-926	U.S. Pat. No. 10,206,154 File History
VASU 002927-37	U.S. Pat. No. 10,368,281
VASU 002938-3711	U.S. Pat. No. 10,368,281 File History
VASU 003712-23	U.S. Pat. No. 10,419,996
VASU 003724-4324	U.S. Pat. No. 10,419,996 File History

Dated: May 15, 2024

By: /s/ Paul J. Andre

Paul J. Andre (*pro hac vice*)
Lisa Kobialka (*pro hac vice*)
James Hannah (*pro hac vice*)
Kristopher Kastens (*pro hac vice*)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Telephone: (650) 752-1700
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
kkastens@kramerlevin.com

Elizabeth L. DeRieux (Bar No. 05770585)
Capshaw DeRieux LLP
114 E. Commerce St.,
Gladewater, Texas 75647
Telephone: 903-845-5770
ederieux@capshawlaw.com

Attorneys for Plaintiff
Vasu Holdings, LLC

CERTIFICATE OF SERVICE

I hereby certify that on May 15, 2024, a true and correct copy of the foregoing documents were served via electronic mail upon counsel for Defendants.

Melissa Richards Smith
Gillam & Smith, LLP
303 South Washington Avenue
Marshall, TX 75670
melissa@gillamsmithlaw.com

Christopher Michael Bonny
David S Chun
Ropes & Gray LLP
1900 University Ave, 6th Floor
East Palo Alto, CA 94303
christopher.bonny@ropesgray.com
david.chun@ropesgray.com

Steven Pepe
Ropes & Gray LLP - New York
1211 Avenue of the Americas
New York, NY 10036
steven.pepe@ropesgray.com

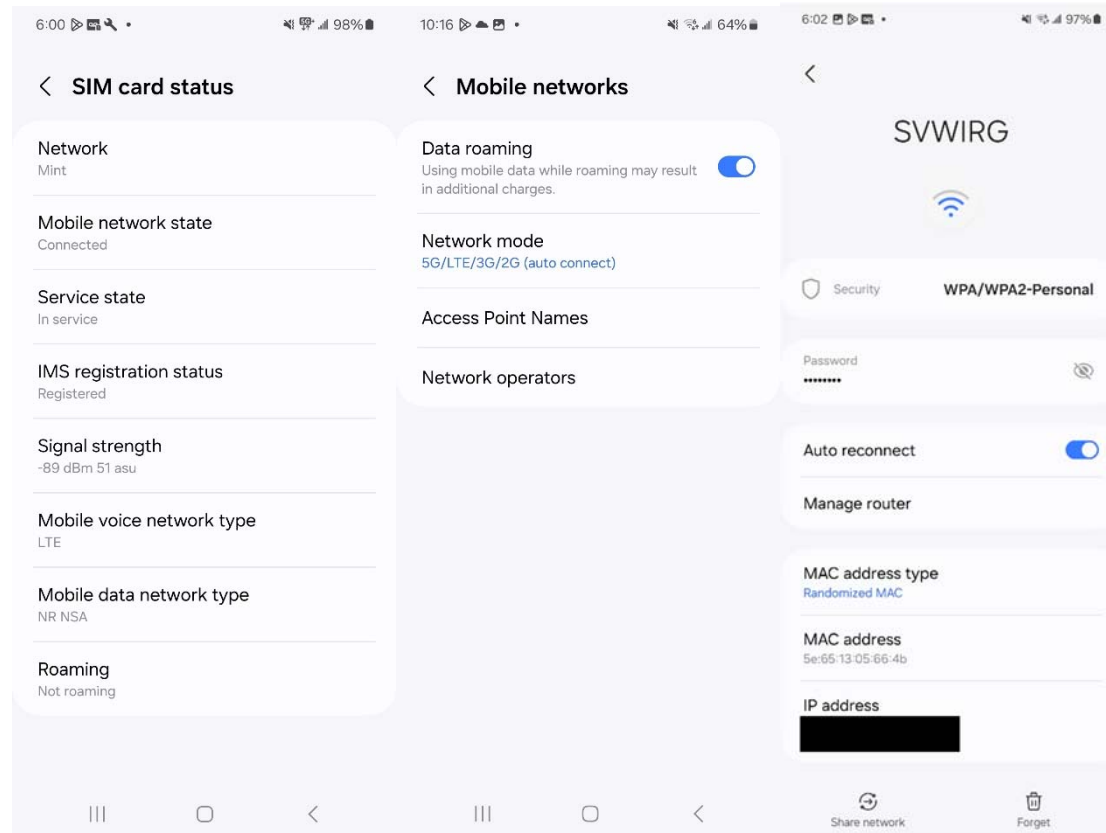
By: /s/ Paul J. Andre
Paul J. Andre

APPENDIX F-1

U.S. Pat. No. 10,419,996	Infringement
The “Accused Products” are devices released in the following product ranges: - Galaxy A Series (“A Series”): A02s, A03s, A10e, A11, A12, A13, A13 5G, A14 5G, A20, A21, A23 5G, A23 5G UW, A34 5G, A51, A51 5G, A51 5G UW, A52 5G, A53 5G, A53 5G UW, A54 5G, A71 5G, A71 5G UW, A73 5G - Galaxy S Series (“S Series”): S7, S7 Active, S7 Edge, S8, S8 Active, S8+, S9, S9+, S10, S10+, S10e, S10 Lite, S20, S20 5G, S20 Ultra 5G, S20+, S20+ 5G, S20 FE 5G, S21 5G, S21 FE 5G, S21 Ultra 5G, S21+ 5G, S22, S22+, S22 Ultra, S23, S23+, S23 Ultra, S24, S24+, S24 Ultra - Galaxy Z Series (“Z Series”): Z Fold, Z Flip 5G, Z Fold2 5G, Z Fold3 5G, Z Flip3 5G, Z Fold4, Z Fold4 5G, Z Flip4, Z Flip4 5G - Galaxy XCover Series (“XCover”): XCover Pro, XCover FieldPro, XCover 5, XCover 6 Pro, - Galaxy Note Series (“Note”): Note 9, Note 10, Note 10 5G, Note 10+, Note 10+ 5G, Note 20 5G, Note 20 Ultra 5G - Galaxy J Series (“J Series”): Amp Prime 3, J2, J2 Pure, J3, J7, J7 Star, J7 V, J7 Prime Defendants infringe the asserted claims (claims 1, 12, 23, 25, 34, 35, 39, and 41) of the ’996 Patent through direct infringement, inducement of infringement, and contributory infringement. The Accused Products all include technology that operates the same with respect to the claims asserted.	
Claim 1	
1[pre]. A device comprising:	The Accused Products (also referred to as user equipment, UEs) are mobile communication devices that include “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi Settings” or “Wi-Fi preferences,” “Wi-Fi Settings,” or “Advanced Wi-Fi Settings” of the Accused Products.¹ The feature allows the Accused Products to roam and switch between different wireless networks, such as a WiFi wireless network and cellular networks including General Packet Radio Service (“GPRS,” 2G), Global System for Mobile (“GSM,” 2G), Code-Division Multiple Access (“CDMA,” 3G), Long Term Evolution (“LTE,” 4G), or 5G network. The Accused Products are capable of using both Wi-Fi and cellular networks. <i>See</i> screenshots below of Galaxy S22—a representative Accused Product (indicating the representative Accused Product is

¹ These features were previously branded as “Smart Network Switch” and “Adaptive Wi-Fi.”

connected to a network, listing the supported cellular networks by the representative Accused Product, and showing the exemplary Accused Product can connect to Wi-Fi) (redactions added for privacy).²



VASU 031389-98 at 89-91; *see also* VASU 025467-76 at 75 (listing all of the wireless transmissions, including cellular networks supported by the representative Accused Product—Galaxy S22).

² Unless otherwise noted, any redactions are added for privacy.

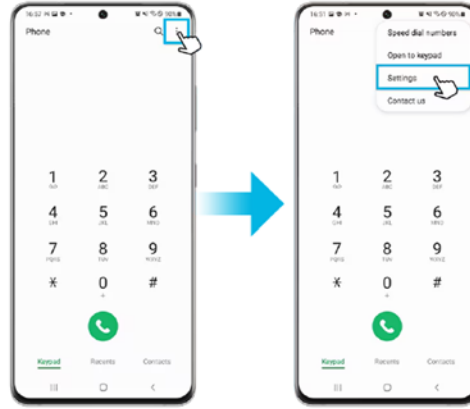
	The Accused Products are mobile communication devices that support at least the following communications: (1) voice over Wi-Fi (“VoWiFi,” Wi-Fi calling), (2) voice over IP (“VoIP”), and (3) constant data streams (<i>e.g.</i>, video or audio streams). The cellular (mobile) networks include radio network served by base stations, including Global System for Mobile Communications (“GSM”), Code Division Multiple Access (“CDMA”), Long Term Evolution (“LTE”), and 5G networks. VASU 025602-04 at 02. The Wi-Fi network include the wireless network that is enabled by the IEEE 802.11 standards (802.11a, 802.11b, 802.11g, 802.11ac, and 802.11ax). VASU 025617-26 at 21-22. The Accused Products are capable of roaming between networks by using the “Switch to mobile data” or “Switch to better Wi-Fi networks” product features. VASU 025185-91 at 86 (“Switch to Mobile Data is the solution for quickly switching from Wi-Fi to a mobile data network when a gray area is encountered.”); <i>see also</i> screenshot below (illustrating the roaming history between Wi-Fi and cellular).
--	--



VASU 031389-98 at 93.

Wi-Fi Calling Specifics

The Wi-Fi calling feature can be enabled either on the phone screen or in the quick setting panel, as shown below.



Step 3. Find and tap the switch to turn the Wi-Fi Calling feature on.



VASU 025173-78 at 74.

Id. at 75.

	Wi-Fi calling Make calls over Wi-Fi when you are connected to a Wi-Fi network. 1. From  Phone, tap  More options > Settings > Wi-Fi calling. 2. Tap  to enable this feature. 3. Follow the prompts to set up and configure Wi-Fi calling. VASU 010302-454 at 386 (showing how to enable the Wi-Fi calling feature in quick settings of an exemplary phone, Galaxy A13 5G). Wi-Fi Calling Make calls over Wi-Fi when you are connected to a Wi-Fi network. Wi-Fi Calling is a service provided by your wireless service provider. You need to activate Advanced calling first. 1. From a Home screen, swipe up to access Apps. 2. Tap  Settings > Connections > Advanced Calling. 3. Tap Activate Wi-Fi Calling. VASU 017373-567 at 477 (how to activate Wi-Fi calling in an exemplary phone, S7). IMS networks allow a user to initiate, modify, and terminate media sessions based on the Session Initiation Protocol (“SIP”). VASU 006576-783 at 585. These sessions include internet telephone calls, multimedia distribution, and multimedia conferences. VASU 025198-466 at 198. SIP is an application-layer control protocol to establish, modify, and terminate multimedia sessions (conferences) such as VoIP calls. <i>Id.</i> at 205. SIP supports the transfer and termination of sessions. <i>Id.</i> at 205. The Accused Products can complete a VoIP call through a SIP user agent after registering with a SIP server (interface server). VASU 025521-29 at 524. A SIP application server resides either in the user’s home network (“HPLMN”) or in a third-party location and can communicate with the Homer Subscriber Server (“HSS”) via Sh and Si interfaces. VASU 005019-113 at 58. Service Centralization and Continuity Application Server (“SCC AS”) is a type of SIP application server within PLMN (described in Element 1b-1c below). VASU 005019-113 at 58. The initial registration procedure consists of the Accused Products sending a REGISTER request. VASU 006784-7874 at 6885. The Accused Products can register a public user identity with any of its contact
--	---

addresses at any time after it has acquired an IP address, discovered a Proxy Call Session Control Function (“P-CSCF”), and established an IP access network bearer that can be used for SIP signaling. *Id.*

In order for P-CSCF to determine the Network Provided Location Information (“NPLI”) of Accused Products in case of a TWAN access, the TWAN shall report over S2a TWAN related access network information at PDN connection establishment, at bearer creation or modification, or release at PDN connection release. VASU 006232-544 at 491. The TWAN identifier shall include the service set identifier (“SSID”) of the access point to which the Accused Products are attached. *Id.*

The SIP UA at the Accused Products maintain the SIP/SDP state machine with the SCC AS also maintaining a copy of the state data. VASU 005865-953 at 880.

The Accused Products roam between multiple types of wireless network (from Wi-Fi to Wi-Fi network or from mobile to Wi-Fi network), further described in the below claim elements.

Wi-Fi Calling in the Accused Products

Below are corresponding documents that illustrate the communications functions including Wi-Fi Calling functionality in the Accused Products.

A Series: A series are communication devices that support both mobile network and Wi-Fi network. VASU 009579-721 at 583, 659 (Wi-Fi calling in A02s), 668-74; VASU 009855-10011 at 868, 948, (Wi-Fi calling in A10e), 959-76; VASU 010011-157 at 015, 089-95 (A11); VASU 010158-301 at 162, 232-36 (A12); VASU 010455-600 at 459, 519-23, 534 (Wi-Fi calling in A13); VASU 010746-901 at 760, 818-20, 825-29, 839 (Wi-Fi calling in A20); VASU 010902-1047 at 907, 970-75, 985 (Wi-Fi calling in A21); VASU 010302-454 at 306, 371-376, 381 (Wi-Fi calling in A13 5G); VASU 010601-745 at 605, 666-670 (A14 5G); VASU 011048-196 at 052, 124-26, 132 (Wi-Fi calling in A23 5G/A23 5G UW); A51_User_Manual.pdf at 99 (Wi-Fi calling in A51); VASU 011197-367 at 202, 231, 283-87, 297 (Wi-Fi calling in A51 5G/A51 5G UW); VASU 011368-531 at 372, 456-58 (A52 5G); VASU 011532-691 at 536, 606-10, 613-15, 620 (Wi-Fi calling in A53 5G/A53 5G UW); VASU 011692-852 at 696, 765-68, 772-75, 779 (Wi-Fi calling in A54 5G); VASU 011853-2015 at 857, 930-33, 945 (Wi-Fi calling in A71 5G); VASU 012016-2186 at 022, 102-06, at 116 (Wi-Fi calling in A71 5G UW); VASU 025133-44 at 38-39 (list of A Series phones that support changing of Wi-Fi network because of roaming).

	S Series: S Series are communication devices that support both mobile network and Wi-Fi network. VASU 017373-567 at 382, 466-71, 105 (Wi-Fi calling in S7); VASU 016965-7166 at 6975, 7052-55, 7072 (Wi-Fi calling in S7 Active); VASU 017167-372 at 180, 261-64, 281 (Wi-Fi calling in S7 Edge); VASU 017730-891 at 7819-22, 7832 (Wi-Fi calling in S8); VASU 017568-729 at 7653-56, 7667 (Wi-Fi calling in S8 Active); VASU 017892-8059 at 7979-82 (S8+); VASU 018060-236 at 74, 160-63, 167-72, 174 (Wi-Fi calling in S9/S9+); VASU 018399-571 at 403-5, 484-87, 499 (Wi-Fi calling in S10/S10e/S10+); VASU 018237-398 at 241, 321-24 (S10 Lite); VASU 018907-9076 at 8911, 8998-9004 (S20 5G/S20 Ultra 5G/S20+ 5G); VASU 018745-906 at 749, 828-835 (S20 FE 5G); VASU 019244-407 at 248-50, 329-36 (S21 5G/S21 Ultra 5G/S21+ 5G); VASU 019782-949 at 786-88, 875-882 (Wi-Fi calling in S22/S22 Ultra/S22+); VASU 019950-20128 at 955, 10049-55, 20056 (Wi-Fi calling in S23/S23+/S23 Ultra); VASU 020129-301 at 133-35, 223-29, 231 (Wi-Fi calling in S24/S24+/S24 Ultra); VASU 025133-44 at 38-39 (list of S Series phones that support changing of Wi-Fi network because of roaming). <u>Note Series</u> Note is a communication device that supports both mobile network and Wi-Fi network. VASU 013837-4053 at 3849, 3937-41, 3956-59, 3966 (Wi-Fi calling in Note 9); VASU 015086-267 at 090-92, 180-83, 188-94 (Note 10/Note 10+/Note 10+ 5G); VASU 014054-245 at 058, 157-61, 165-69, 172 (Wi-Fi calling in Note 20 5G/Note 20 Ultra 5G); VASU 025133-44 at 38-39 (list of Note Series phones that support changing of Wi-Fi network because of roaming). Z Series: Z Series are communication devices that support both mobile network and Wi-Fi network. VASU 024244-407 at 258, 344-50, 351 (Wi-Fi calling in Z Fold); VASU 023726-893 at 754, 817-22, 823 (Wi-Fi calling in Z Flip); VASU 024408-577 at 412, 499-506, 507 (Wi-Fi calling in Z Fold2 5G); Z VASU 023894-4071 at 899, 993-99, 1000 (Wi-Fi calling in Z Fold3 5G/Z Flip3 5G); VASU 024756-929 at 760, 853-60, 861 (Wi-Fi calling in Z Fold4/Z Flip4); VASU 025133-44 at 138-39 (list of Z Series phones that support changing of Wi-Fi network because of roaming). XCover: XCover are communication devices that support both mobile network and Wi-Fi network. VASU 023406-563 at 410, 481-85, 489-94, 496 (Wi-Fi calling in XCover Pro); VASU 023257-405 at 270, 336-40, 349 (Wi-Fi calling in XCover FieldPro); VASU 023090-256 at 094, 120-23, 171-74, 179-83, 186 (Wi-Fi calling in XCover 6 Pro); VASU 025133-44 at 38-39 (list of XCover phones that support changing of Wi-Fi network because of roaming).
--	--

	J Series: J Series are communication devices that support both mobile network and Wi-Fi network. VASU 012187-372 at 197, 269-72, 278-83, 288 (Wi-Fi calling in Amp Prime 3); VASU 012624-795 at 633, 701-04, 710-13, 721 (Wi-Fi calling in J2); VASU 012482-623 at 495, 560-63, 567-71, 573 (Wi-Fi calling in J2 Pure); VASU 012796-937 at 809, 869-71, 876-79, 882 (Wi-Fi calling in J3); VASU 013113-257 at 126, 187-90, 200 (Wi-Fi calling in J7 Star); VASU 013258-446 at 268, 341-44, 354-59, 364 (Wi-Fi calling in J7); VASU 013447-617 at 457, 528-31, 539 (Wi-Fi calling in J7 V); VASU 012938-3112 at 947, 1022-25, 1032 (Wi-Fi calling in J7 Prime).
--	--

1[a]. a switching system to switch operation between a first communication module and a second communication module, wherein if a context changes for known networks or a new network is detected with a more favorable context, a previously established communication automatically switches accordingly, wherein upon activation of a timer, the switching system causes the second communication module to change state from a sleep mode to a stand-by mode, and the switching system causes the second communication module to change state from the stand-by mode to an active mode before a communication is	The Accused Products operated as mobile communication devices that establish a voice call or data stream sessions (a first wireless communication link) between the Accused Products and an end destination device (another user equipment) such as a mobile phone, a laptop, the Internet of Things, or server. In the context of a voice call, the call can be over a VoIP or VoWiFi network (“Internet”) or a public land mobile network (“PLMN”), defined by the 3GPP standards. The Accused Products include a switching system, “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi Settings” in A Series, S Series, X Cover, and Z Series. VASU 010302-454 at 398 (A13 5G); VASU 010601-745 at 691 (A14 5G); VASU 011048-196 at 143 (A23 5G/A23 5G UW); VASU 011532-691 at 633 (A53 5G/A53 5G UW); VASU 011692-852 at 792 (A54 5G); VASU 018745-906 at 848 (S20 FE 5G); VASU 019244-407 at 351 (S21 5G/ S21 Ultra 5G/ S21+ 5G); VASU 019782-949 at 895 (S22/S22+/S22 Ultra); VASU 019950-20128 at 1070 (S23/S23+/S23 Ultra); VASU 023406-563 at 508 (XCover Pro); VASU 023564-725 at 672 (Z Flip 5G); VASU 023894-4071 at 1014 (Z Fold3 5G/Z Flip3 5G); VASU 024756-929 at 877 (Z Flip4); VASU 024408-577 at 520 (Z Fold2 5G). Similarly, the Accused Products include another switching system, “Switch to Mobile Data” product feature under “Wi-Fi Preferences.” VASU 012187-372 at 300 (Amp Prime 3); VASU 012624-795 at 737 (J2); VASU 013258-446 at 375 (J7); VASU 013447-617 at 557 (J7 V); VASU 012938-3112 at 1050 (J7 Prime); VASU 017373-567 at 490 (S7); VASU 016965-7166 at 1090 (S7 Active); VASU 017167-372 at 294 (S7 Edge); VASU 013837-4053 at 986 (Note 9).
--	---

switched to the second communication module.	Wi-Fi preferences Customize advanced Wi-Fi services. 1. From  Settings, tap Connections > Wi-Fi, and then tap On/Off to turn on Wi-Fi. 2. Tap  More options > Advanced. To view all network settings, tap View more. • Switch to mobile data: Connect automatically to a mobile network connection when the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi. • Turn on Wi-Fi automatically: Enable Wi-Fi in frequently used locations. • Wi-Fi power saving mode: Reduce battery usage by analyzing Wi-Fi traffic patterns. • Wi-Fi notifications: Receive notifications when open networks in range are detected. • Show Wi-Fi pop-up: When opening apps, indicate when Wi-Fi is available. VASU 013837-4053 at 3977. Moreover, the Accused Products include a similar switching system, “Switch to Mobile Data” product feature in “Advanced Wi-Fi Settings” to switch between mobile and Wi-Fi networks. VASU 009579-721 at 669 (A02s); VASU 009855-10011 at 116 (A10e); VASU 010011-157 at 104 (A11); VASU 010158-301 at 250 (A12); VASU 010455-600 at 546 (A13); VASU 010746-901 at 851 (A20); VASU 010902-1047 at 996 (A21); A51_User_Manual.pdf at 116 (A51); VASU 011197-367 at 315 (A51 5G/A51 5G UW); VASU 011368-531 at 477 (A52 5G); VASU 011853-2015 at 958 (A71 5G); VASU 012016-2186 at 2134 (A71 5G UW); VASU 015086-267 at 209 (Note 10+); VASU 014054-245 at 191 (Note 20 5G/Note 20 Ultra 5G); VASU 017730-891 at 838 (S8), VASU 017568-729 at 676 (S8 Active); VASU 017892-8059 at 8006 (S8+); VASU 018060-236 at 183 (S9/S9+); VASU 018399-571 at 511 (S10/S10e/S10+); VASU 018237-398 at 345 (S10 Lite); VASU 018907-9076 (S20 5G/S20 Ultra 5G/S20+ 5G); VASU 024244-407 at 348 (Z
---	---

Fold); VASU 023090-256 at 199 (XCover 6 Pro); VASU 023257-405 at 358 (XCover FieldPro); VASU 012482-623 at 570 (J2 Pure); VASU 012796-937 at 890 (J3); VASU 013113-257 at 209 (J7 Star).

Advanced Wi-Fi settings

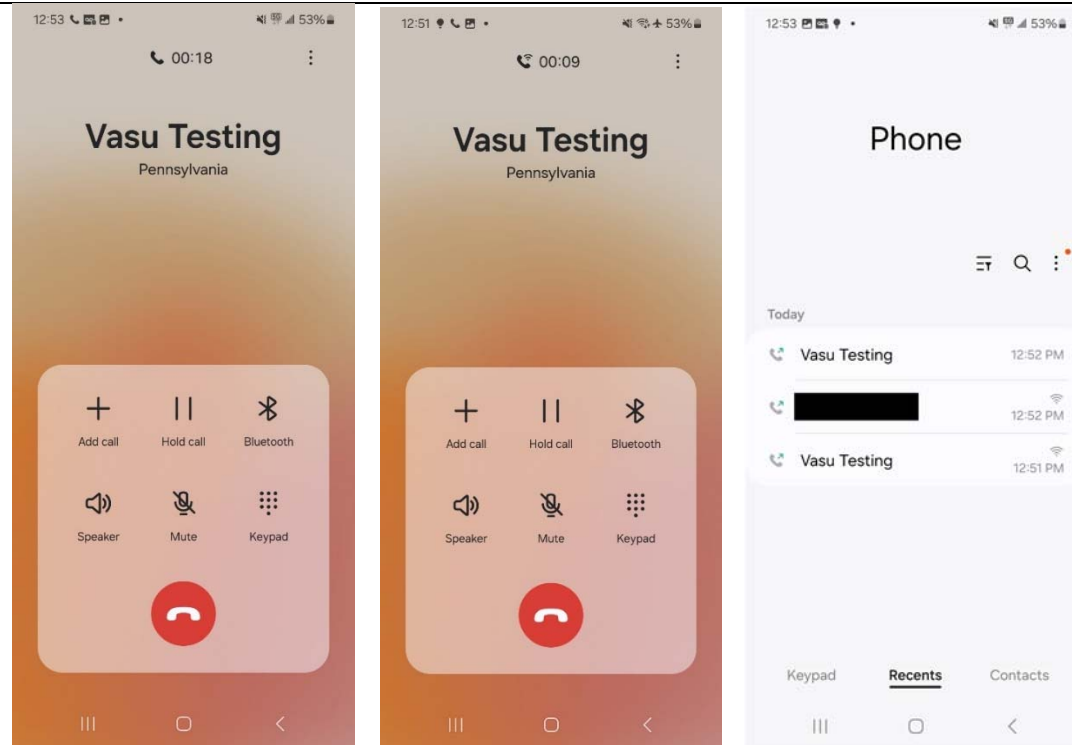
You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by carrier.

1. From Settings, tap  **Connections** > **Wi-Fi**, and then tap  to turn on Wi-Fi.
2. Tap  **More options** > **Advanced**.
 - **Sync with Samsung Cloud/account:** Sync Wi-Fi profiles with your Samsung account.
 - **Switch to mobile data:** When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi.
 - **Turn on Wi-Fi automatically:** Turn on Wi-Fi in frequently-used locations.
 - **Detect suspicious networks:** Get notified when suspicious activity is detected on the current Wi-Fi network.

VASU 010455-600 at 546.

The Accused Products “Intelligent Wi-Fi” product feature is another switching system in “Wi-Fi Settings,” which switches between mobile and Wi-Fi networks depending on the signal strength. VASU 020129-301 at 243 (S24/S24+/S24 Ultra); VASU 024756-929 at 874 (Z Fold4/Z Flip4).

	Wi-Fi settings You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider. 1. From Settings, tap  Connections > Wi-Fi, and then tap  to turn on Wi-Fi. 2. Tap  More options for the following options: • Wi-Fi Direct: Share data directly between devices over Wi-Fi. • Intelligent Wi-Fi: Configure Wi-Fi switching and detection features. • Advanced settings: Configure Wi-Fi connections and Hotspot settings. • Contact us: Contact Samsung support through Samsung Members. VASU 024756-929 at 874 (Z Fold4/Z Flip4). The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module (further described in Element 1[b]). This first communication link is over a first type of wireless network, either a Wi-Fi network or a PLMN or Cellular Network. With respect to a voice call, it can be initiated within the Wi-Fi network or over the PLMN/Cellular Network. <i>Compare</i> left screenshot (illustrating a cellular call via 5G by the lack of Wi-Fi symbol in the top ribbon and showing 5G cellular connectivity), <i>with</i> middle screenshot (illustrating a WiFi call by noting the phone is in airplane mode and by bearing a Wi-Fi symbol above the phone symbol); <i>see also</i> right screenshot (showing two calls made to the contact “Vasu Testing” where the earlier call has a Wi-Fi symbol above the time indicating a Wi-Fi call and the later call does not have a Wi-Fi symbol above the time indicating a cellular call).
--	---



VASU 031389-98 at 93-95.

The first connection link between the Accused Product and end destination device can be made under at least three scenarios: (1) Wi-Fi to Wi-Fi connection, (2) Wi-Fi to Home PLMN, and (3) Wi-Fi to Visitor PLMN. The vice versa is also true. Wi-Fi, Home PLMNs, and Visitor PLMNs are type of wireless networks.

The Accused Products established the calls via a wireless communication link with PLMN through gateways and interfaces supported by Evolved Packet Core (“EPC”) functions. EPC can be accessed via a trusted or untrusted network. There are differences when accessing these types of networks. However, the

differences are not relevant to whether the Accused Products establish a communication link with an end destination device.

The Supported EPC Functions

Trusted WLAN Access Network (“TWAN”): For access to PLMN’s EPC via a trusted non-3GPP access network such as trusted TWLAN, a connection shall be established between the Accused Products and TWAN using specific signal procedures. VASU 008198-326 at 230. Access authentication signaling for access to the EPC shall be executed between the Accused Products and the AAA server, which is an interface server, to ensure mutual authentication of the user and the EPC. *Id.* at 230.

Evolved Packet Data Gateway (“ePDG”): ePDG is the local mobility anchor within untrusted non-3GPP access. VASU 006232-544 at 262. The PLMNs included in the ePDG information are the PLMNs that have roaming agreements with HPLMN. VASU 006232-544 at 269.

Through a network interface (Swn interface), the ePDG connects with an untrusted non-3GPP access. VASU 005019-113 at 92. The ePDG connects with the Accused Products (through the SWu interface) to establish data tunnels and user data packet transmission within the tunnels. *Id.* at 93.

Call Session Control Function (“CSCF”): CSCF can act as Proxy CSCF (“P-CSCF”), serving CSCF (“S-CSCF”), emergency CSCF (“E-CSCF”), or Interrogating CSCF (“I-CSCF”). VASU 005019-113 at 56. The P-CSCF is the first contact point for the Accused Products within the International Mobile Subscriber Identity (“IMSI”); the S-CSCF actually handles the session states in the network; the E-CSCF handles emergency sessions such as routing an emergency requests to the correct emergency center; the I-CSCF is the contact point within an operator’s network for all IMS connections destined to a subscriber of that network operator or roaming subscriber located within the network operator’s service area. *Id.*

Home Subscriber Server (“HSS”): The HSS supports the authentication procedures to access CS domain, PS domain, and system services by storing the generated data for authentication, integrity, and ciphering and by providing these data to the appropriate entities including AAA server or CSCF. VASU 005019-113 at 41. The diagram below illustrates . . .

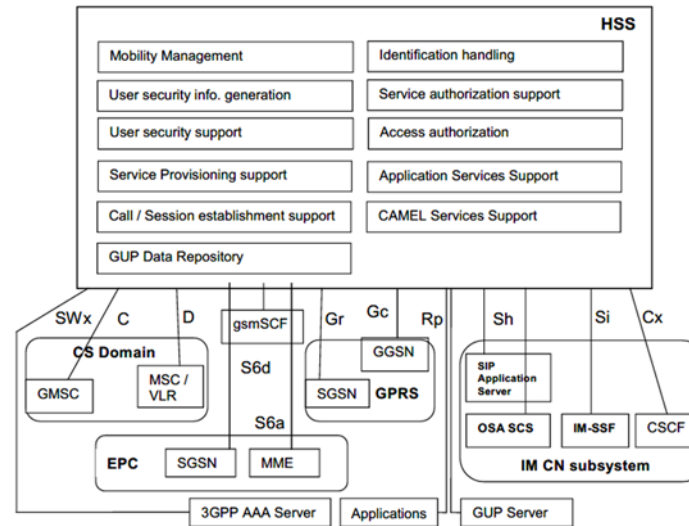


Figure 0.b: HSS logical functions

VASU 005019-113 at 40.

Authentication, Authorization, and Accounting (“AAA”): The Accused Products is authenticated and authorized through AAA to roam between networks. AAA server (interface server) is located at HPLMN and provides support for non-3GPP access users with services like authentication, authorization, and location management services to access evolved packet systems (“EPS”) in mobile networks. VASU 005019-113 at 49. It interacts with HSS to maintain consistent information to support service continuity between 3GPP (mobile networks) and non-3GPP (Wi-Fi) networks. *Id.* It contains user information to gain access to non-3GPP access. *Id.* Non-3GPP access authentication defines the process to permit or deny a subscriber to attach to and use the sources of a non-3GPP IP access interworked with the EPC network. VASU 006232-544 at 307. Non-3GPP access authentication signaling is executed between the Accused Products and the AAA server/HSS (interface server). *Id.* During the authentication of the

Accused Products for accessing the EPC via ePDG, ePDG shall initiate EAP-AKA based authentication between the Accused Products and the AAA server. VASU 006232-544 at 279.

Roaming Scenarios After the Accused Products Establish a Call

Exemplary Scenario 1: Wi-Fi to Wi-Fi

- (1) The Accused Products initiate a call within a first Wi-Fi network through VoIP or VoWiFi and roam from a first Wi-Fi network to a second Wi-Fi network.

The Accused Products may go out of range of access points and shift network association to another access point without losing connection. VASU 025133-44 at 134. Weak signals can trigger roaming on the Accused Products. *Id.* The Accused Products support 802.11k and 802.11v standards to reduce the length of time of lost connectivity during basic service set (“BSS”) transition. *Id.* at 138-42.

Exemplary Scenario 2: Wi-Fi to Home PLMN

- (1) The Accused Products initiate a call over a first Wi-Fi network through VoIP or VoWiFi and roam from the first Wi-Fi network to the coverage area of the home PLMN (“HPLMN”) of the Accused Products.
- (2) The Accused Products initiate a call within a first Wi-Fi network, but set up a backend of the call over PLMN network and roam from the first Wi-Fi network to the coverage area of the HPLMN of the Accused Products.

In a non-roaming scenario when the Accused Products establish the communication link with a home network, the trust relationship of Wi-Fi (non-3GPP IP wireless network) is determined by the HPLMN operators. VASU 008198-326 at 227. The trust relationship is indicated to the Accused Products via either pre-configured policies in the Accused Products by the home PLMN operator or dynamic indication during 3GPP-based access authentication. *Id.*

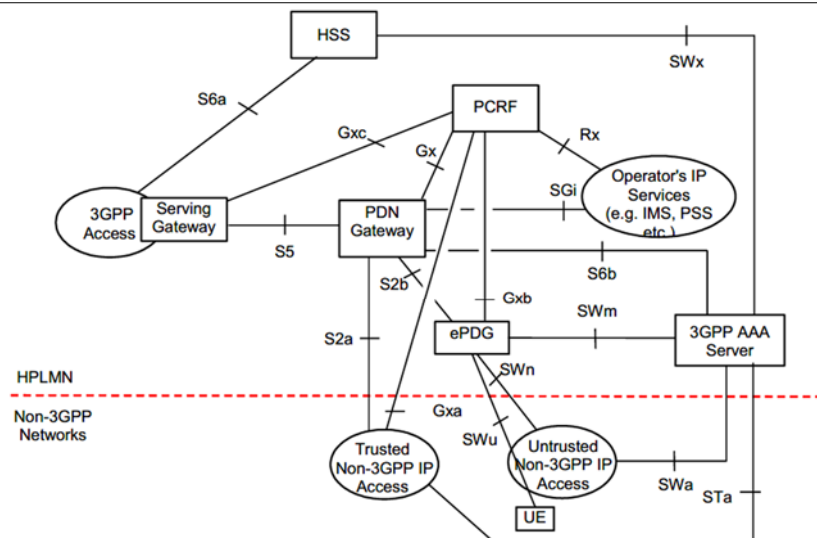


Figure 4.2.2-1: Non-Roaming Architecture within EPS using S5, S2a, S2b

VASU 006232-544 at 254 (non-roaming architecture showing trusted or untrusted non-3PPP wireless network connecting to AAA server in PLMN using the SWa or STa interface to access the trusted or untrusted 3GPP networks).

	Authorization of EPC access shall be performed by the AAA server upon successful user authentication. <i>Id.</i> <u><i>Exemplary Scenario 3: Wi-Fi to Visitor PLMN</i></u> (1) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over VoIP or VoWiFi, and roam from the first Wi-Fi network to the coverage area of a visitor PLMN (“VPLMN”) of the Accused Products. (2) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over a HPLMN, and roam from the first Wi-Fi network to the coverage area of a VPLMN. In roaming scenario when the Accused Products establish the communication link with a visitor network, the HSS or AAA server (interface server) in HPLMN makes the final decision if a non-3GPP wireless network is trusted or untrusted. VASU 006232-544 at 260. The HSS/AAA server (interface server) may take the visitor PLMN (“VPLMN”) policy and capability returned from the AAA proxy or roaming agreement into account. <i>Id.</i> at 260.
--	--

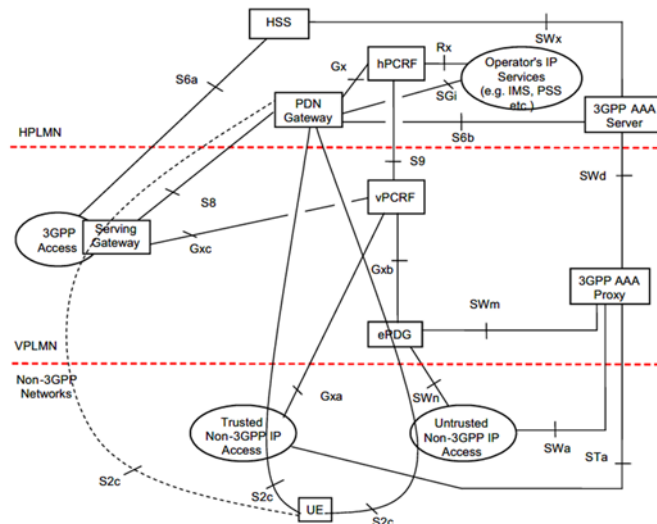


Figure 4.2.3-3: Roaming Architecture for EPS using S8 – S2c - Home Routed

VASU 006232-544 at 258 (roaming architecture showing trusted or untrusted non-3GPP IP access to AAA server/proxy in PLMN through STa or SWa interface).

The session origination procedures specify the signaling path between the Accused Products initiate a session setup attempt and the S-CSCF assigned to perform the session origination service. VASU 005263-653 at 380. The Accused Products initiate a session setup attempt and assigned a S-CSCF to perform the session origination service. VASU 005263-653 at 380. The signaling path between the Accused Products and S-CSCF is determined at the time of the Accused Products registration. *Id.* The S-CSCF to application server interface is used to provide services in the application server in the HPLMN or in a trusted external network (e.g., third-party or VPLMN). VASU 005019-113 at 58.

If the Accused Products are located in a VPLMN, it determines the P-CSCF via the CSCF discovery procedure. VASU 005263-653 at 380. The HPLMN advertises the S-CSCF as the entry point from the VPLMN. *Id.* When registration is completed, P-CSCF knows the name/address of the next hop in the signaling path toward the S-CSCF. *Id.* If the Accused Products are located in the HPLMN, the HPLMN

allocates an S-CSCF in the HPLMN. *Id.* at 383. When registration is completed, P-CSCF knows the name/address of S-CSCF. *Id.*

Detection of Context Changes in the Established Communication

The Accused Products monitor the network context (signal strength or user preference) of their communication link to the wireless network to detect context changes.

The second (preferred) network could be a known network (user locally stored data) or a newly discovered network (by PLMN selection procedure). VASU 008198-326 at 222. The second network could also be defined by the operator policy or user preferences. VASU 005654-93 at 64; VASU 025185-91 at 187 (describing how user preference works during switching to mobile data). Furthermore, Upon UE's request, the access network discovery and selection function ("ANDSF") in either HPLMN or VPLMN may provide a list of wireless access networks available in the vicinity of the UE for all the access technology types requested by the UE to establish a second communication link through Wi-Fi. VASU 006232-544 at 293.

"Switch to Mobile Data" detects the network context changes to "automatically switch[] networks based on both network quality and user preferences." VASU 025185-91 at 187. The connection manager will not be active until it accumulates enough data to determine user preference. *Id.*



Id. at 187 (determining user preference).

Through "Switch to mobile data" or "Switch to better Wi-Fi networks" product feature within "Intelligent Wi-Fi settings" on the Accused Products (shown below), the Accused Products can seamlessly switch to mobile data if there are signal strength issues and "whenever the Wi-Fi connection is unstable." VASU 019950-20128 at 1070. When the Wi-Fi signal strength is strong, it switches "back to Wi-Fi." *Id.*

	Intelligent Wi-Fi settings You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider. 1. From Settings, tap  Connections > Wi-Fi, and then tap  to turn on Wi-Fi. 2. Tap  More options > Intelligent Wi-Fi for the following options: • Switch to mobile data: When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi. • Switch to better Wi-Fi networks: Automatically switch to faster or more stable Wi-Fi networks. • Turn Wi-Fi on/off automatically: Turn on Wi-Fi in frequently-used locations. • Show network quality info: Display network information (such as speed and stability) in the list of available Wi-Fi networks. • Prioritize real-time data: Give network priority to games, video calls, and other tasks that are sensitive to lag. • Detect suspicious networks: Get notified when suspicious activity is detected on the current Wi-Fi network. • Wi-Fi power saving mode: Enable Wi-Fi traffic analysis to reduce battery usage. • Auto Hotspot connection: Automatically connect to a Wi-Fi hotspot when detected. • Intelligent Wi-Fi: View the Intelligent Wi-Fi version. VASU 019950-20128 at 1070 (intelligent Wi-Fi settings in an exemplary S23+ phone). The Accused Products measure signal strength of Wi-Fi networks by Received Signal Strength Indicator (“RSSI”), and its unit of measurement is dBm. The table below provides a point of reference for interpreting the RSSI value.
--	--

Signal Strength	TL;DR		Required for
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWi-Fi, streaming video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

VASU 025540-45 at 43-44.

The screenshot below illustrate that the Accused Products continuously monitor the signal strength.



VASU 031389-98 at 96.

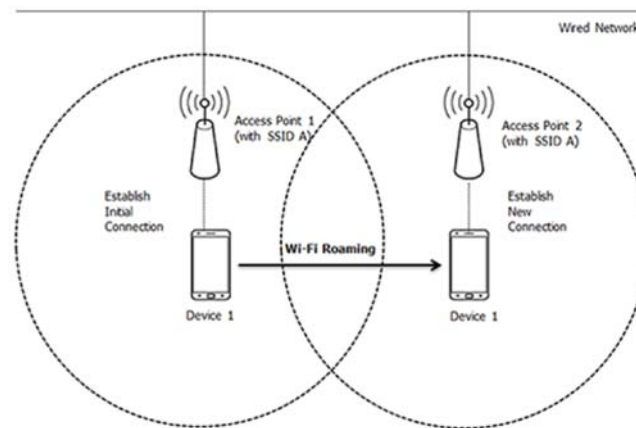
The Accused Products include “Auto Wi-Fi,” which turns Wi-Fi on and off depending on locations. VASU 025185-91 at 88. It turns Wi-Fi on when the favorite network is available by user preference and turns off Wi-Fi when this network is unavailable. *Id.* Auto Wi-Fi is triggered based on user’s location by geofencing (a virtual geological fence based on cellular stations). *Id.*

Furthermore, The Wi-Fi network selection functions in the Accused Products continuously

evaluate the quality of the connected network and assess the quality of available networks. VASU 025102-18 at 02. The Accused Products scan the available networks depending whether the screen of the Accused Products is on or off. *Id.*

If the screen of the Accused Products is on and the Accused Products is connected, the Wi-Fi framework of the Accused Products evaluates whether the current network is good enough to skip network selection when all the following conditions are met: (1) the RSSI is above the required RSSI threshold or sufficient traffic is flowing over the connection; (2) the network is evaluated, or user approved for use without internet access; and (3) the network is unmetered. *Id.* at 2. If the connection isn't good enough, the connectivity subsystem triggers a scan to detect available networks (a set of networks to choose for the second network). *Id.*

Once connected, the Wi-Fi service calculate "a connected score" based on the RSSI and determine whether to connect to a Wi-Fi network or another network type, such as a mobile network. *Id.* at 3-4. the Wi-Fi service may pass the score to the connectivity service, which uses the score to determine whether to connect to a Wi-Fi network or to a mobile network. *Id.* at 5.



VASU 025133-44 at 34 (roaming from one Wi-Fi to another Wi-Fi access point is triggered due to weak signal).

Moreover, if the screen is on and the Accused Products are disconnected, the Android connectivity system issues periodic scans (activation of a timer) following an exponential back off schedule (increasing the waiting time between retries). *Id.* at 02. The module evaluates scan results received by evaluating if the signal level is below a predefined threshold and tries to select the best network to connect to. *Id.* When the Accused Products' screen is off, the network selection process might occur if scans are initiated by other services such as location services. *Id.* at 06.

Automatically Switching to a Second Communication Module over a Second Network

When the Accused Products are active in an IMS session, the session transfer procedures provide session continuity between wireless networks using signal strength information. VASU 005654-93 at 62. The Accused Products initiate session transfer procedure based on trigger criteria, including the current operator policy, user preferences, and wireless network conditions for conducting a session continuity operation to the SCC AS (interface server). VASU 005654-93 at 64. A third-party call control function (call function from the Accused Products) is employed for subscriber IMS sessions at the SCC AS upon session establishment for enablement of Session Transfer. *Id.*

The first communication link (voice or video call) uses IP Multimedia Core Network Subsystem ("IMS"), which is the framework for delivering multimedia services using PS and CS bearers (data tunnels between the network gateways and the Accused Products) for the media. VASU 005654-93 at 58. IMS service continuity requires a Service Centralization and Continuity ("SCC") Application Server ("AS"). VASU 005654-93 at 63. The SCC AS is a home network based IMS application that provides functionality required to enable IMS centralized services. VASU 005865-953 at 77. The screenshot below illustrates the information used for IMS service continuity that may be provided between SCC AS and the Accused Products:

- session transfer indicator to indicate that this new session is for session transfer.
- details about the access and the media components being transferred / kept / released.
- optionally, an IMS Communication Service Identifier defined in 3GPP TS 23.228 [7]
- which session is required to be replaced or updated;
- whether to merge the session(s):

VASU 005654-93 at 63. SCC AS provides an IMS-based mechanism for enabling session continuity. It executes the transfer of the IMS session between different wireless networks and implements third-party call control upon session establishment. VASU 005654-93 at 64.

A Service Control Signaling Path transports service control signaling between the Accused Products and the SCC AS when using CS or PS access. VASU 005865-953 at 79. The access leg is formed by combining the Service Control Signaling Path and the CS Bearer Control Signaling Path. VASU 005865-953 at 80. The SCC AS presents the remote leg to the CSCF as an IMS session using IMS SIP signaling on behalf of the Accused Products. *Id.*

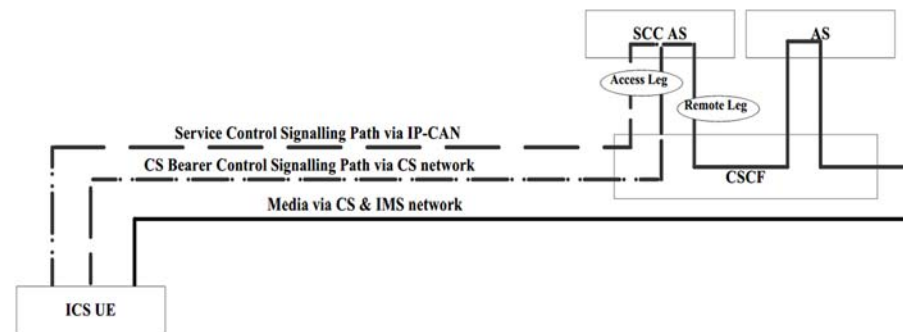


Figure 7.1.1-1: ICS UE session signalling and bearer path using PS network for Service Control

VASU 005865-953 at 80 (Accused Products (or UEs), session signaling and bearer path in access leg and remote leg in PS network).

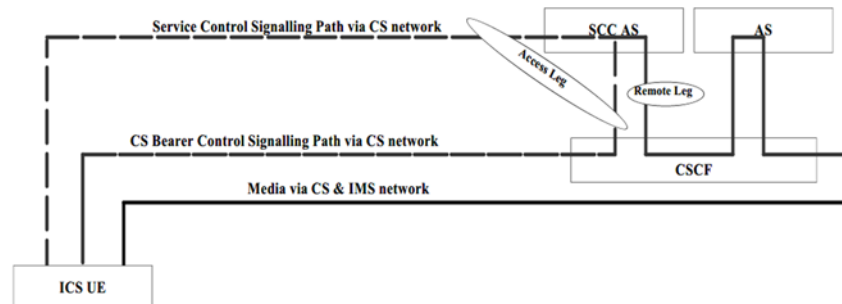


Figure 7.1.1-2: ICS UE session signalling and bearer path using CS network for Service Control Signalling Path

VASU 005865-953 at 80 (Accused Products (or UEs), session signaling and bearer path in access leg and remote leg in CS network).

Moreover, the access transfer control function (“ASCF”) is a function in HPLMN or visitor network (“VPLMN”) may be co-located with the existing functional entities such as P-CSCF. VASU 005694-864 at 720. Based on carrier policy, it shall be allocated a session transfer number (“STN-TR”) and keeps track of sessions (either in alerting state, active, or held) to be able to perform session transfer. *Id.* at 720-21. The following implementation method determines if the ASCF should be included during registration: if Accused Products are roaming, based on the roaming agreement; based on local configuration; based on registered communication service of the Accused Products; based on the access type. *Id.* at 721.

Upon session initiation, the Accused Products or the SCC AS establishes the Service Control Signaling Path for communication of service control signaling via the PS network using the Gm reference point. VASU 005865-953 at 80.

Session Continuity between Mobile Networks

When the signal strength drops below a predetermined threshold, the Accused Products may also use locally stored data for selecting a second EPC network available for connectivity via the currently selected non-3GPP wireless network to establish a second communication link. VASU 008198-326 at 222. UE

shall select a PLMN according to the PLMN selection procedure of the selected non-3GPP wireless network. *Id.*

Signaling and bearer resources are allocated in the transferring-in wireless network and the user's sessions are transferred from the transferring-out wireless network. VASU 005654-93 at 669. The SCC AS executes access transfer procedures and resources in the transferring-out wireless network is released. *Id.*

The Accused Products establish the second communication link (the second call session with the second network, transferred-in network) with the transfer-in network without disrupting the first communication link in the transfer-out network. IMS sessions from and to the Accused Products are anchored at the SCC AS in the home IMS based on initial filtering criteria ("iFC") to provide service continuity for the user during the transition between two wireless networks. VASU 005654-93 at 62.

For single radio voice call continuity ("SRVCC"), voice call continuity between PLMN/VPLMN over PS and CS are anchored when the UE is capable of transmitting or receiving only one of the access networks at a given time. VASU 005195-214 at 200.

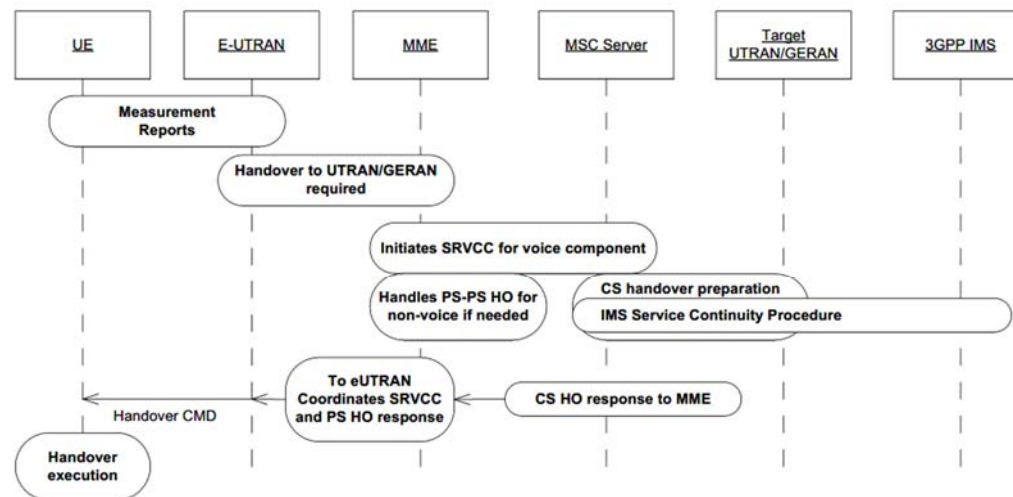


Figure 4.2.2-1: Overall high level concepts for SRVCC from E-UTRAN to UTRAN/GERAN

VASU 005195-214 at 202 (how SRVCC works in E-UTRAN, 4G to UTRAN/GERN, 3G/2G).

A third-party call control function (functions provided by the Accused Products) is employed at the SCC AS to facilitate inter-access network mobility through the user of access transfer between the two wireless networks. *Id.*

PS-CS transfer

IMS session established in CS or PS wireless networks are anchored at the SCC AS. VASU 005654-93 at 662. IMS sessions using CS bearer are established at session setup or upon access transfer. *Id.*

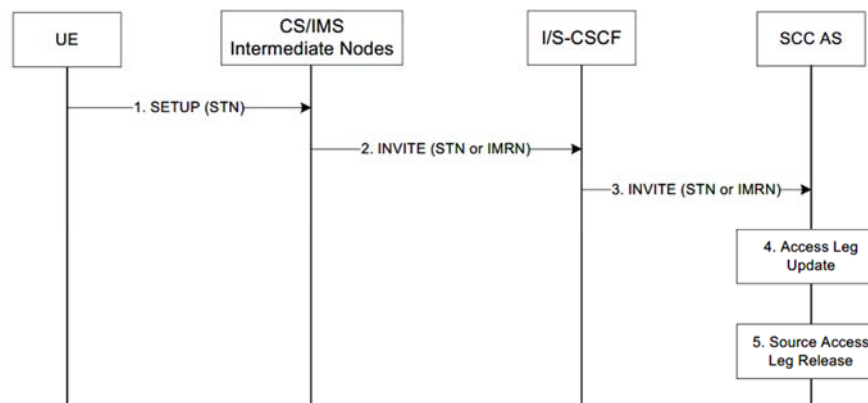


Figure 6.3.2.1.1-1: PS – CS Access Transfer: PS to CS

VASU 005654-93 at 72 (user is active in an IMS originating or terminating session using PS media at the time of transfer).

CS-PS Transfer

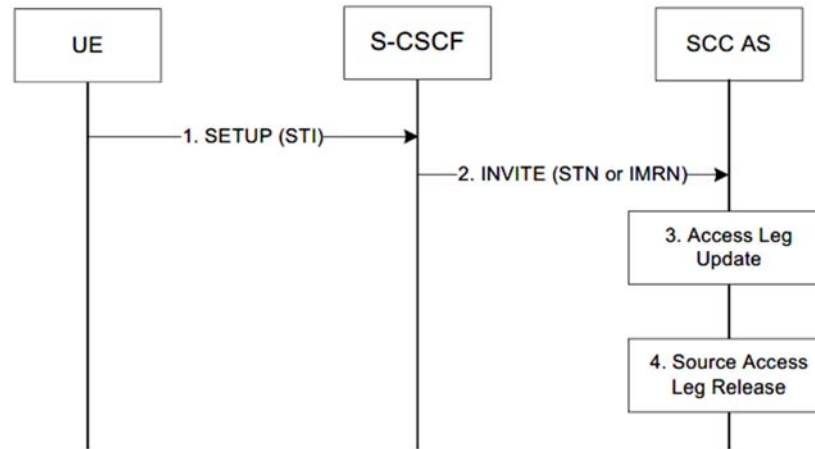


Figure 6.3.2.1.2-1: PS – CS Access Transfer: CS to PS

VASU 005654-93 at 73 (the user is active in the IMS originating or terminating session using CS at the time of transfer).

PS-PS Transfer

US is attached to one IP connectivity access network (“IP-CAN”), and it registers to the S-CSCF. VASU 005654-93 at 75. UE-1 and UE-2 establish an active multimedia session via this IP-CAN. *Id.* After changing to a new IP-CAN, obtaining new signaling and media addresses, and completing the Access Transfer procedures, UE-1 continues the session with UE-2 on the new IP-CAN. *Id.*

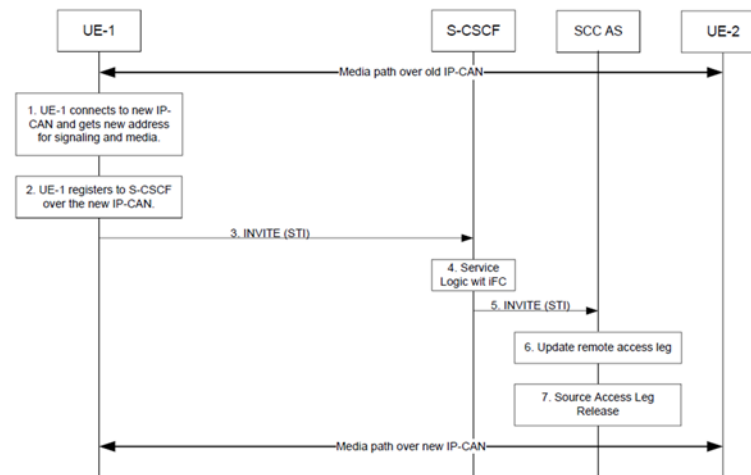


Figure 6.3.2.2.1-1: Information flow for PS-PS Access Transfer

Id.

Session Continuity between Wi-Fi and Mobile Networks

Upon the Accused Products' request, the access network discovery and selection function ("ANDSF") in either HPLMN or VPLMN may provide a list of wireless access networks available in the vicinity of the UE for all the access technology types requested by the UE to establish a second communication link through Wi-Fi. VASU 006232-544 at 293. An ANDSF element located in the HPLMN of a UE is referred to as Home-ANDSF ("H-ANDSF") and an ANDSF element located in the visited PLMN of a UE is

referred to as the visited-ANDSF (V-ANDSF) for this UE. VASU 006232-544 at 291. The H-ANDSF in the subscriber's HPLMN may interact with HSS user profile information. *Id.* at 61.

The ANDSF provides information for access networks that are available to the UE including:

- the access technology type (e.g. WLAN, WiMAX).
- the radio access network identifier (e.g. the SSID of a WLAN).
- other technology specific information, e.g. one or more carrier frequencies.
- validity conditions, i.e. conditions indicating when the provided access network discovery information is valid (such conditions may include e.g. a location).

VASU 006232-544 at 293.

ANDSF contains data management and control functionality necessary to provide network discovery and selection assistance data per operator's policy. VASU 006232-544 at 292. ANDSF may provide other information, including access network discovery information, WLAN selection information, and ePDG configuration information. VASU 008198-326 at 252. If the UE is roaming in a VPLMN, the UE may receive Inter-system mobility policies or access network discovery information from H-ANDSF or V-ANDSF or both. *Id.*

Moreover, access network selection and traffic steering between 3GPP access and WLAN is supported using ANDSF and is also supported using radio access network rule procedure without ANDSF. VASU 006232-544 at 290.

The home network preference may be provided by the Accused Products' HPLMN and include information that assists the UE to select a WLAN network and to select a PLMN for 3GPP-based authentication over WLAN. VASU 006232-544 at 297. Similarly, a visited network preference may be provided by the VPLMN, but UE shall ignore the preference if provided a HPLMN preference. *Id.*

Activation of Timer

Through a timer (pre-defined time window), the switching system causes the second communication module (Wi-Fi framework/Wi-Fi firmware/VoWiFi) to change state from a sleep mode to a stand-by mode, then from the stand-by mode to an active mode before switching the first communication link to the second communication module.

There are a number of ways that a timer is activated to wake up the second communication module (mobile call functions) in the Accused Products to change from a sleep state to an active state and establish time window of a pre-defined size.

(1) The Accused Products activate a timer through Doze to improve battery life by monitoring device use and wakefulness. VASU 025192-97 at 92. Through Doze, the Accused Products that are idle (stationary or having the screen off) periodically (timer) enter a maintenance window, during which apps can complete pending work. *Id.* at 93. Doze resumes sleep for a longer period, followed by another maintenance window. *Id.* The platform continues this sleep and maintenance alternation until a maximum of sleep time (a few hours). *Id.* (Android 7.0 and higher triggers a lighter set of optimizations). During Doze, Wi-Fi scan is not performed. *Id.* at 93. But the platform exits Doze (from sleep state to an active mode) by user interaction, device movement, turning on the screen, or imminent AlarmClock alarm (another timer). *Id.* at 94.

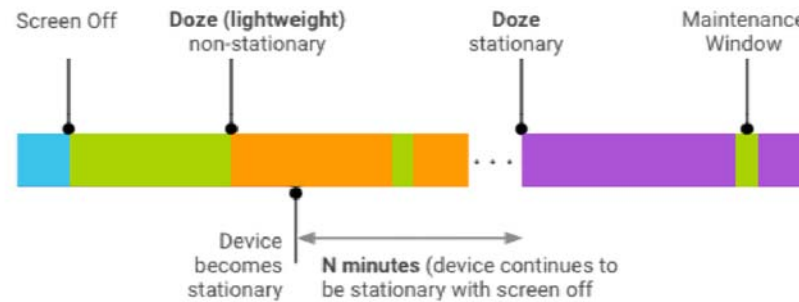


Figure 1. Doze modes for nonstationary and stationary devices.

Id. at 94 (showing the Doze mode in sleep and active alteration). Doze can be enabled when the Accused Products have a cloud messaging service. *Id.* at 95.

	To enable Doze for a device: 1. Confirm that the device has a cloud messaging service installed. 2. In the device overlay config file <code>overlay/frameworks/base/core/res/res/values/config.xml</code>, set <code>config_enableAutoPowerModes</code> to <code>true</code>: <pre><bool name="config_enableAutoPowerModes">true</bool></pre> <i>Id.</i> (how to enable Doze). When the Accused Products exit Doze by the triggering events, the Accused Products can change from sleep state (idle) to an active state and resume Wi-Fi scan by the second communication module. (2) The Wi-Fi network selection functions in the Wi-Fi framework (the second communication module) continuously evaluate the quality of the connected network and assess the quality of available networks. VASU 025102-18 at 02. The Accused Products scan the available networks depending whether the screen of the Accused Products is on or off. <i>Id.</i> The Wi-Fi framework triggers scan decisions at increasing interval (timer) when the screen is turned on. <i>Id.</i> at 06. The scan decision intervals are configured (config_wifiDisconnectedScanIntervalScheduleSec, config_wifiConnectedScanIntervalScheduleSec, and config_wifiSingleSavedNetworkConnected ScanIntervalScheduleSec). <i>Id.</i> By default, the scans occur at exponential intervals (timer) of 20, 40, 80, and 160 seconds. <i>Id.</i> If the screen of the Accused Products is on and the Accused Products is connected, the Wi-Fi framework evaluates whether the current network is good enough to skip network selection when all the following conditions are met: (1) the RSSI is above the required received signal strength indicator (“RSSI”) threshold (predefined size) or sufficient traffic is flowing over the connection; (2) the network is evaluated, or user approved for use without internet access; and (3) the network is unmetered. <i>Id.</i> at 03. If the connection isn’t good enough, the connectivity subsystem triggers a scan to detect available networks. <i>Id.</i> Moreover, if the screen is on and the Accused Products are disconnected, the Android connectivity system issues periodic scans (activation of a timer) following an exponential back off schedule (increasing the
--	---

waiting time between retries). *Id.* at 02. The module evaluates scan results received by evaluating if the signal level is below a predefined threshold and tries to select the best network to connect to. *Id.*

When the screen is off and the Accused Products are disconnected, the Accused Products program the firmware with a list of preferred networks using preferred network offload (“PNO”) scans when the screen goes off. *Id.* The firmware wakes the host from sleep mode to active mode if it finds any of the preferred networks. *Id.*

The `WifiManager#allowAutoJoinGlobal(boolean)` method can be used to disable automatic connections. This is a privileged API that can be used by device manufacturers in limited circumstances (for example, a nonmobile, preconfigured device).

If the device is connected and the `config_wifi_framework_enable_associated_network_selection` overlay is set to `false`, no connectivity scans are performed and scan results don't trigger network selection. This setting has no effect when the device is disconnected, meaning that connectivity scans and network selection still occur.

Id. at 03 (showing WifiManager in Android disables automatic connections).

The scan results are filtered to remove Basic Service Set (“BSS”) Identifiers (“BSSIDs”) that have an RSSI below the entry RSSI (configurable), shown below.

The scan results are *filtered* to remove BSSIDs that have an RSSI below the entry RSSI (configurable using the `config_wifi_framework_wifi_score_entry_rssi_threshold_24GHz`, `config_wifi_framework_wifi_score_entry_rssi_threshold_5GHz`, and `config_wifiFrameworkScoreEntryRssiThreshold6ghz` overlays). Additionally,

Id. at 04.

When the screen of the Accused Products is on, Wi-Fi service calculates a connected score based on RSSI and link-layer stats. *Id.* at 05. Moreover, the Wi-Fi service may pass the score to the connectivity service (a switching system), which uses the score to determine whether to connect to a Wi-Fi network or to a mobile network. *Id.* at 06.

	When the Accused Products' screen is off, the network selection process might occur if scans are initiated by other services such as location services. <i>Id.</i> at 06. The Wi-Fi firmware evaluates the network quality and if the network quality is bad, the firmware might roam or disassociate from the network and wake up the Accused Products from a sleep mode to an active mode. <i>Id.</i> The RSSI threshold values are (1) above -73 dBm for the 2.4 GHz band, configured with the <code>config_wifi_framework_wifi_score_low_rssi_threshold_24GHz</code>, (2) -70 dBm for the 5 Ghz and 6 Ghz bands, configured with the <code>config_wifi_framework_wifi_score_low_rssi_threshold_5GHz</code> and <code>config_wifiFrameworkScoreLowRssiThreshold6ghz</code>. <i>Id.</i> at 07. When the device is connected and screen is on, a connected scorer periodically monitors Wi-Fi quality by looking at signals such as RSSI and the number of packets transferred. <i>Id.</i> at 07. If Wi-Fi quality is determined to be bad, and the device supports dual concurrent stations, a scan will get triggered. <i>Id.</i> The <code>config_wifiLowConnectedScoreThresholdToTriggerScanForMbb</code> can be used to configure the score threshold that triggers the scanning, and the <code>config_wifiLowConnectedScoreScanPeriodSeconds</code> can be used to configure the period of these scans. <i>Id.</i> (3) When the screen is off and Wi-Fi is disconnected, the Wi-Fi firmware (the second communication module) performs preferred network offload ("PNO") scanning for SSIDs. <i>Id.</i> at 08. The Wi-Fi framework configures the firmware with a list of SSIDs to scan for and a list of channels on which to scan. <i>Id.</i> If a configured SSID is found, the Wi-Fi firmware wakes the framework from a sleep mode to an active mode. <i>Id.</i> The Wi-Fi framework also configures the interval (timer) at which the firmware is to perform PNO scans, using the device mobility state to select different scan intervals. <i>Id.</i> In a low mobility state (the device is stationary), the interval is 60 seconds for the first three scans (controlled by <code>config_wifiStationaryPnoScanIntervalMillis</code>) and 180 seconds for subsequent scans. <i>Id.</i> In a high mobility state, the interval is 20 seconds for the first three scans (controlled by <code>config_wifiMovingPnoScanIntervalMillis</code>), and 60 seconds for subsequent scans. <i>Id.</i> If the signal monitor in Wi-Fi framework/Wi-Fi firmware or switching system such as "Switch to mobile data" and "Switching to better Wi-Fi networks" detect that the alternative signal level is below a second predefined threshold value, a second time window of a pre-defined size is activated with a third pre-defined threshold value.
--	--

	In an exemplary scenario, when the screen of the Accused Products is on, and the Wi-Fi service may poll RSSI and link-layer stats every 3 seconds (the first time window with a pre-defined size) or by other configuration (config_wifiPollRssiIntervalMilliseconds or config_wifiAdjustPollRssiIntervalEnabled for dynamic adjustment based on the device mobility state and RSSI). <i>Id.</i> at 05. The polling interval is extended to 6 seconds when the device is stationary and RSSI is above -68 dBm (configured by the config_wifiClientRssiMonitorThresholdDbm and config_wifiClientRssiMonitorHysteresisDb), which is the second pre-defined threshold value. <i>Id.</i> The polling interval is reduced back to 3 seconds (the second time window with a pre-defined size, configured by the config_wifiPollRssiIntervalMilliseconds) when the device is non-stationary or RSSI is below -73 dBm, which is the third pre-defined threshold value and smaller than the second pre-defined size (-68 dBm). <i>Id.</i> <u>Termination of the Established Communication</u> The Accused Products will terminate a wireless communication link when appropriate, according to its connection criteria and signal strength.
--	---

For example, in the representative Accused Product—the Galaxy S22—screenshot below, the device sent a DEAUTH command when the RSSI value was -84 dBm, thereby terminating the Wi-Fi connection.

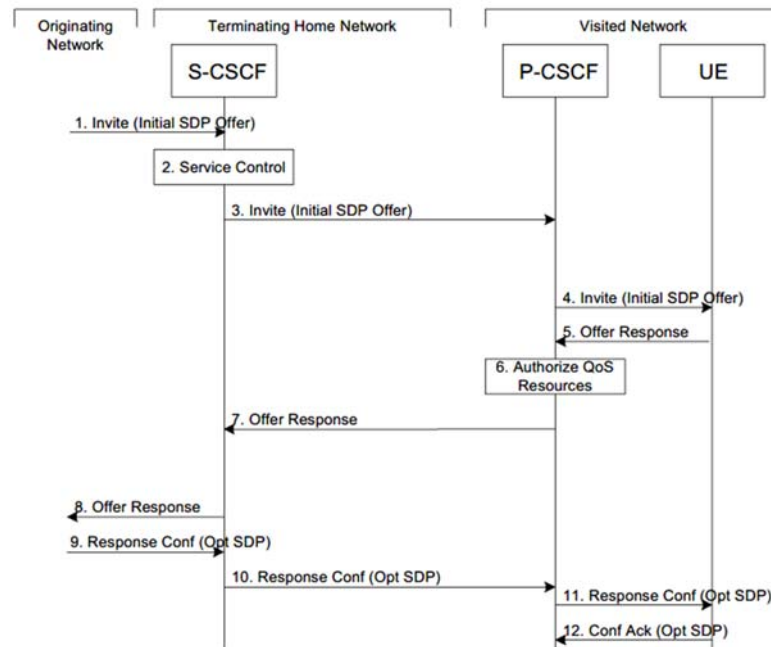


VASU 031389-98 at 97.

The SCC AS notifies the Accused Products through the service control signaling path to terminate transmitting over the first communication link (access leg) with the first wireless network.

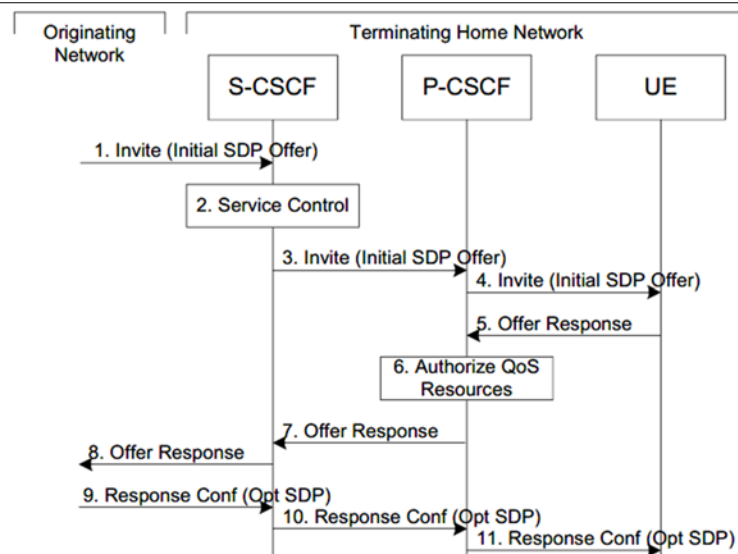
The termination procedures specify the signaling path between the S-CSCF assigned to perform the session termination service and the Accused Products. VASU 005263-653 at 392. The signaling path is determined at the time of UE registration and remains fixed for the life of the registration. *Id.*

When registration is completed in the roaming scenario, S-CSCF knows the name/address of its next hop in the signaling path and the P-CSCF, and P-CSCF knows the name/address of the UE. *Id.*



VASU 005263-653 at 393 (mobile termination procedure during roaming scenario).

When registration is completed in non-roaming scenario, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE. *Id.* at 395.



Id. at 395 (mobile termination procedure during non-roaming scenario).

For detection of conditions requiring session transfer, the Accused Products establish an access leg with the SCC AS via the transferred-in wireless network to request session transfer to the transferred-in wireless network. VASU 005654-93 at 70. When the UE initiates a session transfer request, it includes the session transfer identifier. *Id.* The SCC AS executes the session transfer procedure by replacing the access leg currently communicating to the remote leg (the first communication link) with the access leg established via the transferred-in access (the second communication link). *Id.* The access leg established via the transferred-out wireless network is subsequently released (terminating the first communication link). *Id.*

If the SCC AS detects that the Accused Products are not reachable over Service Control Signaling Path, the SCC AS should clear all held sessions related to the user if any are present and update the remote leg if necessary. VASU 005865-953 at 912.

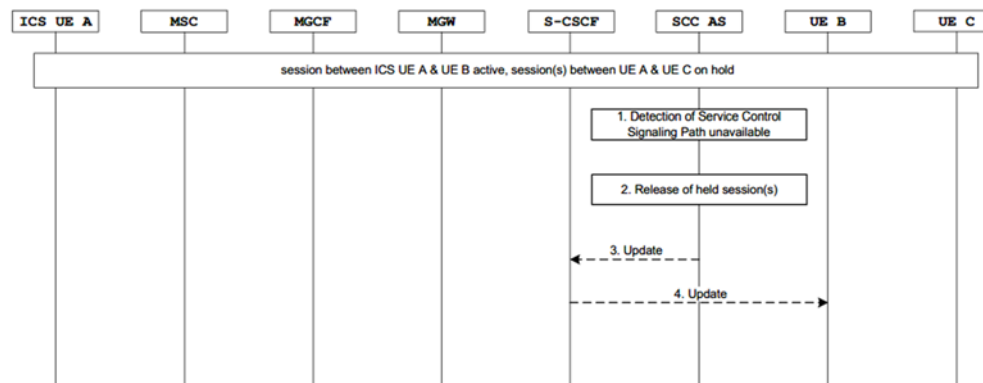


Figure 7.5.1.1.3-1: release of held sessions at SCC AS when Service Control Signalling Path unavailable

VASU 005865-953 at 912.

A delete session request message will notify the Accused Products (UEs) to terminate transmission of the first call session with the first wireless network (transfer-out). The “Delete Session Request” (shown below) is sent over the S2b interface of EPC as part of the following procedure: UE/ePDG initiated detach, UE requested disconnection with packet data network (“PDN”), or HSS/AAA initiated detach. VASU 009199-578 at 307.

	SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)			
32	Create Session Request		X	
33	Create Session Response			X
36	Delete Session Request		X	
37	Delete Session Response			X

VASU 009199-578 at 226.

Redirect to the Second Communication

The Accused Products redirect to the second communication link to maintain the connection by the mobile communication device to transparently maintain a connection.

For example, in the representative Accused Product—the Galaxy S22—screenshot below, the device shows a connection to both the 5G cellular network and a WiFi network.



VASU 031389-98 at 98.

The Accused Products, upon receiving a request for execution of session transfer, use the SCC AS (interface server) to perform the access leg update by switching (re-directing) the access leg communicating with the remote leg from transferring-out access to transferring-in access. VASU 005654-93 at 70. The SCC AS subsequently coordinates the session control signaling exchange between the access

leg and the remote leg associated with a subscriber IMS session, thereby establishing a second wireless communication link between the Accused Products and the second wireless network. *Id.*

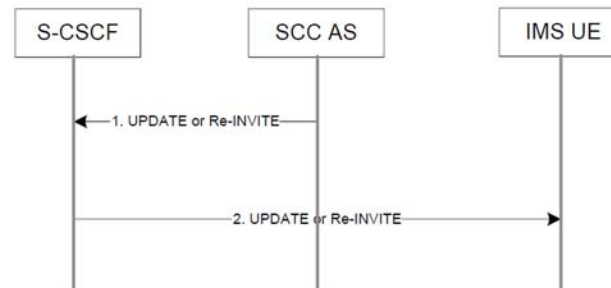


Figure 6.3.1.5-1: Access Leg Update toward the remote end

VASU 005654-93 at 71 (how access leg is updated toward the remote end). The SCC AS updates the access leg by communicating the session description protocol (“SDP”) of the Access leg established in the transferring-in access to the remote end via the user’s S-CSCF. *Id.*

When the Accused Products determine that the access transfer is desirable because the signal strength drops below a pre-determined threshold based on criteria such as operator policy or user preferences, a registration in IMS is performed by the UE via the transferring-in wireless network if the user is not already registered via that network. VASU 005654-93 at 69.

The create session request is part of the procedure to hand over to untrusted or trusted non-3GPP access from ePDG/TWAN to PGW via S2b interface of EPC. VASU 009199-578 at 234. The ePDG/TWAN may

	include AAA server identifier in the create session request to the PGW through S2a/S2b interface. VASU 009199-578 at 247 (information element in a create session request). <table border="1"> <thead> <tr> <th></th><th>SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)</th></tr> </thead> <tbody> <tr> <td>32</td><td>Create Session Request</td></tr> <tr> <td>33</td><td>Create Session Response</td></tr> <tr> <td>36</td><td>Delete Session Request</td></tr> <tr> <td>37</td><td>Delete Session Response</td></tr> </tbody> </table> VASU 009199-578 at 226 (message types for GRPS Tunneling Protocol in PLMN). The direction of the message is from MME/S4-SGSN to SGW, from SGW to PGW, and from ePDG/TWAN to PGW. VASU 009199-578 at 233. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.		SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)	32	Create Session Request	33	Create Session Response	36	Delete Session Request	37	Delete Session Response
	SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)										
32	Create Session Request										
33	Create Session Response										
36	Delete Session Request										
37	Delete Session Response										
Claim 12											
12[pre]. A method comprising:	As described in Element 1[pre], the Accused Products (also referred to as user equipment, UEs) perform every step of the method of the claims through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi Settings” or “Wi-Fi preferences,” “Wi-Fi Settings,” or “Advanced Wi-Fi Settings” of the Accused Products.³ The feature allows the Accused Products to roam and switch between different wireless networks, such as a WiFi wireless network and cellular networks including General Packet Radio Service (“GPRS,” 2G), Global System for Mobile (“GSM,” 2G), Code-Division Multiple Access (“CDMA,” 3G), Long Term Evolution (“LTE,” 4G), or 5G network.										

³ These features were previously branded as “Smart Network Switch” and “Adaptive Wi-Fi.”

	<u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
12[a]. detecting a first context;	The Accused Products include a switching system to determine a first context of a first established communication link, “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi Settings” in A Series, S Series, X Cover, and Z Series. VASU 010302-454 at 398 (A13 5G); VASU 010601-745 at 691 (A14 5G); VASU 011048-196 at 143 (A23 5G/A23 5G UW); VASU 011532-691 at 633 (A53 5G/A53 5G UW); VASU 011692-852 at 792 (A54 5G); VASU 018745-906 at 848 (S20 FE 5G); VASU 019244-407 at 351 (S21 5G/ S21 Ultra 5G/ S21+ 5G); VASU 019782-949 at 895 (S22/S22+/S22 Ultra); VASU 019950-20128 at 1070 (S23/S23+/S23 Ultra); VASU 023406-563 at 508 (XCover Pro); VASU 023564-725 at 672 (Z Flip 5G); VASU 023894-4071 at 1014 (Z Fold3 5G/Z Flip3 5G); VASU 024756-929 at 877 (Z Flip4); VASU 024408-577 at 520 (Z Fold2 5G). Similarly, the Accused Products include another switching system to do the same, “Switch to Mobile Data” product feature under “Wi-Fi Preferences.” VASU 012187-372 at 300 (Amp Prime 3); VASU 012624-795 at 737 (J2); VASU 013258-446 at 375 (J7); VASU 013447-617 at 557 (J7 V); VASU 012938-3112 at 1050 (J7 Prime); VASU 017373-567 at 490 (S7); VASU 016965-7166 at 1090 (S7 Active); VASU 017167-372 at 294 (S7 Edge); VASU 013837-4053 at 986 (Note 9).

	Wi-Fi preferences Customize advanced Wi-Fi services. 1. From  Settings, tap Connections > Wi-Fi, and then tap On/Off to turn on Wi-Fi. 2. Tap  More options > Advanced. To view all network settings, tap View more. • Switch to mobile data: Connect automatically to a mobile network connection when the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi. • Turn on Wi-Fi automatically: Enable Wi-Fi in frequently used locations. • Wi-Fi power saving mode: Reduce battery usage by analyzing Wi-Fi traffic patterns. • Wi-Fi notifications: Receive notifications when open networks in range are detected. • Show Wi-Fi pop-up: When opening apps, indicate when Wi-Fi is available. VASU 013837-4053 at 3977. Moreover, the Accused Products include a similar switching system, “Switch to Mobile Data” product feature in “Advanced Wi-Fi Settings” to switch between mobile and Wi-Fi networks. VASU 009579-721 at 669 (A02s); VASU 009855-10011 at 116 (A10e); VASU 010011-157 at 104 (A11); VASU 010158-301 at 250 (A12); VASU 010455-600 at 546 (A13); VASU 010746-901 at 851 (A20); VASU 010902-1047 at 996 (A21); A51_User_Manual.pdf at 116 (A51); VASU 011197-367 at 315 (A51 5G/A51 5G UW); VASU 011368-531 at 477 (A52 5G); VASU 011853-2015 at 958 (A71 5G); VASU 012016-2186 at 2134 (A71 5G UW); VASU 015086-267 at 209 (Note 10+); VASU 014054-245 at 191 (Note 20 5G/Note 20 Ultra 5G); VASU 017730-891 at 838 (S8), VASU 017568-729 at 676 (S8 Active); VASU 017892-8059 at 8006 (S8+); VASU 018060-236 at 183 (S9/S9+); VASU 018399-571 at 511 (S10/S10e/S10+); VASU 018237-398 at 345 (S10 Lite); VASU 018907-9076 (S20 5G/S20 Ultra 5G/S20+ 5G); VASU 024244-407 at 348 (Z
--	---

Fold); VASU 023090-256 at 199 (XCover 6 Pro); VASU 023257-405 at 358 (XCover FieldPro); VASU 012482-623 at 570 (J2 Pure); VASU 012796-937 at 890 (J3); VASU 013113-257 at 209 (J7 Star).

Advanced Wi-Fi settings

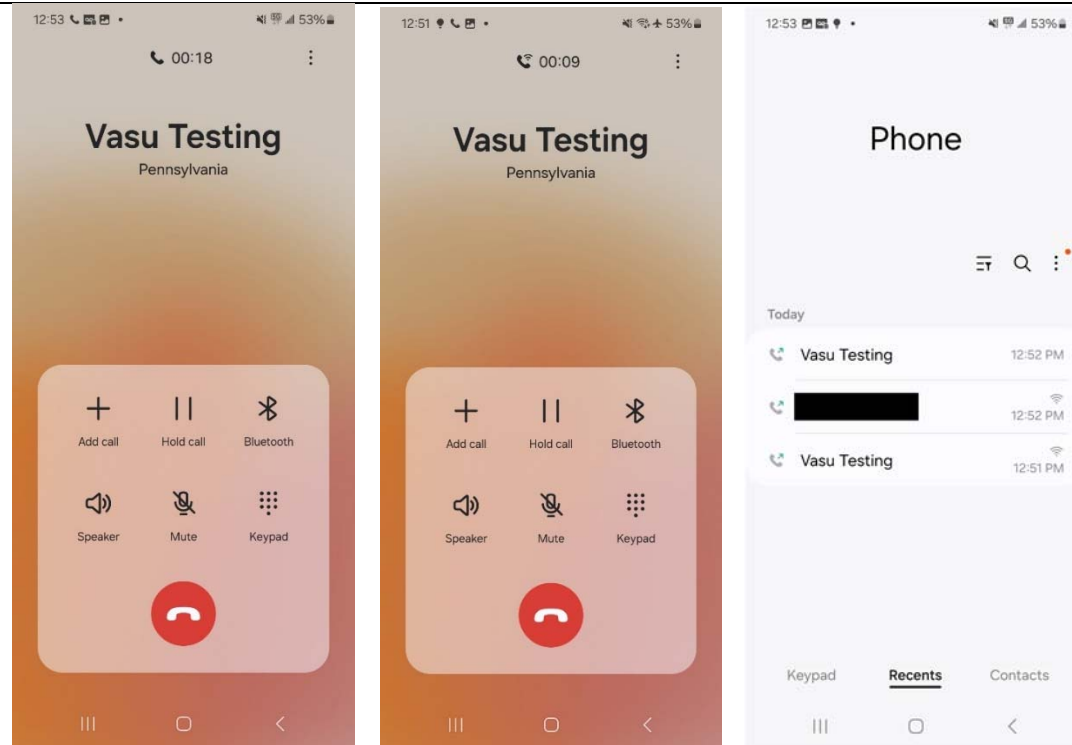
You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by carrier.

1. From Settings, tap  **Connections** > **Wi-Fi**, and then tap  to turn on Wi-Fi.
2. Tap  **More options** > **Advanced**.
 - **Sync with Samsung Cloud/account:** Sync Wi-Fi profiles with your Samsung account.
 - **Switch to mobile data:** When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi.
 - **Turn on Wi-Fi automatically:** Turn on Wi-Fi in frequently-used locations.
 - **Detect suspicious networks:** Get notified when suspicious activity is detected on the current Wi-Fi network.

VASU 010455-600 at 546.

The Accused Products “Intelligent Wi-Fi” product feature is another switching system in “Wi-Fi Settings,” which monitors the first context of a first communication link and switches between mobile and Wi-Fi networks depending on the signal strength. VASU 020129-301 at 243 (S24/S24+/S24 Ultra); VASU 024756-929 at 874 (Z Fold4/Z Flip4).

	Wi-Fi settings You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider. 1. From Settings, tap  Connections > Wi-Fi, and then tap  to turn on Wi-Fi. 2. Tap  More options for the following options: • Wi-Fi Direct: Share data directly between devices over Wi-Fi. • Intelligent Wi-Fi: Configure Wi-Fi switching and detection features. • Advanced settings: Configure Wi-Fi connections and Hotspot settings. • Contact us: Contact Samsung support through Samsung Members. VASU 024756-929 at 874 (Z Fold4/Z Flip4). The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching context. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module (further described in Element 1[b]). This first communication link is over a first type of wireless network, either a Wi-Fi network or a PLMN or Cellular Network. With respect to a voice call, it can be initiated within the Wi-Fi network or over the PLMN/Cellular Network. <i>Compare</i> left screenshot (illustrating a cellular call via 5G by the lack of Wi-Fi symbol in the top ribbon and showing 5G cellular connectivity), <i>with</i> middle screenshot (illustrating a WiFi call by noting the phone is in airplane mode and by bearing a Wi-Fi symbol above the phone symbol); <i>see also</i> right screenshot (showing two calls made to the contact “Vasu Testing” where the earlier call has a Wi-Fi symbol above the time indicating a Wi-Fi call and the later call does not have a Wi-Fi symbol above the time indicating a cellular call).
--	---



VASU 031389-98 at 93-95.

The first connection link between the Accused Product and end destination device can be made under at least three scenarios: (1) Wi-Fi to Wi-Fi connection, (2) Wi-Fi to Home PLMN, and (3) Wi-Fi to Visitor PLMN. The vice versa is also true. Wi-Fi, Home PLMNs, and Visitor PLMNs are type of wireless networks.

The Accused Products established the calls via a wireless communication link with PLMN through gateways and interfaces supported by Evolved Packet Core (“EPC”) functions. EPC can be accessed via a trusted or untrusted network. There are differences when accessing these types of networks. However, the differences are not relevant to whether the Accused Products establish a communication link with an end destination device.

The Supported EPC Functions

Trusted WLAN Access Network (“TWAN”): For access to PLMN’s EPC via a trusted non-3GPP access network such as trusted TWLAN, a connection shall be established between the Accused Products and TWAN using specific signal procedures. VASU 008198-326 at 230. Access authentication signaling for access to the EPC shall be executed between the Accused Products and the AAA server, which is an interface server, to ensure mutual authentication of the user and the EPC. *Id.* at 230.

Evolved Packet Data Gateway (“ePDG”): ePDG is the local mobility anchor within untrusted non-3GPP access. VASU 006232-544 at 262. The PLMNs included in the ePDG information are the PLMNs that have roaming agreements with HPLMN. VASU 006232-544 at 269.

Through a network interface (Swn interface), the ePDG connects with an untrusted non-3GPP access. VASU 005019-113 at 92. The ePDG connects with the Accused Products (through the SWu interface) to establish data tunnels and user data packet transmission within the tunnels. *Id.* at 93.

Call Session Control Function (“CSCF”): CSCF can act as Proxy CSCF (“P-CSCF”), serving CSCF (“S-CSCF”), emergency CSCF (“E-CSCF”), or Interrogating CSCF (“I-CSCF”). VASU 005019-113 at 56. The P-CSCF is the first contact point for the Accused Products within the International Mobile Subscriber Identity (“IMSI”); the S-CSCF actually handles the session states in the network; the E-CSCF handles emergency sessions such as routing an emergency requests to the correct emergency center; the I-CSCF is the contact point within an operator’s network for all IMS connections destined to a subscriber of that network operator or roaming subscriber located within the network operator’s service area. *Id.*

Home Subscriber Server (“HSS”): The HSS supports the authentication procedures to access CS domain, PS domain, and system services by storing the generated data for authentication, integrity, and ciphering and by providing these data to the appropriate entities including AAA server or CSCF. VASU 005019-113 at 41. The diagram below illustrates . . .

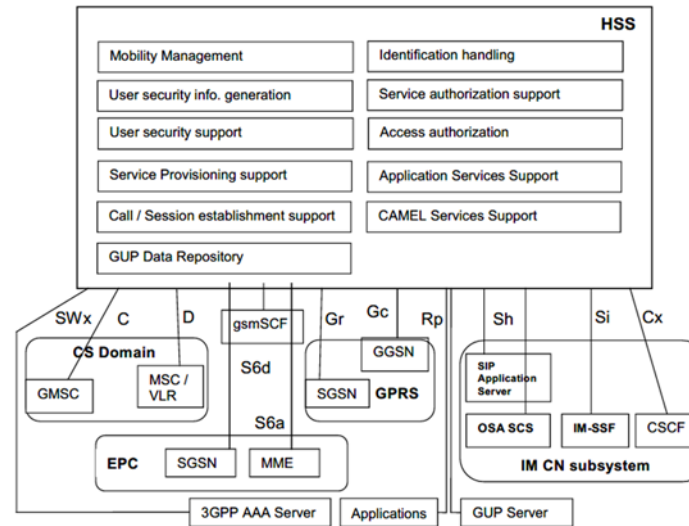


Figure 0.b: HSS logical functions

VASU 005019-113 at 40.

Authentication, Authorization, and Accounting (“AAA”): The Accused Products is authenticated and authorized through AAA to roam between networks. AAA server (interface server) is located at HPLMN and provides support for non-3GPP access users with services like authentication, authorization, and location management services to access evolved packet systems (“EPS”) in mobile networks. VASU 005019-113 at 49. It interacts with HSS to maintain consistent information to support service continuity between 3GPP (mobile networks) and non-3GPP (Wi-Fi) networks. *Id.* It contains user information to gain access to non-3GPP access. *Id.* Non-3GPP access authentication defines the process to permit or deny a subscriber to attach to and use the sources of a non-3GPP IP access interworked with the EPC network. VASU 006232-544 at 307. Non-3GPP access authentication signaling is executed between the Accused Products and the AAA server/HSS (interface server). *Id.* During the authentication of the Accused Products for accessing the EPC via ePDG, ePDG shall initiate EAP-AKA based authentication between the Accused Products and the AAA server. VASU 006232-544 at 279.

Roaming Scenarios After the Accused Products Establish a Call

Exemplary Scenario 1: Wi-Fi to Wi-Fi

- (2) The Accused Products initiate a call within a first Wi-Fi network through VoIP or VoWiFi and roam from a first Wi-Fi network to a second Wi-Fi network.

The Accused Products may go out of range of access points and shift network association to another access point without losing connection. VASU 025133-44 at 134. Weak signals can trigger roaming on the Accused Products. *Id.* The Accused Products support 802.11k and 802.11v standards to reduce the length of time of lost connectivity during basic service set (“BSS”) transition. *Id.* at 138-42.

Exemplary Scenario 2: Wi-Fi to Home PLMN

- (3) The Accused Products initiate a call over a first Wi-Fi network through VoIP or VoWiFi and roam from the first Wi-Fi network to the coverage area of the home PLMN (“HPLMN”) of the Accused Products.
- (4) The Accused Products initiate a call within a first Wi-Fi network, but set up a backend of the call over PLMN network and roam from the first Wi-Fi network to the coverage area of the HPLMN of the Accused Products.

In a non-roaming scenario when the Accused Products establish the communication link with a home network, the trust relationship of Wi-Fi (non-3GPP IP wireless network) is determined by the HPLMN operators. VASU 008198-326 at 227. The trust relationship is indicated to the Accused Products via either pre-configured policies in the Accused Products by the home PLMN operator or dynamic indication during 3GPP-based access authentication. *Id.*

	Authorization of EPC access shall be performed by the AAA server upon successful user authentication. <i>Id.</i> <u><i>Exemplary Scenario 3: Wi-Fi to Visitor PLMN</i></u> (3) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over VoIP or VoWiFi, and roam from the first Wi-Fi network to the coverage area of a visitor PLMN (“VPLMN”) of the Accused Products. (4) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over a HPLMN, and roam from the first Wi-Fi network to the coverage area of a VPLMN. In roaming scenario when the Accused Products establish the communication link with a visitor network, the HSS or AAA server (interface server) in HPLMN makes the final decision if a non-3GPP wireless network is trusted or untrusted. VASU 006232-544 at 260. The HSS/AAA server (interface server) may take the visitor PLMN (“VPLMN”) policy and capability returned from the AAA proxy or roaming agreement into account. <i>Id.</i> at 260.
--	---

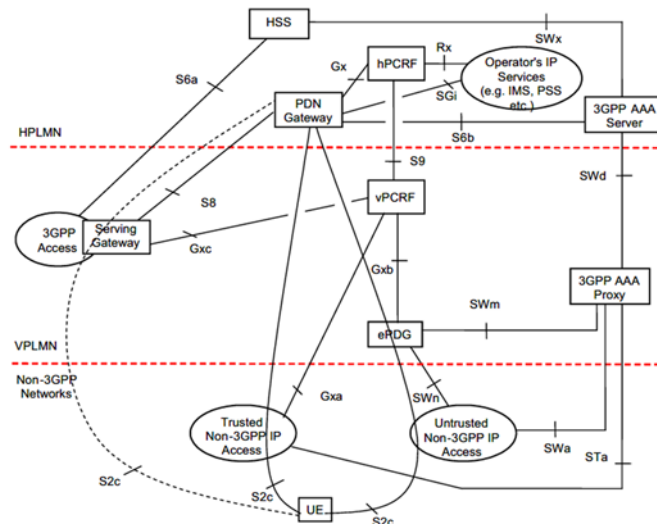


Figure 4.2.3-3: Roaming Architecture for EPS using S8 – S2c - Home Routed

VASU 006232-544 at 258 (roaming architecture showing trusted or untrusted non-3GPP IP access to AAA server/proxy in PLMN through STa or SWa interface).

The session origination procedures specify the signaling path between the Accused Products initiate a session setup attempt and the S-CSCF assigned to perform the session origination service. VASU 005263-653 at 380. The Accused Products initiate a session setup attempt and assigned a S-CSCF to perform the session origination service. VASU 005263-653 at 380. The signaling path between the Accused Products and S-CSCF is determined at the time of the Accused Products registration. *Id.* The S-CSCF to application server interface is used to provide services in the application server in the HPLMN or in a trusted external network (e.g., third-party or VPLMN). VASU 005019-113 at 58.

If the Accused Products are located in a VPLMN, it determines the P-CSCF via the CSCF discovery procedure. VASU 005263-653 at 380. The HPLMN advertises the S-CSCF as the entry point from the VPLMN. *Id.* When registration is completed, P-CSCF knows the name/address of the next hop in the signaling path toward the S-CSCF. *Id.* If the Accused Products are located in the HPLMN, the HPLMN

allocates an S-CSCF in the HPLMN. *Id.* at 383. When registration is completed, P-CSCF knows the name/address of S-CSCF. *Id.*

Determining the First Context in the First Communication Link

The Accused Products monitor the signal strength (first context) of the first communication link to the wireless network to detect context changes.

“Switch to Mobile Data” determines the first context (signal strength or user preference) to “automatically switch[] networks based on both network quality and user preferences.” VASU 025185-91 at 187. The connection manager will not be active until it accumulates enough data to determine user preference. *Id.*



Id. at 187 (determining user preference).

Through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi settings” on the Accused Products (shown below), the Accused Products can seamlessly switch to mobile data if there are signal strength issues and “whenever the Wi-Fi connection is unstable.” VASU 019950-20128 at 1070. When the Wi-Fi signal strength is strong, it switches “back to Wi-Fi.” *Id.*

	Intelligent Wi-Fi settings You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider. 1. From Settings, tap  Connections > Wi-Fi, and then tap  to turn on Wi-Fi. 2. Tap  More options > Intelligent Wi-Fi for the following options: • Switch to mobile data: When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi. • Switch to better Wi-Fi networks: Automatically switch to faster or more stable Wi-Fi networks. • Turn Wi-Fi on/off automatically: Turn on Wi-Fi in frequently-used locations. • Show network quality info: Display network information (such as speed and stability) in the list of available Wi-Fi networks. • Prioritize real-time data: Give network priority to games, video calls, and other tasks that are sensitive to lag. • Detect suspicious networks: Get notified when suspicious activity is detected on the current Wi-Fi network. • Wi-Fi power saving mode: Enable Wi-Fi traffic analysis to reduce battery usage. • Auto Hotspot connection: Automatically connect to a Wi-Fi hotspot when detected. • Intelligent Wi-Fi: View the Intelligent Wi-Fi version. VASU 019950-20128 at 1070 (intelligent Wi-Fi settings in an exemplary S23+ phone). The Accused Products measure signal strength of Wi-Fi networks by Received Signal Strength Indicator (“RSSI”), and its unit of measurement is dBm. The table below provides a point of reference for interpreting the RSSI value.
--	--

Signal Strength	TL;DR		Required for
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWi-Fi, streaming video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

VASU 025540-45 at 43-44. The screenshot below illustrate that the Accused Products continuously monitor the signal strength.

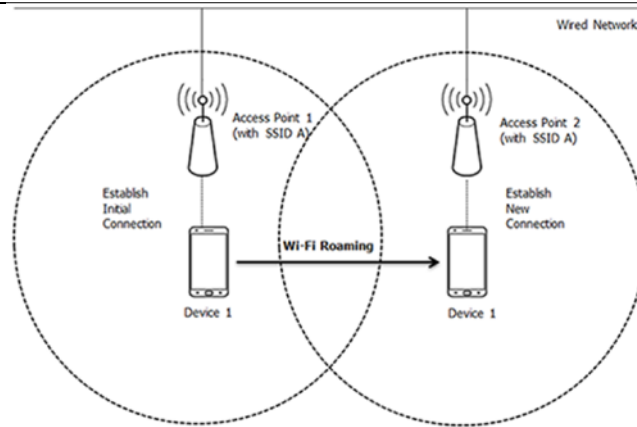


VASU 031389-98 at 96.

SOURCE CODE SUPPLEMENTATION

As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.

12[b]. detecting a second context; and	As described in Element 12[a], the Accused Products determines the second context (via signal strength by RSSI or user preference). The Accused Products also include “Auto Wi-Fi,” which turns Wi-Fi on and off depending on locations to detect context changes to a second context (signal strength via RSSI). VASU 025185-91 at 88. It turns Wi-Fi on when the favorite network is available by user preference and turns off Wi-Fi when this network is unavailable. <i>Id.</i> Auto Wi-Fi is triggered based on user’s location by geofencing (a virtual geological fence based on cellular stations). <i>Id.</i> Furthermore, The Wi-Fi network selection functions in the Accused Products continuously evaluate the quality of the connected network (context of the network) and assess the quality of available networks. VASU 025102-18 at 02. The Accused Products scan the available networks depending whether the screen of the Accused Products is on or off. <i>Id.</i> If the screen of the Accused Products is on and the Accused Products is connected, the Wi-Fi framework of the Accused Products evaluates whether the current network is good enough to skip network selection when all the following conditions are met: (1) the RSSI is above the required RSSI threshold or sufficient traffic is flowing over the connection; (2) the network is evaluated, or user approved for use without internet access; and (3) the network is unmetered. <i>Id.</i> at 2. If the connection isn’t good enough, the connectivity subsystem triggers a scan to detect available networks (a set of networks to choose for the second network). <i>Id.</i> Once connected, the Wi-Fi service calculate “a connected score” based on the RSSI and determine whether to connect to a Wi-Fi network or another network type, such as a mobile network. <i>Id.</i> at 3-4. the Wi-Fi service may pass the score to the connectivity service, which uses the score to determine whether to connect to a Wi-Fi network or to a mobile network. <i>Id.</i> at 5.
--	---



VASU 025133-44 at 34 (roaming from one Wi-Fi to another Wi-Fi access point is triggered due to weak signal).

Moreover, if the screen is on and the Accused Products are disconnected, the Android connectivity system issues periodic scans (activation of a timer) following an exponential back off schedule (increasing the waiting time between retries). *Id.* at 02. The module evaluates scan results received by evaluating if the signal level is below a predefined threshold and tries to select the best network to connect to. *Id.* When the Accused Products' screen is off, the network selection process might occur if scans are initiated by other services such as location services. *Id.* at 06.

SOURCE CODE SUPPLEMENTATION

As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.

12[c]. automatically switching, with a server, a communication in progress via a wireless network to a communication via a network based on the second context, wherein automatically switching is based on detecting the second context being preferred over the first context within a set of known networks or from a newly discovered network,	Through the switching system (described in Element 12[a]), the Accused Products automatically switch to a second network by establishing a second communication link via a wireless network (Wi-Fi or mobile network) based on the second detected context (changes in signal strength or user preference as described in Element 12[b]-12d), with a server for Wi-Fi framework/Wi-Fi firmware or interface server such as SCC AS. The second (preferred) network could be a known network (user locally stored data) or a newly discovered network (by PLMN selection procedure). VASU 008198-326 at 222. The second network could also be defined by the operator policy or user preferences. VASU 005654-93 at 64; VASU 025185-91 at 187 (describing how user preference works during switching to mobile data). Furthermore, Upon UE's request, the access network discovery and selection function ("ANDSF") in either HPLMN or VPLMN may provide a list of wireless access networks available in the vicinity of the UE for all the access technology types requested by the UE to establish a second communication link through Wi-Fi. VASU 006232-544 at 293. When the Accused Products are active in an IMS session, the session transfer procedures provide session continuity between wireless networks using signal strength information. VASU 005654-93 at 62. The Accused Products initiate session transfer procedure based on trigger criteria, including the current operator policy, user preferences, and wireless network conditions for conducting a session continuity operation to the SCC AS (interface server). VASU 005654-93 at 64. A third-party call control function (call function from the Accused Products) is employed for subscriber IMS sessions at the SCC AS upon session establishment for enablement of Session Transfer. <i>Id.</i> The first communication link (voice or video call) uses IP Multimedia Core Network Subsystem ("IMS"), which is the framework for delivering multimedia services using PS and CS bearers (data tunnels between the network gateways and the Accused Products) for the media. VASU 005654-93 at 58. IMS service continuity requires a Service Centralization and Continuity ("SCC") Application Server ("AS"). VASU 005654-93 at 63. The SCC AS is a home network based IMS application that provides functionality required to enable IMS centralized services. VASU 005865-953 at 77. The screenshot below illustrates the information used for IMS service continuity that may be provided between SCC AS and the Accused Products:
--	---

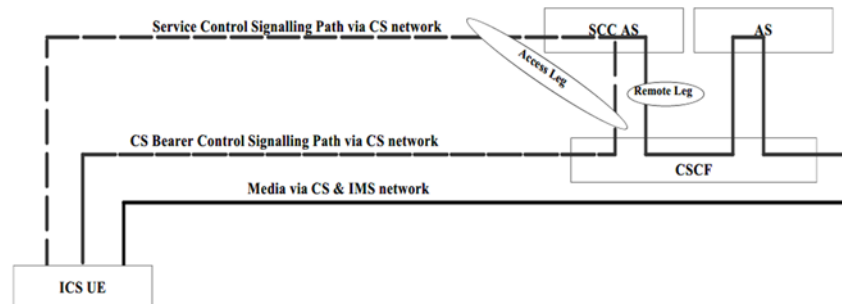


Figure 7.1.1-2: ICS UE session signalling and bearer path using CS network for Service Control Signalling Path

VASU 005865-953 at 80 (Accused Products (or UEs), session signaling and bearer path in access leg and remote leg in CS network).

Moreover, the access transfer control function (“ASCF”) is a function in HPLMN or visitor network (“VPLMN”) may be co-located with the existing functional entities such as P-CSCF. VASU 005694-864 at 720. Based on carrier policy, it shall be allocated a session transfer number (“STN-TR”) and keeps track of sessions (either in alerting state, active, or held) to be able to perform session transfer. *Id.* at 720-21. The following implementation method determines if the ASCF should be included during registration: if Accused Products are roaming, based on the roaming agreement; based on local configuration; based on registered communication service of the Accused Products; based on the access type. *Id.* at 721.

Upon session initiation, the Accused Products or the SCC AS establishes the Service Control Signaling Path for communication of service control signaling via the PS network using the Gm reference point. VASU 005865-953 at 80.

Session Continuity between Mobile Networks

When the signal strength drops below a predetermined threshold, the Accused Products may also use locally stored data for selecting a second EPC network available for connectivity via the currently selected non-3GPP wireless network to establish a second communication link. VASU 008198-326 at 222. UE shall select a PLMN according to the PLMN selection procedure of the selected non-3GPP wireless network. *Id.*

Signaling and bearer resources are allocated in the transferring-in wireless network and the user's sessions are transferred from the transferring-out wireless network. VASU 005654-93 at 669. The SCC AS executes access transfer procedures and resources in the transferring-out wireless network is released. *Id.*

The Accused Products establish the second communication link (the second call session with the second network, transferred-in network) with the transfer-in network without disrupting the first communication link in the transfer-out network. IMS sessions from and to the Accused Products are anchored at the SCC AS in the home IMS based on initial filtering criteria ("iFC") to provide service continuity for the user during the transition between two wireless networks. VASU 005654-93 at 62.

For single radio voice call continuity ("SRVCC"), voice call continuity between PLMN/VPLMN over PS and CS are anchored when the UE is capable of transmitting or receiving only one of the access networks at a given time. VASU 005195-214 at 200.

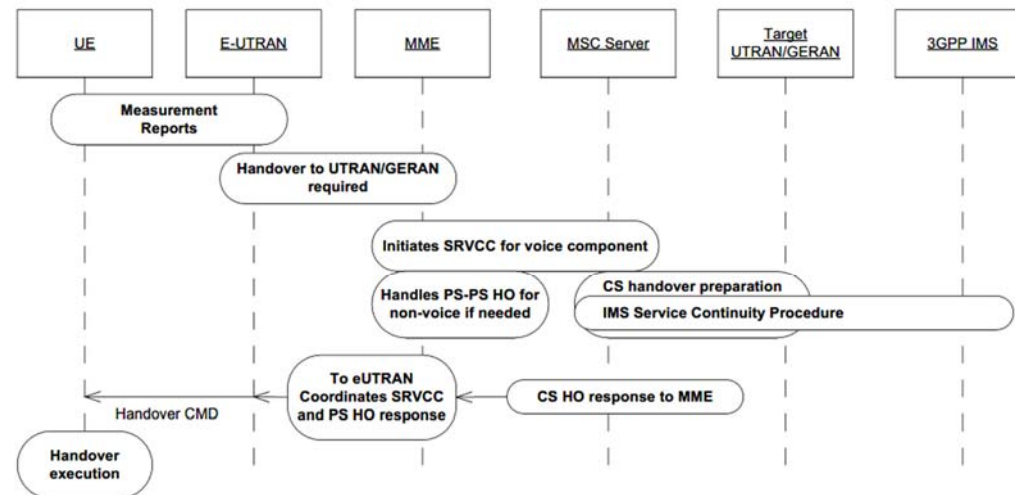


Figure 4.2.2-1: Overall high level concepts for SRVCC from E-UTRAN to UTRAN/GERAN

VASU 005195-214 at 202 (how SRVCC works in E-UTRAN, 4G to UTRAN/GERN, 3G/2G).

A third-party call control function (functions provided by the Accused Products) is employed at the SCC AS to facilitate inter-access network mobility through the user of access transfer between the two wireless networks. *Id.*

PS-CS transfer

IMS session established in CS or PS wireless networks are anchored at the SCC AS. VASU 005654-93 at 662. IMS sessions using CS bearer are established at session setup or upon access transfer. *Id.*

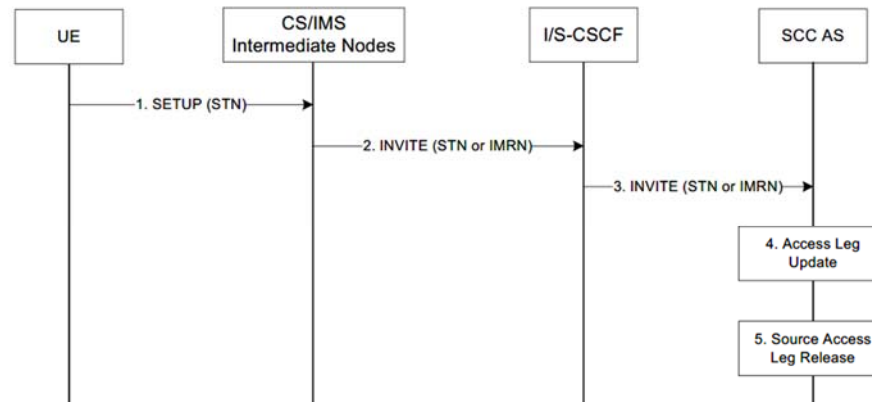


Figure 6.3.2.1.1-1: PS – CS Access Transfer: PS to CS

VASU 005654-93 at 72 (user is active in an IMS originating or terminating session using PS media at the time of transfer).

CS-PS Transfer

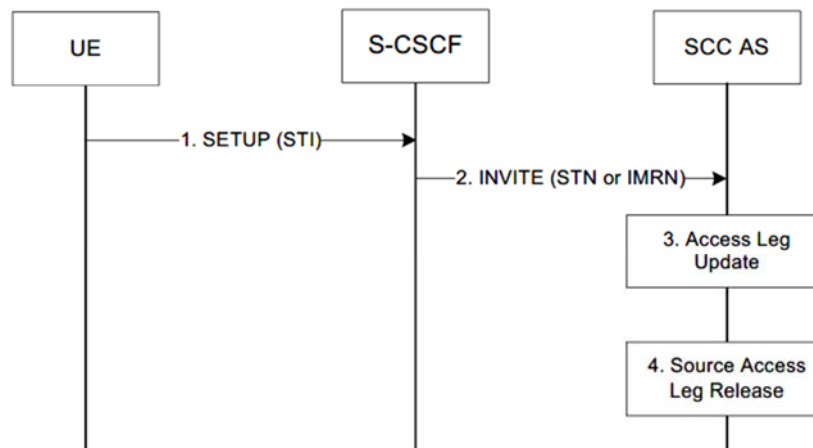


Figure 6.3.2.1.2-1: PS – CS Access Transfer: CS to PS

VASU 005654-93 at 73 (the user is active in the IMS originating or terminating session using CS at the time of transfer).

PS-PS Transfer

US is attached to one IP connectivity access network (“IP-CAN”), and it registers to the S-CSCF. VASU 005654-93 at 75. UE-1 and UE-2 establish an active multimedia session via this IP-CAN. *Id.* After changing to a new IP-CAN, obtaining new signaling and media addresses, and completing the Access Transfer procedures, UE-1 continues the session with UE-2 on the new IP-CAN. *Id.*

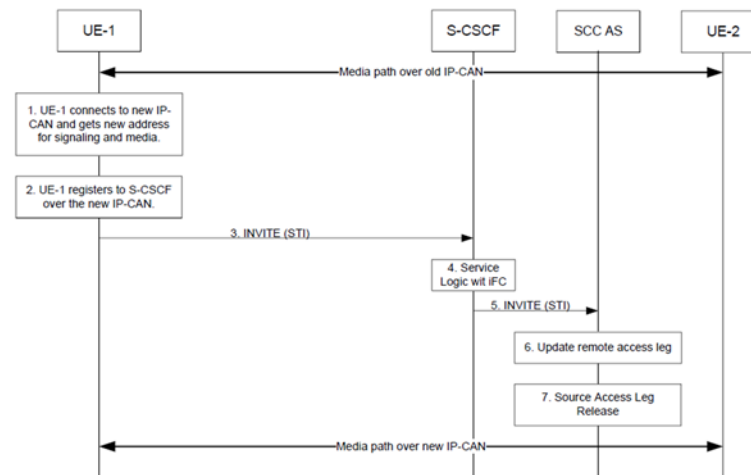


Figure 6.3.2.2.1-1: Information flow for PS-PS Access Transfer

Id.

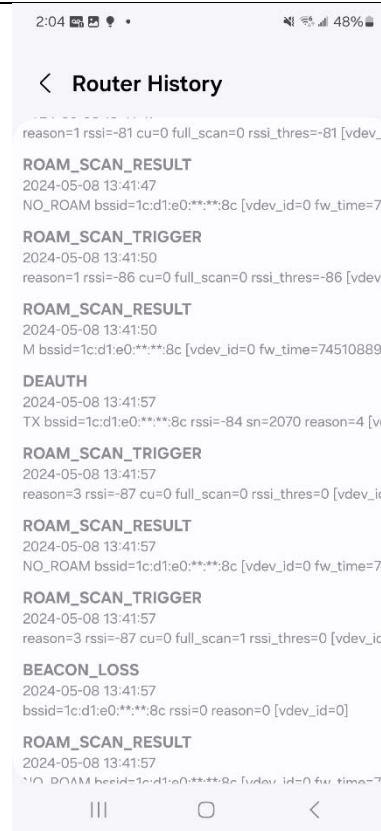
Session Continuity between Wi-Fi and Mobile Networks

Upon the Accused Products' request, the access network discovery and selection function ("ANDSF") in either HPLMN or VPLMN may provide a list of wireless access networks available in the vicinity of the UE for all the access technology types requested by the UE to establish a second communication link through Wi-Fi. VASU 006232-544 at 293. An ANDSF element located in the HPLMN of a UE is referred to as Home-ANDSF ("H-ANDSF") and an ANDSF element located in the visited PLMN of a UE is referred to as the visited-ANDSF (V-ANDSF) for this UE. VASU 006232-544 at 291. The H-ANDSF in the subscriber's HPLMN may interact with HSS user profile information. *Id.* at 61.

The ANDSF provides information for access networks that are available to the UE including:

- the access technology type (e.g. WLAN, WiMAX).
- the radio access network identifier (e.g. the SSID of a WLAN).
- other technology specific information, e.g. one or more carrier frequencies.
- validity conditions, i.e. conditions indicating when the provided access network discovery information is valid (such conditions may include e.g. a location).

	VASU 006232-544 at 293. ANDSF contains data management and control functionality necessary to provide network discovery and selection assistance data per operator's policy. VASU 006232-544 at 292. ANDSF may provide other information, including access network discovery information, WLAN selection information, and ePDG configuration information. VASU 008198-326 at 252. If the UE is roaming in a VPLMN, the UE may receive Inter-system mobility policies or access network discovery information from H-ANDSF or V-ANDSF or both. <i>Id.</i> Moreover, access network selection and traffic steering between 3GPP access and WLAN is supported using ANDSF and is also supported using radio access network rule procedure without ANDSF. VASU 006232-544 at 290. The home network preference may be provided by the Accused Products' HPLMN and include information that assists the UE to select a WLAN network and to select a PLMN for 3GPP-based authentication over WLAN. VASU 006232-544 at 297. Similarly, a visited network preference may be provided by the VPLMN, but UE shall ignore the preference if provided a HPLMN preference. <i>Id.</i> <u>Termination of the Established Communication</u> The Accused Products will terminate a wireless communication link when appropriate, according to its connection criteria and signal strength. For example, in the representative Accused Product—the Galaxy S22—screenshot below, the device sent a DEAUTH command when the RSSI value was -84 dBm, thereby terminating the Wi-Fi connection.
--	--

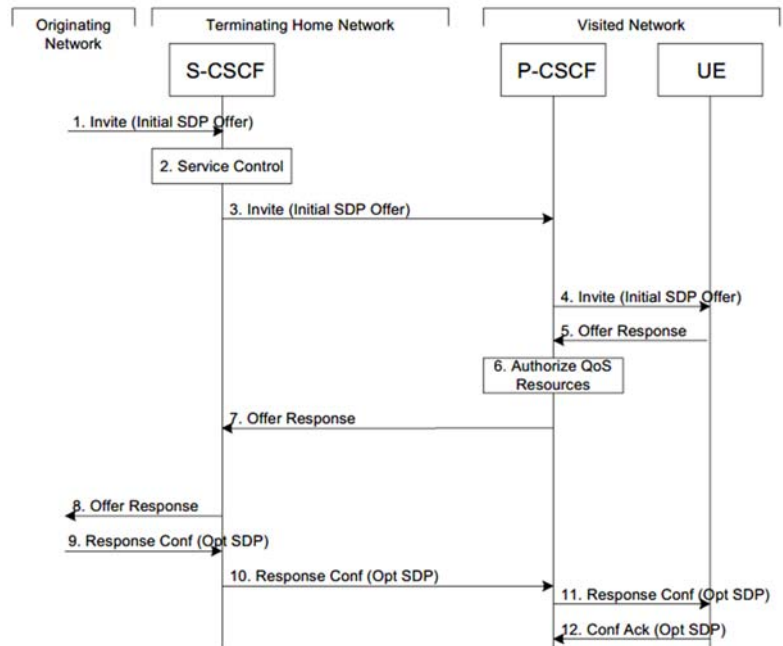


VASU 031389-98 at 97.

The SCC AS notifies the Accused Products through the service control signaling path to terminate transmitting over the first communication link (access leg) with the first wireless network.

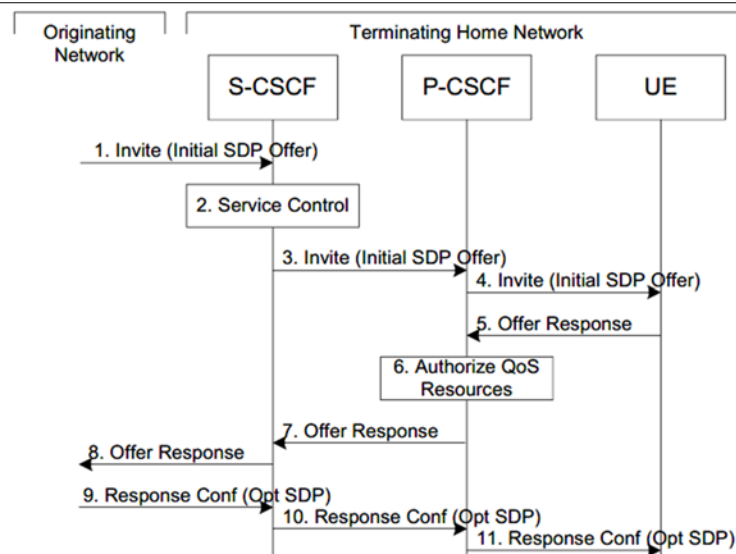
The termination procedures specify the signaling path between the S-CSCF assigned to perform the session termination service and the Accused Products. VASU 005263-653 at 392. The signaling path is determined at the time of UE registration and remains fixed for the life of the registration. *Id.*

When registration is completed in the roaming scenario, S-CSCF knows the name/address of its next hop in the signaling path and the P-CSCF, and P-CSCF knows the name/address of the UE. *Id.*



VASU 005263-653 at 393 (mobile termination procedure during roaming scenario).

When registration is completed in non-roaming scenario, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE. *Id.* at 395.



Id. at 395 (mobile termination procedure during non-roaming scenario).

For detection of conditions requiring session transfer, the Accused Products establish an access leg with the SCC AS via the transferred-in wireless network to request session transfer to the transferred-in wireless network. VASU 005654-93 at 70. When the UE initiates a session transfer request, it includes the session transfer identifier. *Id.* The SCC AS executes the session transfer procedure by replacing the access leg currently communicating to the remote leg (the first communication link) with the access leg established via the transferred-in access (the second communication link). *Id.* The access leg established via the transferred-out wireless network is subsequently released (terminating the first communication link). *Id.*

If the SCC AS detects that the Accused Products are not reachable over Service Control Signaling Path, the SCC AS should clear all held sessions related to the user if any are present and update the remote leg if necessary. VASU 005865-953 at 912.

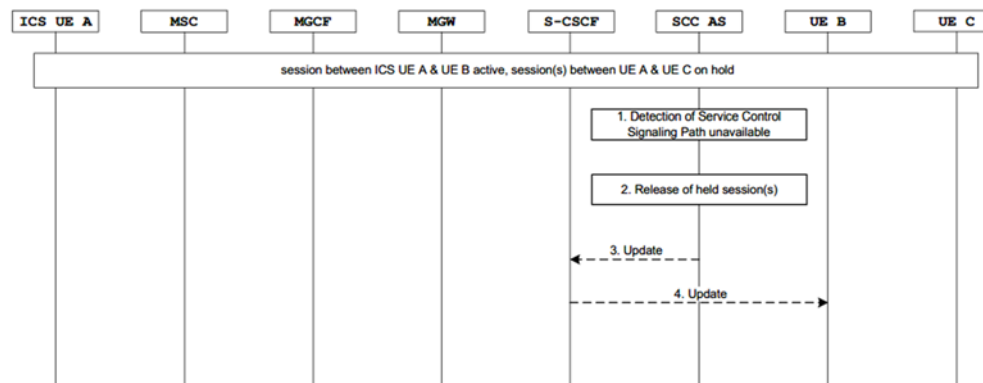


Figure 7.5.1.1.3-1: release of held sessions at SCC AS when Service Control Signalling Path unavailable

VASU 005865-953 at 912.

A delete session request message will notify the Accused Products (UEs) to terminate transmission of the first call session with the first wireless network (transfer-out). The “Delete Session Request” (shown below) is sent over the S2b interface of EPC as part of the following procedure: UE/ePDG initiated detach, UE requested disconnection with packet data network (“PDN”), or HSS/AAA initiated detach. VASU 009199-578 at 307.

	SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)			
32	Create Session Request		X	
33	Create Session Response			X
36	Delete Session Request		X	
37	Delete Session Response			X

VASU 009199-578 at 226.

Redirect to the Second Communication

The Accused Products redirect to the second communication link to maintain the connection by the mobile communication device to transparently maintain a connection.

For example, in the representative Accused Product—the Galaxy S22—screenshot below, the device shows a connection to both the 5G cellular network and a WiFi network.



VASU 031389-98 at 98.

The Accused Products, upon receiving a request for execution of session transfer, use the SCC AS (interface server) to perform the access leg update by switching (re-directing) the access leg communicating with the remote leg from transferring-out access to transferring-in access. VASU 005654-93 at 70. The SCC AS subsequently coordinates the session control signaling exchange between the access

leg and the remote leg associated with a subscriber IMS session, thereby establishing a second wireless communication link between the Accused Products and the second wireless network. *Id.*

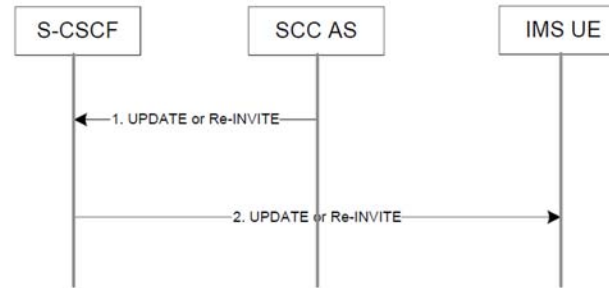


Figure 6.3.1.5-1: Access Leg Update toward the remote end

VASU 005654-93 at 71 (how access leg is updated toward the remote end). The SCC AS updates the access leg by communicating the session description protocol (“SDP”) of the Access leg established in the transferring-in access to the remote end via the user’s S-CSCF. *Id.*

When the Accused Products determine that the access transfer is desirable because the signal strength drops below a pre-determined threshold based on criteria such as operator policy or user preferences, a registration in IMS is performed by the UE via the transferring-in wireless network if the user is not already registered via that network. VASU 005654-93 at 69.

The create session request is part of the procedure to hand over to untrusted or trusted non-3GPP access from ePDG/TWAN to PGW via S2b interface of EPC. VASU 009199-578 at 234. The ePDG/TWAN may include AAA server identifier in the create session request to the PGW through S2a/S2b interface. VASU 009199-578 at 247 (information element in a create session request).

	SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)
32	Create Session Request
33	Create Session Response
36	Delete Session Request
37	Delete Session Response

	VASU 009199-578 at 226 (message types for GRPS Tunneling Protocol in PLMN). The direction of the message is from MME/S4-SGSN to SGW, from SGW to PGW, and from ePDG/TWAN to PGW. VASU 009199-578 at 233. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
12[d]. wherein upon activation of a timer, the server causes a communication module to change state from a sleep mode to a stand-by mode, and the server causes the communication module to change state from the stand-by mode to an active mode before a communication is switched to the communication module.	Through a timer (pre-defined time window), the switching system (“Switch to mobile data” or “Switch to better Wi-Fi networks”) causes the second communication module (Wi-Fi framework/Wi-Fi firmware/VoWiFi) to change state from a sleep mode to a stand-by mode, then from the stand-by mode to an active mode before switching the first communication link to the second communication module. There are a number of ways that a timer is activated to wake up the second communication module (mobile call functions) in the Accused Products to change from a sleep state to an active state and establish time window of a pre-defined size. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module. (1) The Accused Products activate a timer through Doze to improve battery life by monitoring device use and wakefulness. VASU 025192-97 at 92. Through Doze, the Accused Products that are idle (stationary or having the screen off) periodically (timer) enter a maintenance window, during which apps can complete pending work. <i>Id.</i> at 93. Doze resumes sleep for a longer period, followed by another maintenance window. <i>Id.</i> The platform continues this sleep and maintenance alternation until a maximum of sleep time (a few hours). <i>Id.</i> (Android 7.0 and higher triggers a lighter set of optimizations).

During Doze, Wi-Fi scan is not performed. *Id.* at 93. But the platform exits Doze (from sleep state to an active mode) by user interaction, device movement, turning on the screen, or imminent AlarmClock alarm (another timer). *Id.* at 94.

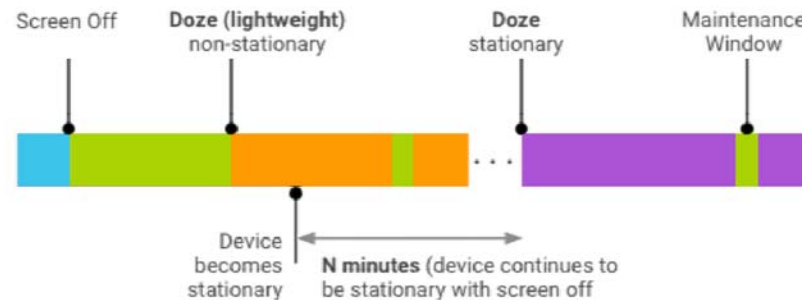


Figure 1. Doze modes for nonstationary and stationary devices.

Id. at 94 (showing the Doze mode in sleep and active alteration). Doze can be enabled when the Accused Products have a cloud messaging service. *Id.* at 95.

To enable Doze for a device:

1. Confirm that the device has a cloud messaging service installed.

2. In the device overlay config file

`overlay/frameworks/base/core/res/res/values/config.xml`, set `config_enableAutoPowerModes` to `true`:

```
<bool name="config_enableAutoPowerModes">true</bool>
```

Id. (how to enable Doze).

When the Accused Products exit Doze by the triggering events, the Accused Products can change from sleep state (idle) to an active state and resume Wi-Fi scan by the second communication module.

(2) The Wi-Fi network selection functions in the Wi-Fi framework (the second communication

	module) continuously evaluate the quality of the connected network and assess the quality of available networks. VASU 025102-18 at 02. The Accused Products scan the available networks depending whether the screen of the Accused Products is on or off. <i>Id.</i> The Wi-Fi framework triggers scan decisions at increasing interval (timer) when the screen is turned on. <i>Id.</i> at 06. The scan decision intervals are configured (config_wifiDisconnectedScanIntervalScheduleSec, config_wifiConnectedScanIntervalScheduleSec, and config_wifiSingleSavedNetworkConnected ScanIntervalScheduleSec). <i>Id.</i> By default, the scans occur at exponential intervals (timer) of 20, 40, 80, and 160 seconds. <i>Id.</i> If the screen of the Accused Products is on and the Accused Products is connected, the Wi-Fi framework evaluates whether the current network is good enough to skip network selection when all the following conditions are met: (1) the RSSI is above the required received signal strength indicator (“RSSI”) threshold (predefined size) or sufficient traffic is flowing over the connection; (2) the network is evaluated, or user approved for use without internet access; and (3) the network is unmetered. <i>Id.</i> at 03. If the connection isn’t good enough, the connectivity subsystem triggers a scan to detect available networks. <i>Id.</i> Moreover, if the screen is on and the Accused Products are disconnected, the Android connectivity system issues periodic scans (activation of a timer) following an exponential back off schedule (increasing the waiting time between retries). <i>Id.</i> at 02. The module evaluates scan results received by evaluating if the signal level is below a predefined threshold and tries to select the best network to connect to. <i>Id.</i> When the screen is off and the Accused Products are disconnected, the Accused Products program the firmware with a list of preferred networks using preferred network offload (“PNO”) scans when the screen goes off. <i>Id.</i> The firmware wakes the host from sleep mode to active mode if it finds any of the preferred networks. <i>Id.</i>
--	--

The `WifiManager#allowAutojoinGlobal(boolean)` method can be used to disable automatic connections. This is a privileged API that can be used by device manufacturers in limited circumstances (for example, a nonmobile, preconfigured device).

If the device is connected and the `config_wifi_framework_enable_associated_network_selection` overlay is set to `false`, no connectivity scans are performed and scan results don't trigger network selection. This setting has no effect when the device is disconnected, meaning that connectivity scans and network selection still occur.

Id. at 03 (showing WifiManager in Android disables automatic connections).

The scan results are filtered to remove Basic Service Set (“BSS”) Identifiers (“BSSIDs”) that have an RSSI below the entry RSSI (configurable), shown below.

The scan results are *filtered* to remove BSSIDs that have an RSSI below the entry RSSI (configurable using the `config_wifi_framework_wifi_score_entry_rssi_threshold_24GHz`, `config_wifi_framework_wifi_score_entry_rssi_threshold_5GHz`, and `config_wifiFrameworkScoreEntryRssiThreshold6ghz` overlays). Additionally,

Id. at 04.

When the screen of the Accused Products is on, Wi-Fi service calculates a connected score based on RSSI and link-layer stats. *Id.* at 05. Moreover, the Wi-Fi service may pass the score to the connectivity service (a switching system), which uses the score to determine whether to connect to a Wi-Fi network or to a mobile network. *Id.* at 06.

When the Accused Products’ screen is off, the network selection process might occur if scans are initiated by other services such as location services. *Id.* at 06. The Wi-Fi firmware evaluates the network quality and if the network quality is bad, the firmware might roam or disassociate from the network and wake up the Accused Products from a sleep mode to an active mode. *Id.*

The RSSI threshold values are (1) above -73 dBm for the 2.4 GHz band, configured with the `config_wifi_framework_wifi_score_low_rssi_threshold_24GHz`, (2) -70 dBm for the 5 Ghz and 6 Ghz

	bands, configured with the <code>config_wifi_framework_wifi_score_low_rssi_threshold_5GHz</code> and <code>config_wifiFrameworkScoreLowRssiThreshold6ghz</code>. <i>Id.</i> at 07. When the device is connected and screen is on, a connected scorer periodically monitors Wi-Fi quality by looking at signals such as RSSI and the number of packets transferred. <i>Id.</i> at 07. If Wi-Fi quality is determined to be bad, and the device supports dual concurrent stations, a scan will get triggered. <i>Id.</i> The <code>config_wifiLowConnectedScoreThresholdToTriggerScanForMbb</code> can be used to configure the score threshold that triggers the scanning, and the <code>config_wifiLowConnectedScoreScanPeriodSeconds</code> can be used to configure the period of these scans. <i>Id.</i> (3) When the screen is off and Wi-Fi is disconnected, the Wi-Fi firmware (the second communication module) performs preferred network offload (“PNO”) scanning for SSIDs. <i>Id.</i> at 08. The Wi-Fi framework configures the firmware with a list of SSIDs to scan for and a list of channels on which to scan. <i>Id.</i> If a configured SSID is found, the Wi-Fi firmware wakes the framework from a sleep mode to an active mode. <i>Id.</i> The Wi-Fi framework also configures the interval (timer) at which the firmware is to perform PNO scans, using the device mobility state to select different scan intervals. <i>Id.</i> In a low mobility state (the device is stationary), the interval is 60 seconds for the first three scans (controlled by <code>config_wifiStationaryPnoScanIntervalMillis</code>) and 180 seconds for subsequent scans. <i>Id.</i> In a high mobility state, the interval is 20 seconds for the first three scans (controlled by <code>config_wifiMovingPnoScanIntervalMillis</code>), and 60 seconds for subsequent scans. <i>Id.</i> The Accused Products pre-define a time window with threshold values for the signal levels when scanning Wi-Fi networks. When the screen of the Accused Products is on, and the Wi-Fi service may poll RSSI and link-layer stats every 3 seconds (time window) or by other configuration (<code>config_wifiPollRssiIntervalMilliseconds</code> or <code>config_wifiAdjustPollRssiIntervalEnabled</code> for dynamic adjustment based on the device mobility state and RSSI). <i>Id.</i> at 05. The polling interval is extended to 6 seconds (time window) when the device is stationary and RSSI is above -68 dBm (configured by the <code>config_wifiClientRssiMonitorThresholdDbm</code> and <code>config_wifiClientRssiMonitorHysteresisDb</code>), which is the second pre-defined threshold value. <i>Id.</i> The polling interval is reduced back to 3 seconds (time window, configured by the <code>config_wifiPollRssiIntervalMilliseconds</code>) when the device is non-stationary or RSSI is below -73 dBm. <i>Id.</i>
--	---

	<u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
Claim 23	
23[pre]. A method comprising:	As described in Element 1[pre], the Accused Products (also referred to as user equipment, UEs) perform every step of the method of the claims through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi Settings” or “Wi-Fi preferences,” “Wi-Fi Settings,” or “Advanced Wi-Fi Settings” of the Accused Products.⁴ The feature allows the Accused Products to roam and switch between different wireless networks, such as a WiFi wireless network and cellular networks including General Packet Radio Service (“GPRS,” 2G), Global System for Mobile (“GSM,” 2G), Code-Division Multiple Access (“CDMA,” 3G), Long Term Evolution (“LTE,” 4G), or 5G network. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
23[a]. determining a first context;	As described in Element 12[a], the Accused Products determines a first context (signal strength via RSSI or user preference) in the first communication link.

⁴ These features were previously branded as “Smart Network Switch” and “Adaptive Wi-Fi.”

	<u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
23[b]. determining a second context; and	As described in Element 12[b], the Accused Products determine the second context (signal strength via RSSI or user preference) in the first communication link. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
23[c]. automatically switching, with a server, a communication in progress via a first network to a second network based on the second detected context, wherein automatically switching is based on detecting the second context being preferred over the first context within a set of known networks or from a newly discovered network,	As described in Element 12[c], the Accused Products switch, with a server for Wi-Fi framework/Wi-Fi firmware or SCC AS, a communication in progress via a first network to a second network based on a second detected context (signal strength or user preference) by a pre-defined threshold value. If the second context is preferred over the first context in the first network, the Accused Products automatically switch to the second network (known or newly discovered network). <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.

23[d]. wherein upon activation of a timer, the server causes a communication module to change state from a sleep mode to a stand-by mode, and the server causes the second communication module to change state from the stand-by mode to an active mode before the communication is switched to the communication module.	As described in Element 12[d], the timer (pre-define time window) is activated for a server (server for Wi-Fi network/Wi-Fi firmware or SCC AS) to cause the communication module (Wi-Fi selection functions or VoWiFi function) to change state from the stand-by to an active mode before the communication (video/voice/data) is switched to the communication module. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
Claim 25	
25[pre]. A method comprising:	As described in Element 1[pre], the Accused Products (also referred to as user equipment, UEs) perform every step of the method of the claims through "Switch to mobile data" or "Switch to better Wi-Fi networks" product feature within "Intelligent Wi-Fi Settings" or "Wi-Fi preferences," "Wi-Fi Settings," or "Advanced Wi-Fi Settings" of the Accused Products.⁵ The feature allows the Accused Products to roam and switch between different wireless networks, such as a WiFi wireless network and cellular networks including General Packet Radio Service ("GPRS," 2G), Global System for Mobile ("GSM," 2G), Code-Division Multiple Access ("CDMA," 3G), Long Term Evolution ("LTE," 4G), or 5G network.

⁵ These features were previously branded as "Smart Network Switch" and "Adaptive Wi-Fi."

	<u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
25[a]. determining a first context;	As described in Element 12[a], the Accused Products determines the first context (signal strength or user preference) of the communication over the first network. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
25[b]. determining a second context; and	As described in Element 12[b], the Accused Products determines the second context (signal strength or user preference) of the communication over the first network. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
25[c]. automatically switching a communication in progress via a first device to a communication via a second device based on the second detected context, wherein	As described in Element 12[c], the Accused Products switch a communication in progress via a first communication module to a second communication module based on a second detected context (signal strength or user preference) by a pre-defined threshold value. If the second context is preferred over the first context in the first network, the Accused Products automatically switch to the second network (known or newly discovered network). The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is

automatically switching is based on detecting the second context being preferred over the first context within a set of known networks or from a newly discovered network,	switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
25[d]. wherein upon activation of a timer, a communication module of the second device changes state from a sleep mode to a stand-by mode, and the communication module of the second device changes state from the stand-by mode to an active mode before the communication is switched to the communication module of the second device.	As described in Element 12[d], the timer (pre-define time window) is activated to cause the communication module (Wi-Fi selection functions or VoWiFi function) of a second network (Wi-Fi or mobile) to change state from the stand-by to an active mode before the communication (video/voice/data) is switched to the communication module of the second network. The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.

Claim 34	
34[pre]. A server device comprising:	As described in Element 1[pre], the Accused Products are communication server devices.
34[a]. a switching system to switch operation between a communication module and a Wi-Fi communication module, wherein based on a first context and a second context, a communication automatically switches accordingly, wherein automatically switching is based on detecting the second context being preferred over the first context within a set of known networks or from a newly discovered network,	The Accused Products operated as mobile communication devices that establish a voice call or data stream sessions (a first wireless communication link) between the Accused Products and an end destination device (another user equipment) such as a mobile phone, a laptop, the Internet of Things, or server. In the context of a voice call, the call can be over a VoIP or VoWiFi network (“Internet”) or a public land mobile network (“PLMN”), defined by the 3GPP standards. The Accused Products include a switching system, “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi Settings” in A Series, S Series, X Cover, and Z Series. VASU 010302-454 at 398 (A13 5G); VASU 010601-745 at 691 (A14 5G); VASU 011048-196 at 143 (A23 5G/A23 5G UW); VASU 011532-691 at 633 (A53 5G/A53 5G UW); VASU 011692-852 at 792 (A54 5G); VASU 018745-906 at 848 (S20 FE 5G); VASU 019244-407 at 351 (S21 5G/ S21 Ultra 5G/ S21+ 5G); VASU 019782-949 at 895 (S22/S22+/S22 Ultra); VASU 019950-20128 at 1070 (S23/S23+/S23 Ultra); VASU 023406-563 at 508 (XCover Pro); VASU 023564-725 at 672 (Z Flip 5G); VASU 023894-4071 at 1014 (Z Fold3 5G/Z Flip3 5G); VASU 024756-929 at 877 (Z Flip4); VASU 024408-577 at 520 (Z Fold2 5G). Similarly, the Accused Products include another switching system, “Switch to Mobile Data” product feature under “Wi-Fi Preferences.” VASU 012187-372 at 300 (Amp Prime 3); VASU 012624-795 at 737 (J2); VASU 013258-446 at 375 (J7); VASU 013447-617 at 557 (J7 V); VASU 012938-3112 at 1050 (J7 Prime); VASU 017373-567 at 490 (S7); VASU 016965-7166 at 1090 (S7 Active); VASU 017167-372 at 294 (S7 Edge); VASU 013837-4053 at 986 (Note 9).

	Wi-Fi preferences Customize advanced Wi-Fi services. 1. From  Settings, tap Connections > Wi-Fi, and then tap On/Off to turn on Wi-Fi. 2. Tap  More options > Advanced. To view all network settings, tap View more. • Switch to mobile data: Connect automatically to a mobile network connection when the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi. • Turn on Wi-Fi automatically: Enable Wi-Fi in frequently used locations. • Wi-Fi power saving mode: Reduce battery usage by analyzing Wi-Fi traffic patterns. • Wi-Fi notifications: Receive notifications when open networks in range are detected. • Show Wi-Fi pop-up: When opening apps, indicate when Wi-Fi is available. VASU 013837-4053 at 3977. Moreover, the Accused Products include a similar switching system, “Switch to Mobile Data” product feature in “Advanced Wi-Fi Settings” to switch between mobile and Wi-Fi networks. VASU 009579-721 at 669 (A02s); VASU 009855-10011 at 116 (A10e); VASU 010011-157 at 104 (A11); VASU 010158-301 at 250 (A12); VASU 010455-600 at 546 (A13); VASU 010746-901 at 851 (A20); VASU 010902-1047 at 996 (A21); A51_User_Manual.pdf at 116 (A51); VASU 011197-367 at 315 (A51 5G/A51 5G UW); VASU 011368-531 at 477 (A52 5G); VASU 011853-2015 at 958 (A71 5G); VASU 012016-2186 at 2134 (A71 5G UW); VASU 015086-267 at 209 (Note 10+); VASU 014054-245 at 191 (Note 20 5G/Note 20 Ultra 5G); VASU 017730-891 at 838 (S8), VASU 017568-729 at 676 (S8 Active); VASU 017892-8059 at 8006 (S8+); VASU 018060-236 at 183 (S9/S9+); VASU 018399-571 at 511 (S10/S10e/S10+); VASU 018237-398 at 345 (S10 Lite); VASU 018907-9076 (S20 5G/S20 Ultra 5G/S20+ 5G); VASU 024244-407 at 348 (Z
--	---

Fold); VASU 023090-256 at 199 (XCover 6 Pro); VASU 023257-405 at 358 (XCover FieldPro); VASU 012482-623 at 570 (J2 Pure); VASU 012796-937 at 890 (J3); VASU 013113-257 at 209 (J7 Star).

Advanced Wi-Fi settings

You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by carrier.

1. From Settings, tap  **Connections** > **Wi-Fi**, and then tap  to turn on Wi-Fi.
2. Tap  **More options** > **Advanced**.
 - **Sync with Samsung Cloud/account:** Sync Wi-Fi profiles with your Samsung account.
 - **Switch to mobile data:** When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi.
 - **Turn on Wi-Fi automatically:** Turn on Wi-Fi in frequently-used locations.
 - **Detect suspicious networks:** Get notified when suspicious activity is detected on the current Wi-Fi network.

VASU 010455-600 at 546.

The Accused Products “Intelligent Wi-Fi” product feature is another switching system in “Wi-Fi Settings,” which switches between mobile and Wi-Fi networks depending on the signal strength. VASU 020129-301 at 243 (S24/S24+/S24 Ultra); VASU 024756-929 at 874 (Z Fold4/Z Flip4).

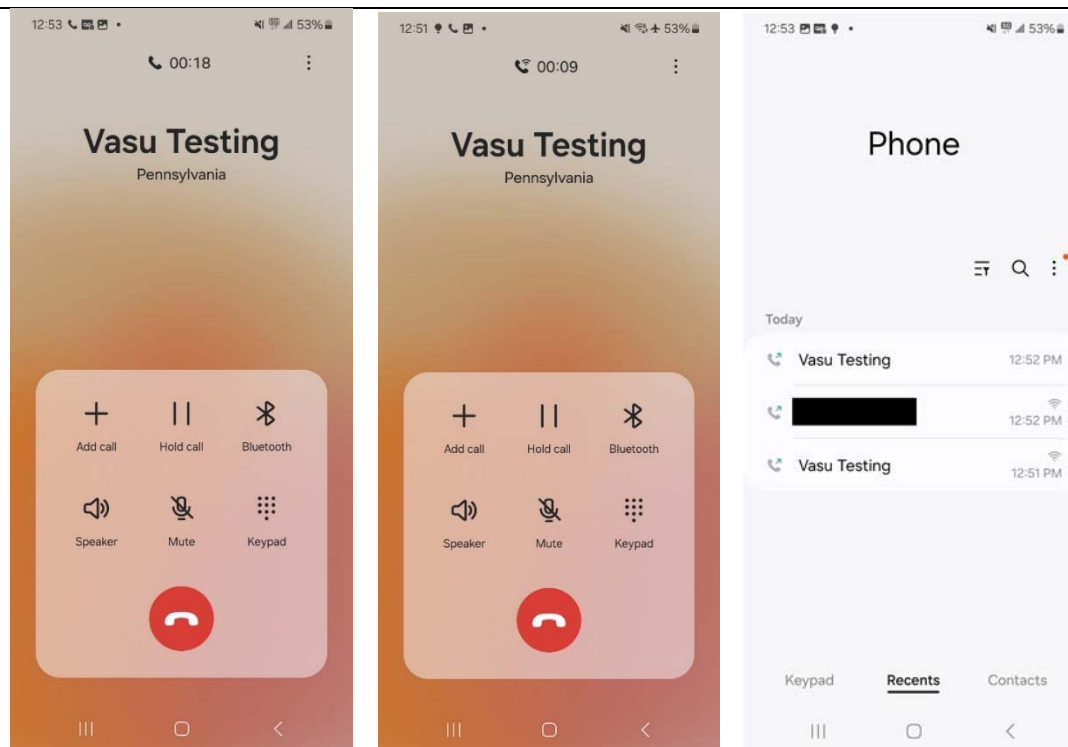
Wi-Fi settings

You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider.

1. From Settings, tap  **Connections** > **Wi-Fi**, and then tap  to turn on Wi-Fi.
2. Tap  **More options** for the following options:
 - **Wi-Fi Direct:** Share data directly between devices over Wi-Fi.
 - **Intelligent Wi-Fi:** Configure Wi-Fi switching and detection features.
 - **Advanced settings:** Configure Wi-Fi connections and Hotspot settings.
 - **Contact us:** Contact Samsung support through Samsung Members.

VASU 024756-929 at 874 (Z Fold4/Z Flip4).

	The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module (further described in Element 1[b]). This first communication link is over a first type of wireless network, either a Wi-Fi network or a PLMN or Cellular Network. With respect to a voice call, it can be initiated within the Wi-Fi network or over the PLMN/Cellular Network. <i>Compare</i> left screenshot (illustrating a cellular call via 5G by the lack of Wi-Fi symbol in the top ribbon and showing 5G cellular connectivity), <i>with</i> middle screenshot (illustrating a WiFi call by noting the phone is in airplane mode and by bearing a Wi-Fi symbol above the phone symbol); <i>see also</i> right screenshot (showing two calls made to the contact “Vasu Testing” where the earlier call has a Wi-Fi symbol above the time indicating a Wi-Fi call and the later call does not have a Wi-Fi symbol above the time indicating a cellular call).
--	---



VASU 031389-98 at 93-95.

The first connection link between the Accused Product and end destination device can be made under at least three scenarios: (1) Wi-Fi to Wi-Fi connection, (2) Wi-Fi to Home PLMN, and (3) Wi-Fi to Visitor PLMN. The vice versa is also true. Wi-Fi, Home PLMNs, and Visitor PLMNs are type of wireless networks.

The Accused Products established the calls via a wireless communication link with PLMN through gateways and interfaces supported by Evolved Packet Core (“EPC”) functions. EPC can be accessed via a trusted or untrusted network. There are differences when accessing these types of networks. However, the differences are not relevant to whether the Accused Products establish a communication link with an end destination device.

The Supported EPC Functions

Trusted WLAN Access Network (“TWAN”): For access to PLMN’s EPC via a trusted non-3GPP access network such as trusted TWLAN, a connection shall be established between the Accused Products and TWAN using specific signal procedures. VASU 008198-326 at 230. Access authentication signaling for access to the EPC shall be executed between the Accused Products and the AAA server, which is an interface server, to ensure mutual authentication of the user and the EPC. *Id.* at 230.

Evolved Packet Data Gateway (“ePDG”): ePDG is the local mobility anchor within untrusted non-3GPP access. VASU 006232-544 at 262. The PLMNs included in the ePDG information are the PLMNs that have roaming agreements with HPLMN. VASU 006232-544 at 269.

Through a network interface (Swn interface), the ePDG connects with an untrusted non-3GPP access. VASU 005019-113 at 92. The ePDG connects with the Accused Products (through the SWu interface) to establish data tunnels and user data packet transmission within the tunnels. *Id.* at 93.

Call Session Control Function (“CSCF”): CSCF can act as Proxy CSCF (“P-CSCF”), serving CSCF (“S-CSCF”), emergency CSCF (“E-CSCF”), or Interrogating CSCF (“I-CSCF”). VASU 005019-113 at 56. The P-CSCF is the first contact point for the Accused Products within the International Mobile Subscriber Identity (“IMSI”); the S-CSCF actually handles the session states in the network; the E-CSCF handles emergency sessions such as routing an emergency requests to the correct emergency center; the I-CSCF is the contact point within an operator’s network for all IMS connections destined to a subscriber of that network operator or roaming subscriber located within the network operator’s service area. *Id.*

Home Subscriber Server (“HSS”): The HSS supports the authentication procedures to access CS domain, PS domain, and system services by storing the generated data for authentication, integrity, and ciphering and by providing these data to the appropriate entities including AAA server or CSCF. VASU 005019-113 at 41. The diagram below illustrates . . .

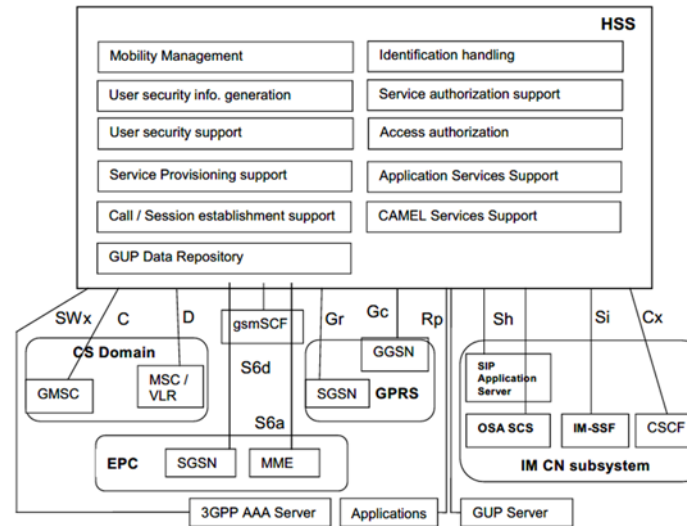


Figure 0.b: HSS logical functions

VASU 005019-113 at 40.

Authentication, Authorization, and Accounting (“AAA”): The Accused Products is authenticated and authorized through AAA to roam between networks. AAA server (interface server) is located at HPLMN and provides support for non-3GPP access users with services like authentication, authorization, and location management services to access evolved packet systems (“EPS”) in mobile networks. VASU 005019-113 at 49. It interacts with HSS to maintain consistent information to support service continuity between 3GPP (mobile networks) and non-3GPP (Wi-Fi) networks. *Id.* It contains user information to gain access to non-3GPP access. *Id.* Non-3GPP access authentication defines the process to permit or deny a subscriber to attach to and use the sources of a non-3GPP IP access interworked with the EPC network. VASU 006232-544 at 307. Non-3GPP access authentication signaling is executed between the Accused Products and the AAA server/HSS (interface server). *Id.* During the authentication of the Accused Products for accessing the EPC via ePDG, ePDG shall initiate EAP-AKA based authentication between the Accused Products and the AAA server. VASU 006232-544 at 279.

Roaming Scenarios After the Accused Products Establish a Call

Exemplary Scenario 1: Wi-Fi to Wi-Fi

- (3) The Accused Products initiate a call within a first Wi-Fi network through VoIP or VoWiFi and roam from a first Wi-Fi network to a second Wi-Fi network.

The Accused Products may go out of range of access points and shift network association to another access point without losing connection. VASU 025133-44 at 134. Weak signals can trigger roaming on the Accused Products. *Id.* The Accused Products support 802.11k and 802.11v standards to reduce the length of time of lost connectivity during basic service set (“BSS) transition. *Id.* at 138-42.

Exemplary Scenario 2: Wi-Fi to Home PLMN

- (5) The Accused Products initiate a call over a first Wi-Fi network through VoIP or VoWiFi and roam from the first Wi-Fi network to the coverage area of the home PLMN (“HPLMN”) of the Accused Products.
- (6) The Accused Products initiate a call within a first Wi-Fi network, but set up a backend of the call over PLMN network and roam from the first Wi-Fi network to the coverage area of the HPLMN of the Accused Products.

In a non-roaming scenario when the Accused Products establish the communication link with a home network, the trust relationship of Wi-Fi (non-3GPP IP wireless network) is determined by the HPLMN operators. VASU 008198-326 at 227. The trust relationship is indicated to the Accused Products via either pre-configured policies in the Accused Products by the home PLMN operator or dynamic indication during 3GPP-based access authentication. *Id.*

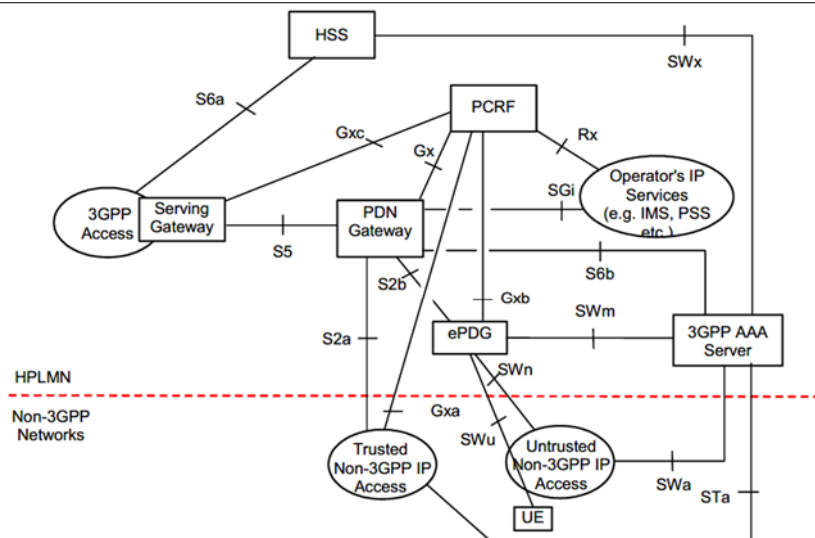
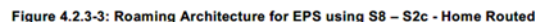


Figure 4.2.2-1: Non-Roaming Architecture within EPS using S5, S2a, S2b

VASU 006232-544 at 254 (non-roaming architecture showing trusted or untrusted non-3PPP wireless network connecting to AAA server in PLMN using the SWa or STa interface to access the trusted or untrusted 3GPP networks).

	Authorization of EPC access shall be performed by the AAA server upon successful user authentication. <i>Id.</i> <u><i>Exemplary Scenario 3: Wi-Fi to Visitor PLMN</i></u> (5) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over VoIP or VoWiFi, and roam from the first Wi-Fi network to the coverage area of a visitor PLMN (“VPLMN”) of the Accused Products. (6) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over a HPLMN, and roam from the first Wi-Fi network to the coverage area of a VPLMN. In roaming scenario when the Accused Products establish the communication link with a visitor network, the HSS or AAA server (interface server) in HPLMN makes the final decision if a non-3GPP wireless network is trusted or untrusted. VASU 006232-544 at 260. The HSS/AAA server (interface server) may take the visitor PLMN (“VPLMN”) policy and capability returned from the AAA proxy or roaming agreement into account. <i>Id.</i> at 260.
--	---



The session origination procedures specify the signaling path between the Accused Products initiate a session setup attempt and the S-CSCF assigned to perform the session origination service. VASU 005263-653 at 380. The Accused Products initiate a session setup attempt and assigned a S-CSCF to perform the session origination service. VASU 005263-653 at 380. The signaling path between the Accused Products and S-CSCF is determined at the time of the Accused Products registration. *Id.* The S-CSCF to application server interface is used to provide services in the application server in the HPLMN or in a trusted external network (e.g., third-party or VPLMN). VASU 005019-113 at 58. If the Accused Products are located in a VPLMN, it determines the P-CSCF via the CSCF discovery procedure. VASU 005263-653 at 380. The HPLMN advertises the S-CSCF as the entry point from the VPLMN. *Id.* When registration is completed, P-CSCF knows the name/address of the next hop in the signaling path toward the S-CSCF. *Id.* If the Accused Products are located in the HPLMN, the HPLMN allocates an S-CSCF in the HPLMN. *Id.* at 383. When registration is completed, P-CSCF knows the name/address of S-CSCF. *Id.*

Detection of Context Changes in the Established Communication

The Accused Products monitor the network context (signal strength or user preference) of their communication link to the wireless network to detect context changes.

“Switch to Mobile Data” detects the network context changes to “automatically switch[] networks based on both network quality and user preferences.” VASU 025185-91 at 187. The connection manager will not be active until it accumulates enough data to determine user preference. *Id.*



Id. at 187 (determining user preference).

Through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi settings” on the Accused Products (shown below), the Accused Products can seamlessly switch to mobile data if there are signal strength issues and “whenever the Wi-Fi connection is unstable.” VASU 019950-20128 at 1070. When the Wi-Fi signal strength is strong, it switches “back to Wi-Fi.” *Id.*

Intelligent Wi-Fi settings

You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider.

1. From Settings, tap **Connections > Wi-Fi**, and then tap to turn on Wi-Fi.
2. Tap **More options > Intelligent Wi-Fi** for the following options:
 - **Switch to mobile data:** When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi.
 - **Switch to better Wi-Fi networks:** Automatically switch to faster or more stable Wi-Fi networks.
 - **Turn Wi-Fi on/off automatically:** Turn on Wi-Fi in frequently-used locations.
 - **Show network quality info:** Display network information (such as speed and stability) in the list of available Wi-Fi networks.
 - **Prioritize real-time data:** Give network priority to games, video calls, and other tasks that are sensitive to lag.
 - **Detect suspicious networks:** Get notified when suspicious activity is detected on the current Wi-Fi network.
 - **Wi-Fi power saving mode:** Enable Wi-Fi traffic analysis to reduce battery usage.
 - **Auto Hotspot connection:** Automatically connect to a Wi-Fi hotspot when detected.
 - **Intelligent Wi-Fi:** View the Intelligent Wi-Fi version.

VASU 019950-20128 at 1070 (intelligent Wi-Fi settings in an exemplary S23+ phone). The Accused Products measure signal strength of Wi-Fi networks by Received Signal Strength Indicator (“RSSI”), and its unit of measurement is dBm. The table below provides a point of reference for interpreting the RSSI value.

Signal Strength	TL;DR		Required for
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWi-Fi, streaming video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

VASU 025540-45 at 43-44.

The screenshot below illustrate that the Accused Products continuously monitor the signal strength.

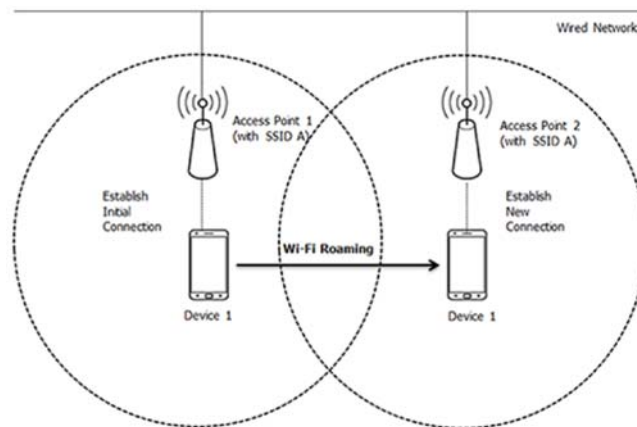


VASU 031389-98 at 96.

The Accused Products include “Auto Wi-Fi,” which turns Wi-Fi on and off depending on locations. VASU 025185-91 at 88. It turns Wi-Fi on when the favorite network is available by user preference and turns off Wi-Fi when this network is unavailable. *Id.* Auto Wi-Fi is triggered based on user’s location by geofencing (a virtual geological fence based on cellular stations). *Id.* Furthermore, The Wi-Fi network selection functions in the Accused Products continuously evaluate the quality of the connected network and assess the quality of available networks. VASU 025102-18 at 02. The Accused Products scan the available networks depending whether the screen of the Accused Products is on or off. *Id.*

If the screen of the Accused Products is on and the Accused Products is connected, the Wi-Fi framework of the Accused Products evaluates whether the current network is good enough to skip network selection when all the following conditions are met: (1) the RSSI is above the required RSSI threshold or sufficient traffic is flowing over the connection; (2) the network is evaluated, or user approved for use without internet access; and (3) the network is unmetered. *Id.* at 2. If the connection isn't good enough, the connectivity subsystem triggers a scan to detect available networks (a set of networks to choose for the second network). *Id.*

Once connected, the Wi-Fi service calculate "a connected score" based on the RSSI and determine whether to connect to a Wi-Fi network or another network type, such as a mobile network. *Id.* at 3-4. the Wi-Fi service may pass the score to the connectivity service, which uses the score to determine whether to connect to a Wi-Fi network or to a mobile network. *Id.* at 5.



VASU 025133-44 at 34 (roaming from one Wi-Fi to another Wi-Fi access point is triggered due to weak signal).

Moreover, if the screen is on and the Accused Products are disconnected, the Android connectivity system issues periodic scans (activation of a timer) following an exponential back off schedule (increasing the waiting time between retries). *Id.* at 02. The module evaluates scan results received by evaluating if the signal level is below a predefined threshold and tries to select the best network to connect to. *Id.* When the Accused Products' screen is off, the network selection process might occur if scans are initiated by other services such as location services. *Id.* at 06.

Switch to a Second Communication Module over a Second Network

When the Accused Products are active in an IMS session, the session transfer procedures provide session continuity between wireless networks using signal strength information. VASU 005654-93 at 62. The Accused Products initiate session transfer procedure based on trigger criteria, including the current operator policy, user preferences, and wireless network conditions for conducting a session continuity operation to the SCC AS (interface server). VASU 005654-93 at 64. A third-party call control function (call function from the Accused Products) is employed for subscriber IMS sessions at the SCC AS upon session establishment for enablement of Session Transfer. *Id.*

The first communication link (voice or video call) uses IP Multimedia Core Network Subsystem (“IMS”), which is the framework for delivering multimedia services using PS and CS bearers (data tunnels between the network gateways and the Accused Products) for the media. VASU 005654-93 at 58. IMS service continuity requires a Service Centralization and Continuity (“SCC”) Application Server (“AS”). VASU 005654-93 at 63. The SCC AS is a home network based IMS application that provides functionality required to enable IMS centralized services. VASU 005865-953 at 77. The screenshot below illustrates the information used for IMS service continuity that may be provided between SCC AS and the Accused Products:

- session transfer indicator to indicate that this new session is for session transfer.
- details about the access and the media components being transferred / kept / released.
- optionally, an IMS Communication Service Identifier defined in 3GPP TS 23.228 [7]
- which session is required to be replaced or updated;
- whether to merge the session(s):

VASU 005654-93 at 63. SCC AS provides an IMS-based mechanism for enabling session continuity. It executes the transfer of the IMS session between different wireless networks and implements third-party call control upon session establishment. VASU 005654-93 at 64.

A Service Control Signaling Path transports service control signaling between the Accused Products and the SCC AS when using CS or PS access. VASU 005865-953 at 79. The access leg is formed by combining the Service Control Signaling Path and the CS Bearer Control Signaling Path. VASU 005865-953 at 80. The SCC AS presents the remote leg to the CSCF as an IMS session using IMS SIP signaling on behalf of the Accused Products. *Id.*

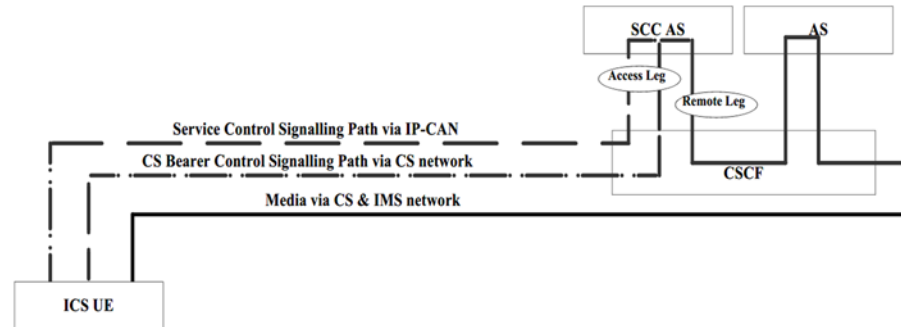


Figure 7.1.1-1: ICS UE session signalling and bearer path using PS network for Service Control Signalling Path

VASU 005865-953 at 80 (Accused Products (or UEs), session signaling and bearer path in access leg and remote leg in PS network).

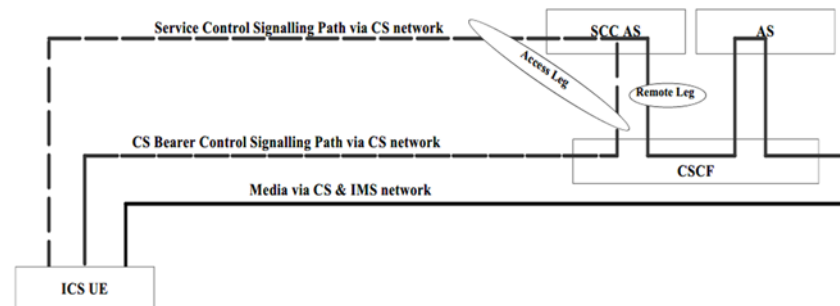


Figure 7.1.1-2: ICS UE session signalling and bearer path using CS network for Service Control Signalling Path

VASU 005865-953 at 80 (Accused Products (or UEs), session signaling and bearer path in access leg and remote leg in CS network).

Moreover, the access transfer control function (“ASCF”) is a function in HPLMN or visitor network (“VPLMN”) may be co-located with the existing functional entities such as P-CSCF. VASU 005694-864 at 720. Based on carrier policy, it shall be allocated a session transfer number (“STN-TR”) and keeps track of sessions (either in alerting state, active, or held) to be able to perform session transfer. *Id.* at 720-21. The following implementation method determines if the ASCF should be included during registration: if Accused Products are roaming, based on the roaming agreement; based on local configuration; based on registered communication service of the Accused Products; based on the access type. *Id.* at 721.

	Upon session initiation, the Accused Products or the SCC AS establishes the Service Control Signaling Path for communication of service control signaling via the PS network using the Gm reference point. VASU 005865-953 at 80. <u>Session Continuity between Mobile Networks</u> When the signal strength drops below a predetermined threshold, the Accused Products may also use locally stored data for selecting a second EPC network available for connectivity via the currently selected non-3GPP wireless network to establish a second communication link. VASU 008198-326 at 222. UE shall select a PLMN according to the PLMN selection procedure of the selected non-3GPP wireless network. <i>Id.</i> Signaling and bearer resources are allocated in the transferring-in wireless network and the user's sessions are transferred from the transferring-out wireless network. VASU 005654-93 at 669. The SCC AS executes access transfer procedures and resources in the transferring-out wireless network is released. <i>Id.</i> The Accused Products establish the second communication link (the second call session with the second network, transferred-in network) with the transfer-in network without disrupting the first communication link in the transfer-out network. IMS sessions from and to the Accused Products are anchored at the SCC AS in the home IMS based on initial filtering criteria ("iFC") to provide service continuity for the user during the transition between two wireless networks. VASU 005654-93 at 62. For single radio voice call continuity ("SRVCC"), voice call continuity between PLMN/VPLMN over PS and CS are anchored when the UE is capable of transmitting or receiving only one of the access networks at a given time. VASU 005195-214 at 200.
--	--

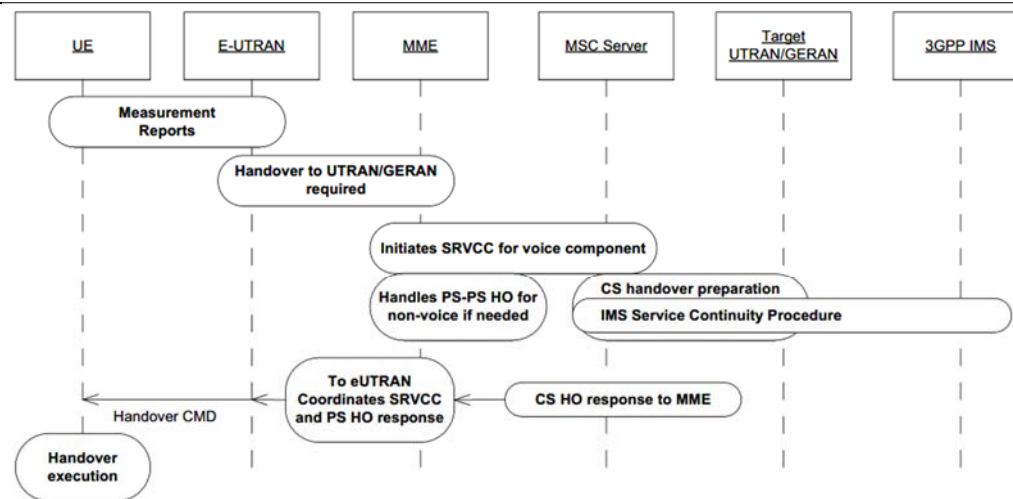


Figure 4.2.2-1: Overall high level concepts for SRVCC from E-UTRAN to UTRAN/GERAN

VASU 005195-214 at 202 (how SRVCC works in E-UTRAN, 4G to UTRAN/GERAN, 3G/2G).

A third-party call control function (functions provided by the Accused Products) is employed at the SCC AS to facilitate inter-access network mobility through the user of access transfer between the two wireless networks. *Id.*

PS-CS transfer

IMS session established in CS or PS wireless networks are anchored at the SCC AS. VASU 005654-93 at 662. IMS sessions using CS bearer are established at session setup or upon access transfer. *Id.*

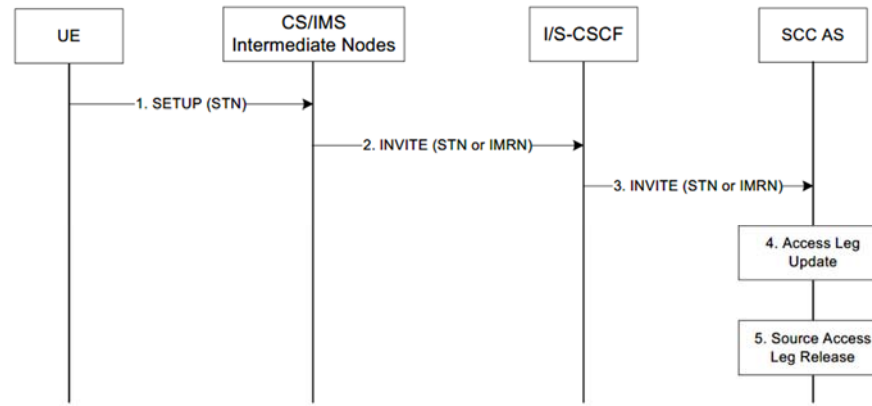


Figure 6.3.2.1.1-1: PS – CS Access Transfer: PS to CS

VASU 005654-93 at 72 (user is active in an IMS originating or terminating session using PS media at the time of transfer).

CS-PS Transfer

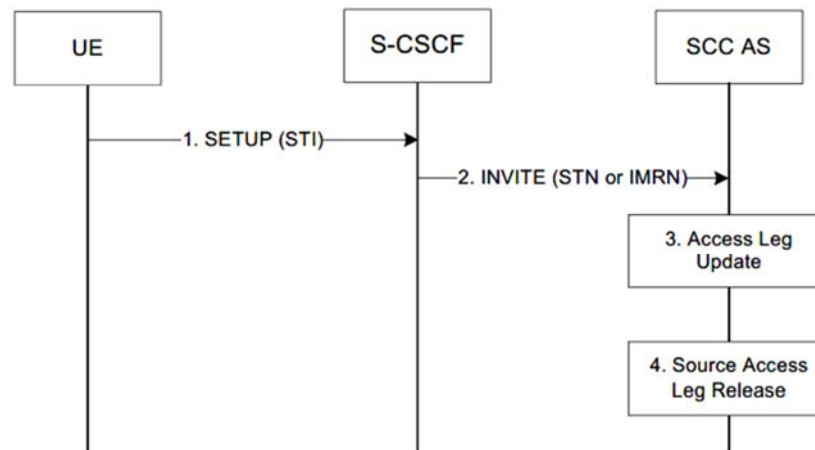


Figure 6.3.2.1.2-1: PS – CS Access Transfer: CS to PS

VASU 005654-93 at 73 (the user is active in the IMS originating or terminating session using CS at the time of transfer).

PS-PS Transfer

US is attached to one IP connectivity access network (“IP-CAN”), and it registers to the S-CSCF. VASU 005654-93 at 75. UE-1 and UE-2 establish an active multimedia session via this IP-CAN. *Id.* After changing to a new IP-CAN, obtaining new signaling and media addresses, and completing the Access Transfer procedures, UE-1 continues the session with UE-2 on the new IP-CAN. *Id.*

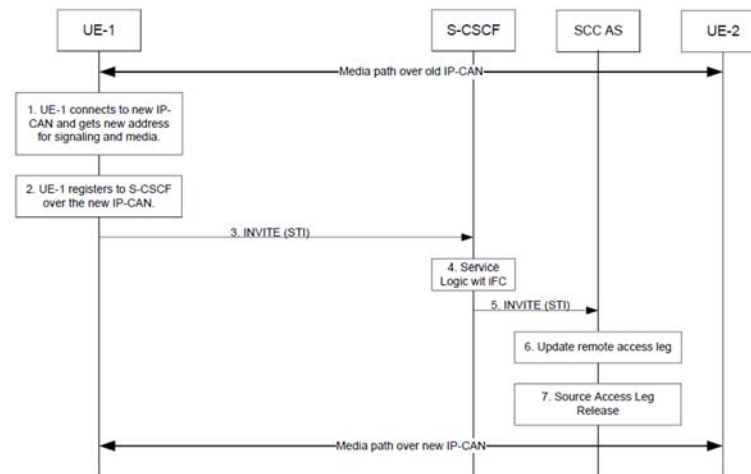


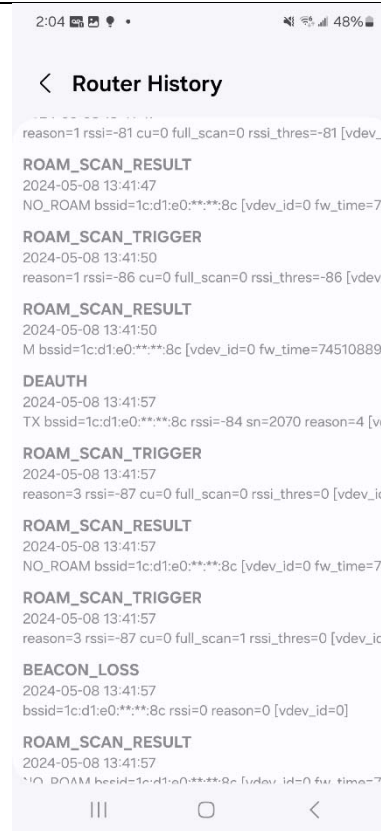
Figure 6.3.2.2.1-1: Information flow for PS-PS Access Transfer

Id.

Session Continuity between Wi-Fi and Mobile Networks

Upon the Accused Products’ request, the access network discovery and selection function (“ANDSF”) in either HPLMN or VPLMN may provide a list of wireless access networks available in the vicinity of the UE for all the access technology types requested by the UE to establish a second communication link through Wi-Fi. VASU 006232-544 at 293. An ANDSF element located in the HPLMN of a UE is referred to as Home-ANDSF (“H-ANDSF”) and an ANDSF element located in the visited PLMN of a UE is referred to as the visited-ANDSF (V-ANDSF) for this UE. VASU 006232-544 at 291. The H-ANDSF in the subscriber’s HPLMN may interact with HSS user profile information. *Id.* at 61.

	The ANDSF provides information for access networks that are available to the UE including: - the access technology type (e.g. WLAN, WiMAX). - the radio access network identifier (e.g. the SSID of a WLAN). - other technology specific information, e.g. one or more carrier frequencies. - validity conditions, i.e. conditions indicating when the provided access network discovery information is valid (such conditions may include e.g. a location). VASU 006232-544 at 293. ANDSF contains data management and control functionality necessary to provide network discovery and selection assistance data per operator's policy. VASU 006232-544 at 292. ANDSF may provide other information, including access network discovery information, WLAN selection information, and ePDG configuration information. VASU 008198-326 at 252. If the UE is roaming in a VPLMN, the UE may receive Inter-system mobility policies or access network discovery information from H-ANDSF or V-ANDSF or both. <i>Id.</i> Moreover, access network selection and traffic steering between 3GPP access and WLAN is supported using ANDSF and is also supported using radio access network rule procedure without ANDSF. VASU 006232-544 at 290. The home network preference may be provided by the Accused Products' HPLMN and include information that assists the UE to select a WLAN network and to select a PLMN for 3GPP-based authentication over WLAN. VASU 006232-544 at 297. Similarly, a visited network preference may be provided by the VPLMN, but UE shall ignore the preference if provided a HPLMN preference. <i>Id.</i> <u>Termination of the Established Communication</u> The Accused Products will terminate a wireless communication link when appropriate, according to its connection criteria and signal strength. For example, in the representative Accused Product—the Galaxy S22—screenshot below, the device sent a DEAUTH command when the RSSI value was -84 dBm, thereby terminating the Wi-Fi connection.
--	---

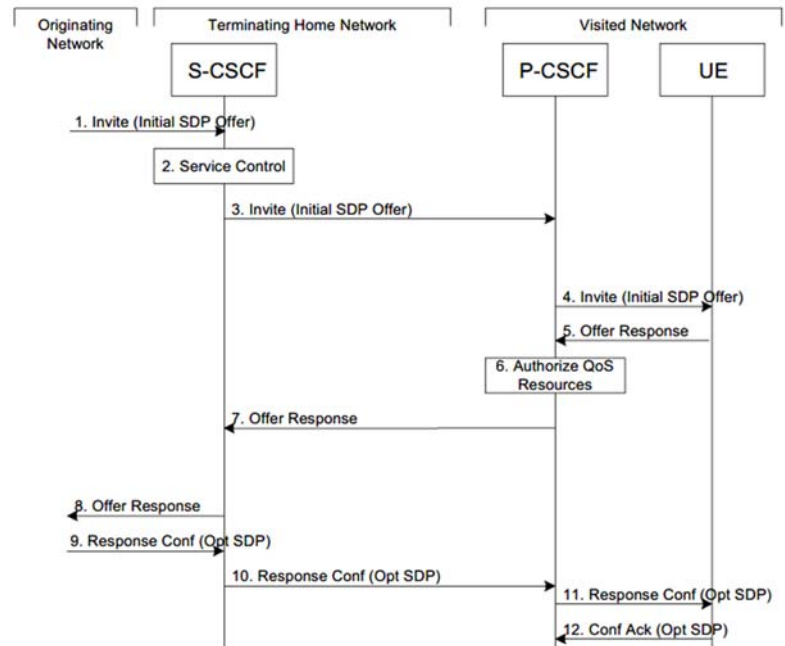


VASU 031389-98 at 97.

The SCC AS notifies the Accused Products through the service control signaling path to terminate transmitting over the first communication link (access leg) with the first wireless network.

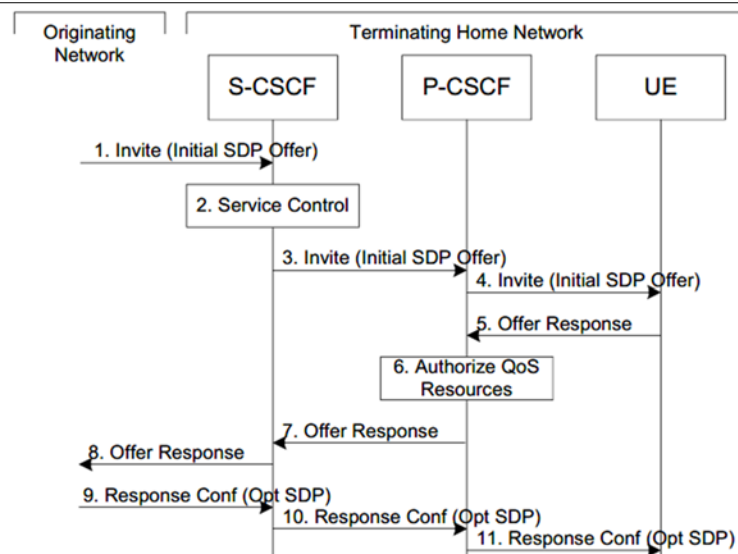
The termination procedures specify the signaling path between the S-CSCF assigned to perform the session termination service and the Accused Products. VASU 005263-653 at 392. The signaling path is determined at the time of UE registration and remains fixed for the life of the registration. *Id.*

When registration is completed in the roaming scenario, S-CSCF knows the name/address of its next hop in the signaling path and the P-CSCF, and P-CSCF knows the name/address of the UE. *Id.*



VASU 005263-653 at 393 (mobile termination procedure during roaming scenario).

When registration is completed in non-roaming scenario, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE. *Id.* at 395.



Id. at 395 (mobile termination procedure during non-roaming scenario).

For detection of conditions requiring session transfer, the Accused Products establish an access leg with the SCC AS via the transferred-in wireless network to request session transfer to the transferred-in wireless network. VASU 005654-93 at 70. When the UE initiates a session transfer request, it includes the session transfer identifier. *Id.* The SCC AS executes the session transfer procedure by replacing the access leg currently communicating to the remote leg (the first communication link) with the access leg established via the transferred-in access (the second communication link). *Id.* The access leg established via the transferred-out wireless network is subsequently released (terminating the first communication link). *Id.* If the SCC AS detects that the Accused Products are not reachable over Service Control Signaling Path, the SCC AS should clear all held sessions related to the user if any are present and update the remote leg if necessary. VASU 005865-953 at 912.

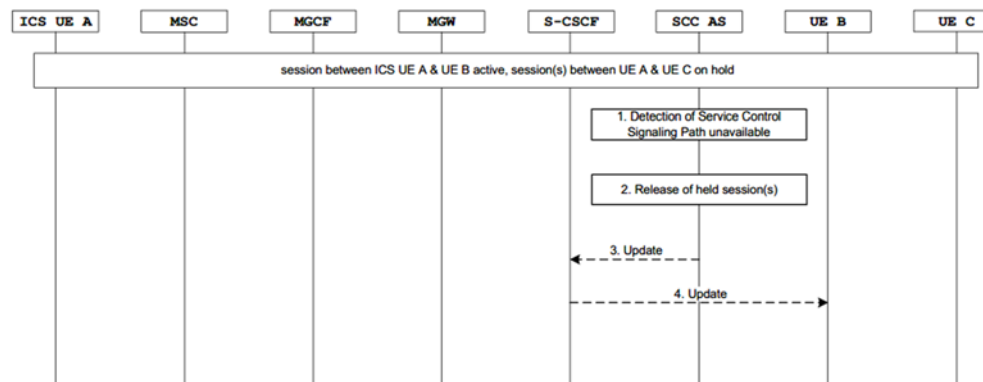


Figure 7.5.1.1.3-1: release of held sessions at SCC AS when Service Control Signaling Path unavailable

VASU 005865-953 at 912.

A delete session request message will notify the Accused Products (UEs) to terminate transmission of the first call session with the first wireless network (transfer-out). The “Delete Session Request” (shown below) is sent over the S2b interface of EPC as part of the following procedure: UE/ePDG initiated detach, UE requested disconnection with packet data network (“PDN”), or HSS/AAA initiated detach. VASU 009199-578 at 307.

	SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)			
32	Create Session Request		X	
33	Create Session Response			X
36	Delete Session Request		X	
37	Delete Session Response			X

VASU 009199-578 at 226.

Redirect to the Second Communication

The Accused Products redirect to the second communication link to maintain the connection by the mobile communication device to transparently maintain a connection.

For example, in the representative Accused Product—the Galaxy S22—screenshot below, the device shows a connection to both the 5G cellular network and a WiFi network.



VASU 031389-98 at 98.

The Accused Products, upon receiving a request for execution of session transfer, use the SCC AS (interface server) to perform the access leg update by switching (re-directing) the access leg communicating with the remote leg from transferring-out access to transferring-in access. VASU 005654-93 at 70. The SCC AS subsequently coordinates the session control signaling exchange between the access leg and the remote leg associated with a subscriber IMS session, thereby establishing a second wireless communication link between the Accused Products and the second wireless network. *Id.*

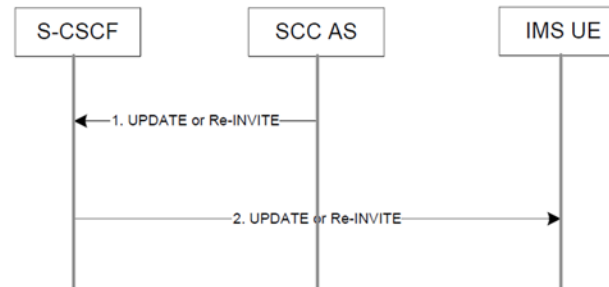


Figure 6.3.1.5-1: Access Leg Update toward the remote end

VASU 005654-93 at 71 (how access leg is updated toward the remote end). The SCC AS updates the access leg by communicating the session description protocol (“SDP”) of the Access leg established in the transferring-in access to the remote end via the user’s S-CSCF. *Id.*

When the Accused Products determine that the access transfer is desirable because the signal strength drops below a pre-determined threshold based on criteria such as operator policy or user preferences, a registration in IMS is performed by the UE via the transferring-in wireless network if the user is not already registered via that network. VASU 005654-93 at 69.

The create session request is part of the procedure to hand over to untrusted or trusted non-3GPP access from ePDG/TWAN to PGW via S2b interface of EPC. VASU 009199-578 at 234. The ePDG/TWAN may include AAA server identifier in the create session request to the PGW through S2a/S2b interface. VASU 009199-578 at 247 (information element in a create session request).

	SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)
32	Create Session Request
33	Create Session Response
36	Delete Session Request
37	Delete Session Response

VASU 009199-578 at 226 (message types for GRPS Tunneling Protocol in PLMN).

The direction of the message is from MME/S4-SGSN to SGW, from SGW to PGW, and from ePDG/TWAN to PGW. VASU 009199-578 at 233.

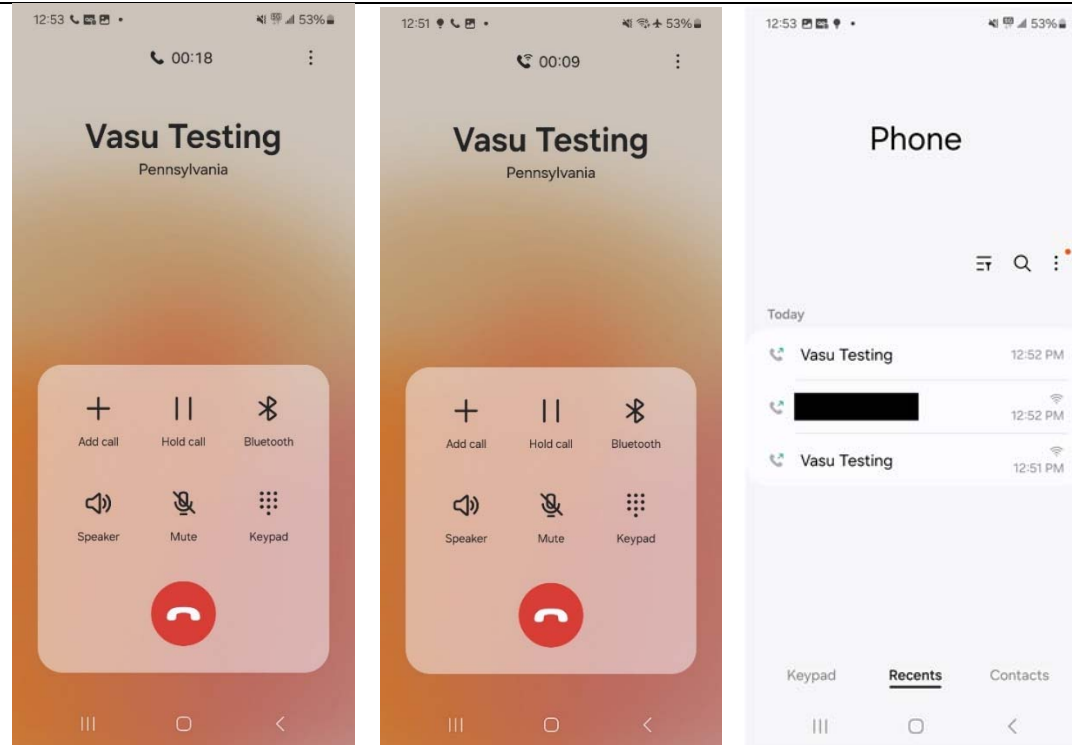
	<u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
34[b]. wherein upon activation of a timer, the switching system causes the Wi-Fi communication module to change state from a sleep mode to a stand-by mode, and the switching system causes the Wi-Fi communication module to change state from the stand-by mode to an active mode before the communication is switched to the Wi-Fi communication module.	As described in Element 12[d], the timer (pre-define time window) is activated to cause the Wi-Fi communication module (Wi-Fi selection functions or VoWiFi function) to change state from the stand-by to an active mode before the communication (video/voice/data) is switched to the Wi-Fi communication module. The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
Claim 35	
35[pre]. A device comprising:	As described in Element 1[pre], the Accused Products are communication devices.

35[a]. a switching system to switch operation between a first communication module and a second communication module, wherein during an established communication if a preferable context is determined, the established communication is switched to a second communication over a network, wherein the preferable context is found in a set of known networks or in a newly discovered network,	As described in Element 34b, a switching system (“Switch to mobile data” or “Switch to better Wi-Fi networks”) switch a first communication module for the first communication (voice/video/data over Wi-Fi or mobile) to a second communication module for the second communication (voice/video/data over Wi-Fi or mobile) if the detected signal strength or user preference (context) is preferred from known or newly discovered networks. The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module.
---	---

	<u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
35[b]. wherein upon activation of a timer, the switching system causes the second communication module to change state from a sleep mode to a stand-by mode, and the switching system causes the second communication module to change state from the stand-by mode to an active mode before a communication is switched to the second communication module.	As described in Element 12[d], the timer (pre-define time window) is activated and the switching system ("Switch to mobile data" or "Switch to better Wi-Fi networks") causes the second communication module to change state from the stand-by to an active mode before the communication (video/voice/data) is switched to the Wi-Fi communication module. The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
Claim 39	
39[pre]. A method comprising:	As described in Element 1[pre], the Accused Products (also referred to as user equipment, UEs) perform every step of the method of the claims through "Switch to mobile data" or "Switch to better Wi-Fi networks" product feature within "Intelligent Wi-Fi Settings" or "Wi-Fi preferences," "Wi-Fi Settings," or

	“Advanced Wi-Fi Settings” of the Accused Products.⁶ The feature allows the Accused Products to roam and switch between different wireless networks, such as a WiFi wireless network and cellular networks including General Packet Radio Service (“GPRS,” 2G), Global System for Mobile (“GSM,” 2G), Code-Division Multiple Access (“CDMA,” 3G), Long Term Evolution (“LTE,” 4G), or 5G network. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
39[a]. establishing a first communication link between a mobile communication device and an end destination device, wherein the first communication link comprises a first wireless communication link between the mobile communication device and a first wireless network;	The Accused Products operated as mobile communication devices that establish a voice call or data stream sessions (a first wireless communication link) between the Accused Products and an end destination device (another user equipment) such as a mobile phone, a laptop, the Internet of Things, or server. In the context of a voice call, the call can be over a VoIP or VoWiFi network (“Internet”) or a public land mobile network (“PLMN”), defined by the 3GPP standards. This first communication link is over a first type of wireless network, either a Wi-Fi network or a PLMN or Cellular Network. For example, with respect to a voice call, it can be initiated within the Wi-Fi network or over the PLMN/Cellular Network. <i>Compare</i> left screenshot (illustrating a cellular call via 5G by the lack of Wi-Fi symbol in the top ribbon and showing 5G cellular connectivity), <i>with</i> middle screenshot (illustrating a WiFi call by noting the phone is in airplane mode and by bearing a Wi-Fi symbol above the phone symbol); <i>see also</i> right screenshot (showing two calls made to the contact “Vasu Testing” where the earlier call has a Wi-Fi symbol above the time indicating a Wi-Fi call and the later call does not have a Wi-Fi symbol above the time indicating a cellular call).

⁶ These features were previously branded as “Smart Network Switch” and “Adaptive Wi-Fi.”



VASU 031389-98 at 93-95.

The first connection link between the Accused Product and end destination device can be made under at least three scenarios: (1) Wi-Fi to Wi-Fi connection, (2) Wi-Fi to Home PLMN, and (3) Wi-Fi to Visitor PLMN. The vice versa is also true. Wi-Fi, Home PLMNs, and Visitor PLMNs are type of wireless networks.

Establishing the First Communication Link

The first communication link (voice or video call) uses IP Multimedia Core Network Subsystem (“IMS”), which is the framework for delivering multimedia services using PS and CS bearers (data tunnels between the network gateways and the Accused Products) for the media. VASU 005654-93 at 58. IMS service

	continuity requires a Service Centralization and Continuity (“SCC”) Application Server (“AS”). VASU 005654-93 at 63. The SCC AS is a home network based IMS application that provides functionality required to enable IMS centralized services. VASU 005865-953 at 77. The screenshot below illustrates the information used for IMS service continuity that may be provided between SCC AS and the Accused Products: - session transfer indicator to indicate that this new session is for session transfer. - details about the access and the media components being transferred / kept / released. - optionally, an IMS Communication Service Identifier defined in 3GPP TS 23.228 [7] - which session is required to be replaced or updated; - whether to merge the session(s): VASU 005654-93 at 63. SCC AS provides an IMS-based mechanism for enabling session continuity. It executes the transfer of the IMS session between different wireless networks and implements third-party call control upon session establishment. VASU 005654-93 at 64. A Service Control Signaling Path transports service control signaling between the Accused Products and the SCC AS when using CS or PS access. VASU 005865-953 at 79. The access leg is formed by combining the Service Control Signaling Path and the CS Bearer Control Signaling Path. VASU 005865-953 at 80. The SCC AS presents the remote leg to the CSCF as an IMS session using IMS SIP signaling on behalf of the Accused Products. <i>Id.</i>
--	--

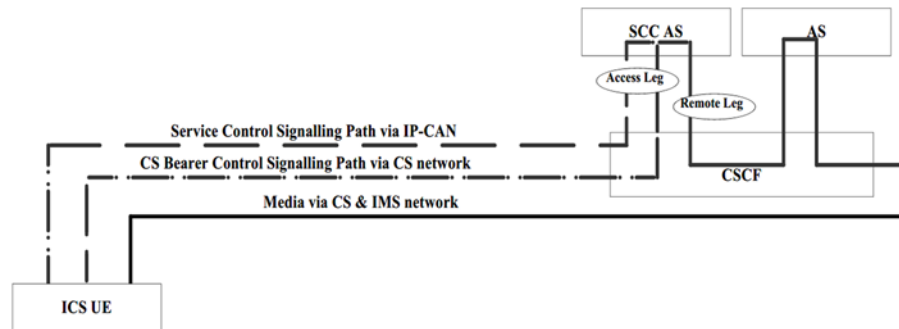


Figure 7.1.1-1: ICS UE session signalling and bearer path using PS network for Service Control Signalling Path

VASU 005865-953 at 80 (Accused Products (or UEs), session signaling and bearer path in access leg and remote leg in PS network).

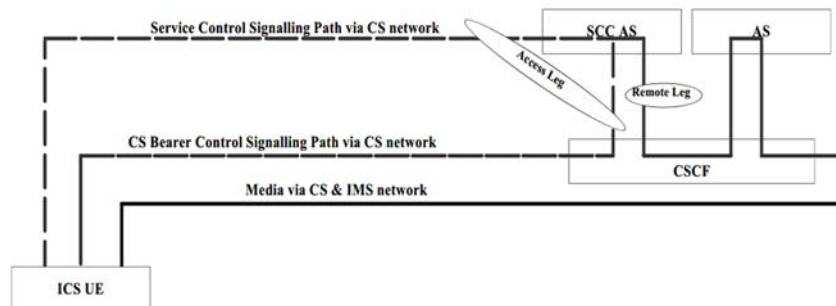


Figure 7.1.1-2: ICS UE session signalling and bearer path using CS network for Service Control Signalling Path

VASU 005865-953 at 80 (Accused Products (or UEs), session signaling and bearer path in access leg and remote leg in CS network).

Moreover, the access transfer control function (“ASCF”) is a function in HPLMN or visitor network (“VPLMN”) may be co-located with the existing functional entities such as P-CSCF. VASU 005694-864 at 720. Based on carrier policy, it shall be allocated a session transfer number (“STN-TR”) and keeps track of sessions (either in alerting state, active, or held) to be able to perform session transfer. *Id.* at 720-21.

	The following implementation method determines if the ASCF should be included during registration: if Accused Products are roaming, based on the roaming agreement; based on local configuration; based on registered communication service of the Accused Products; based on the access type. <i>Id.</i> at 721. Upon session initiation, the Accused Products or the SCC AS establishes the Service Control Signaling Path for communication of service control signaling via the PS network using the Gm reference point. VASU 005865-953 at 80. The Accused Products established the calls via a wireless communication link with PLMN through gateways and interfaces supported by Evolved Packet Core (“EPC”) functions. EPC can be accessed via a trusted or untrusted network. There are differences when accessing these types of networks. However, the differences are not relevant to whether the Accused Products establish a communication link with an end destination device. The Supported EPC Functions <u>Trusted WLAN Access Network (“TWAN”)</u>: For access to PLMN’s EPC via a trusted non-3GPP access network such as trusted TWLAN, a connection shall be established between the Accused Products and TWAN using specific signal procedures. VASU 008198-326 at 230. Access authentication signaling for access to the EPC shall be executed between the Accused Products and the AAA server, which is an interface server, to ensure mutual authentication of the user and the EPC. <i>Id.</i> at 230. <u>Evolved Package Data Gateway (“ePDG”)</u>: ePDG is the local mobility anchor within untrusted non-3GPP access. VASU 006232-544 at 262. The PLMNs included in the ePDG information are the PLMNs that have roaming agreements with HPLMN. VASU 006232-544 at 269. Through a network interface (Swn interface), the ePDG connects with an untrusted non-3GPP access. VASU 005019-113 at 92. The ePDG connects with the Accused Products (through the SWu interface) to establish data tunnels and user data packet transmission within the tunnels. <i>Id.</i> at 93. <u>Call Session Control Function (“CSCF”)</u>: CSCF can act as Proxy CSCF (“P-CSCF”), serving CSCF (“S-CSCF”), emergency CSCF (“E-CSCF”), or Interrogating CSCF (“I-CSCF”). VASU 005019-113 at 56. The P-CSCF is the first contact point for the Accused Products within the International Mobile Subscriber Identity (“IMSI”); the S-CSCF actually handles the session states in the network; the E-CSCF handles
--	---

emergency sessions such as routing an emergency requests to the correct emergency center; the I-CSCF is the contact point within an operator’s network for all IMS connections destined to a subscriber of that network operator or roaming subscriber located within the network operator’s service area. *Id.*

Home Subscriber Server (“HSS”): The HSS supports the authentication procedures to access CS domain, PS domain, and system services by storing the generated data for authentication, integrity, and ciphering and by providing these data to the appropriate entities including AAA server or CSCF. VASU 005019-113 at 41. The diagram below illustrates . . .

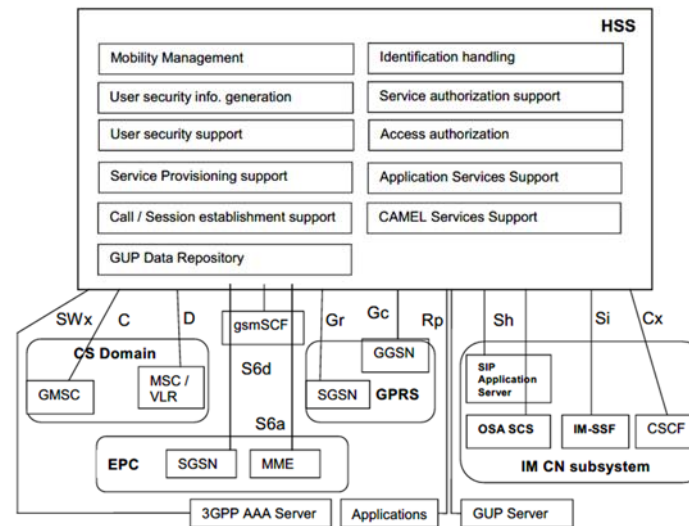


Figure 0.b: HSS logical functions

VASU 005019-113 at 40.

Authentication, Authorization, and Accounting (“AAA”): The Accused Products is authenticated and authorized through AAA to roam between networks. AAA server (interface server) is located at HPLMN and provides support for non-3GPP access users with services like authentication, authorization, and location management services to access evolved packet systems (“EPS”) in mobile networks. VASU 005019-113 at 49. It interacts with HSS to maintain consistent information to support service continuity

between 3GPP (mobile networks) and non-3GPP (Wi-Fi) networks. *Id.* It contains user information to gain access to non-3GPP access. *Id.* Non-3GPP access authentication defines the process to permit or deny a subscriber to attach to and use the sources of a non-3GPP IP access interworked with the EPC network. VASU 006232-544 at 307. Non-3GPP access authentication signaling is executed between the Accused Products and the AAA server/HSS (interface server). *Id.* During the authentication of the Accused Products for accessing the EPC via ePDG, ePDG shall initiate EAP-AKA based authentication between the Accused Products and the AAA server. VASU 006232-544 at 279.

After initiating the call, the Accused Products may roam between Wi-Fi networks and PLMN networks under multiple scenarios.

Exemplary Scenario 1: Wi-Fi to Wi-Fi

- (4) The Accused Products initiate a call within a first Wi-Fi network through VoIP or VoWiFi and roam from a first Wi-Fi network to a second Wi-Fi network.

The Accused Products may go out of range of access points and shift network association to another access point without losing connection. VASU 025133-44 at 134. Weak signals can trigger roaming on the Accused Products. *Id.* The Accused Products support 802.11k and 802.11v standards to reduce the length of time of lost connectivity during basic service set (“BSS”) transition. *Id.* at 138-42.

Exemplary Scenario 2: Wi-Fi to Home PLMN

- (7) The Accused Products initiate a call over a first Wi-Fi network through VoIP or VoWiFi and roam from the first Wi-Fi network to the coverage area of the home PLMN (“HPLMN”) of the Accused Products.
- (8) The Accused Products initiate a call within a first Wi-Fi network, but set up a backend of the call over PLMN network and roam from the first Wi-Fi network to the coverage area of the HPLMN of the Accused Products.

In a non-roaming scenario when the Accused Products establish the communication link with a home network, the trust relationship of Wi-Fi (non-3GPP IP wireless network) is determined by the HPLMN

operators. VASU 008198-326 at 227. The trust relationship is indicated to the Accused Products via either pre-configured policies in the Accused Products by the home PLMN operator or dynamic indication during 3GPP-based access authentication. *Id.*

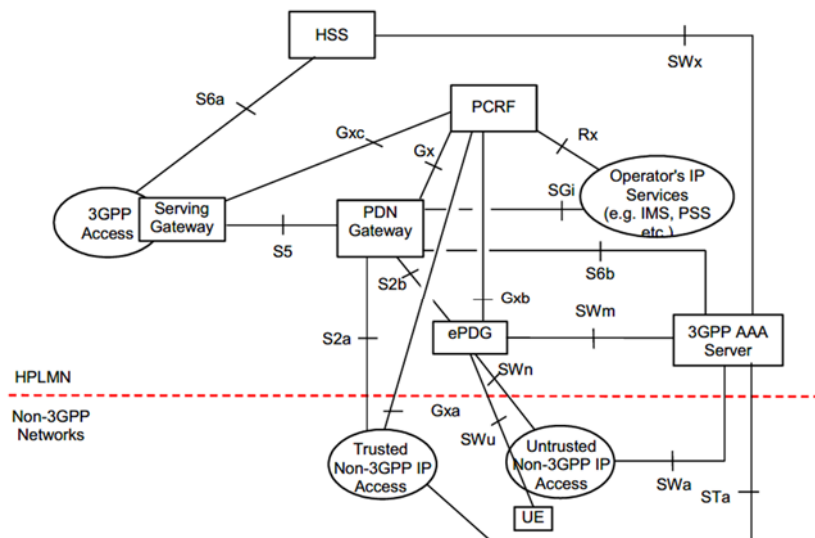


Figure 4.2.2-1: Non-Roaming Architecture within EPS using S5, S2a, S2b

VASU 006232-544 at 254 (non-roaming architecture showing trusted or untrusted non-3PPP wireless network connecting to AAA server in PLMN using the SWa or STa interface to access the trusted or untrusted 3GPP networks).

	Authorization of EPC access shall be performed by the AAA server upon successful user authentication. <i>Id.</i> <u><i>Exemplary Scenario 3: Wi-Fi to Visitor PLMN</i></u> (7) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over VoIP or VoWiFi, and roam from the first Wi-Fi network to the coverage area of a visitor PLMN (“VPLMN”) of the Accused Products. (8) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over a HPLMN, and roam from the first Wi-Fi network to the coverage area of a VPLMN. In roaming scenario when the Accused Products establish the communication link with a visitor network, the HSS or AAA server (interface server) in HPLMN makes the final decision if a non-3GPP wireless network is trusted or untrusted. VASU 006232-544 at 260. The HSS/AAA server (interface server) may take the visitor PLMN (“VPLMN”) policy and capability returned from the AAA proxy or roaming agreement into account. <i>Id.</i> at 260.
--	---

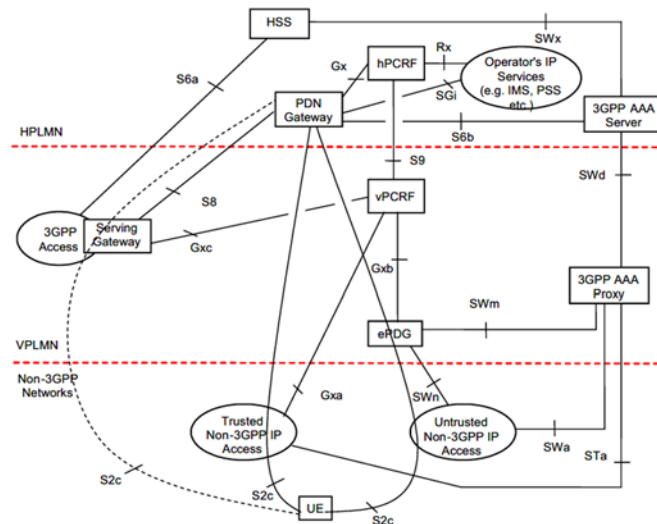


Figure 4.2.3-3: Roaming Architecture for EPS using S8 – S2c - Home Routed

VASU 006232-544 at 258 (roaming architecture showing trusted or untrusted non-3GPP IP access to AAA server/proxy in PLMN through STa or SWa interface).

The session origination procedures specify the signaling path between the Accused Products initiate a session setup attempt and the S-CSCF assigned to perform the session origination service. VASU 005263-653 at 380. The Accused Products initiate a session setup attempt and assigned a S-CSCF to perform the session origination service. VASU 005263-653 at 380. The signaling path between the Accused Products and S-CSCF is determined at the time of the Accused Products registration. *Id.* The S-CSCF to application server interface is used to provide services in the application server in the HPLMN or in a trusted external network (e.g., third-party or VPLMN). VASU 005019-113 at 58.

If the Accused Products are located in a VPLMN, it determines the P-CSCF via the CSCF discovery procedure. VASU 005263-653 at 380. The HPLMN advertises the S-CSCF as the entry point from the VPLMN. *Id.* When registration is completed, P-CSCF knows the name/address of the next hop in the signaling path toward the S-CSCF. *Id.* If the Accused Products are located in the HPLMN, the HPLMN

	allocates an S-CSCF in the HPLMN. <i>Id.</i> at 383. When registration is completed, P-CSCF knows the name/address of S-CSCF. <i>Id.</i> <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
39[b]. monitoring a signal strength of the first wireless communication link;	The Accused Products monitor the signal strength of their communication link to the wireless network. This is performed through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi Settings” in A Series, S Series, X Cover, and Z Series. VASU 010302-454 at 398 (A13 5G); VASU 010601-745 at 691 (A14 5G); VASU 011048-196 at 143 (A23 5G/A23 5G UW); VASU 011532-691 at 633 (A53 5G/A53 5G UW); VASU 011692-852 at 792 (A54 5G); VASU 018745-906 at 848 (S20 FE 5G); VASU 019244-407 at 351 (S21 5G/ S21 Ultra 5G/ S21+ 5G); VASU 019782-949 at 895 (S22/S22+/S22 Ultra); VASU 019950-20128 at 1070 (S23/S23+/S23 Ultra); VASU 023406-563 at 508 (XCover Pro); VASU 023564-725 at 672 (Z Flip 5G); VASU 023894-4071 at 1014 (Z Fold3 5G/Z Flip3 5G); VASU 024756-929 at 877 (Z Flip4); VASU 024408-577 at 520 (Z Fold2 5G). “Switch to Mobile Data” is an improved technology to “automatically switch[] networks based on both network quality and user preferences.” VASU 025185-91 at 187. The connection manager will not be active until it accumulates enough data to determine user preference. <i>Id.</i> <i>Id.</i> at 187 (determining user preference). Through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi settings” on the Accused Products (shown below), the Accused Products can seamlessly switch to

mobile data if there are signal strength issues and “whenever the Wi-Fi connection is unstable.” VASU 019950-20128 at 1070. When the Wi-Fi signal strength is strong, it switches “back to Wi-Fi.” *Id.*

Intelligent Wi-Fi settings

You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider.

1. From Settings, tap  **Connections > Wi-Fi**, and then tap  to turn on Wi-Fi.
2. Tap  **More options > Intelligent Wi-Fi** for the following options:
 - **Switch to mobile data:** When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi.
 - **Switch to better Wi-Fi networks:** Automatically switch to faster or more stable Wi-Fi networks.
 - **Turn Wi-Fi on/off automatically:** Turn on Wi-Fi in frequently-used locations.
 - **Show network quality info:** Display network information (such as speed and stability) in the list of available Wi-Fi networks.
 - **Prioritize real-time data:** Give network priority to games, video calls, and other tasks that are sensitive to lag.
 - **Detect suspicious networks:** Get notified when suspicious activity is detected on the current Wi-Fi network.
 - **Wi-Fi power saving mode:** Enable Wi-Fi traffic analysis to reduce battery usage.
 - **Auto Hotspot connection:** Automatically connect to a Wi-Fi hotspot when detected.
 - **Intelligent Wi-Fi:** View the Intelligent Wi-Fi version.

VASU 019950-20128 at 1070 (intelligent Wi-Fi settings in an exemplary S23+ phone).

Similarly, the Accused Products include a “Switch to Mobile Data” feature under “Wi-Fi Preferences.” VASU 012187-372 at 300 (Amp Prime 3); VASU 012624-795 at 737 (J2); VASU 013258-446 at 375 (J7); VASU 013447-617 at 557 (J7 V); VASU 012938-3112 at 1050 (J7 Prime); VASU 017373-567 at 490 (S7); VASU 016965-7166 at 1090 (S7 Active); VASU 017167-372 at 294 (S7 Edge); VASU 013837-4053 at 986 (Note 9).

	Wi-Fi preferences Customize advanced Wi-Fi services. 1. From  Settings, tap Connections > Wi-Fi, and then tap On/Off to turn on Wi-Fi. 2. Tap  More options > Advanced. To view all network settings, tap View more. • Switch to mobile data: Connect automatically to a mobile network connection when the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi. • Turn on Wi-Fi automatically: Enable Wi-Fi in frequently used locations. • Wi-Fi power saving mode: Reduce battery usage by analyzing Wi-Fi traffic patterns. • Wi-Fi notifications: Receive notifications when open networks in range are detected. • Show Wi-Fi pop-up: When opening apps, indicate when Wi-Fi is available. VASU 013837-4053 at 3977. Moreover, the Accused Products include “Switch to Mobile Data” product feature in “Advanced Wi-Fi Settings” to switch between mobile and Wi-Fi networks. VASU 009579-721 at 669 (A02s); VASU 009855-10011 at 116 (A10e); VASU 010011-157 at 104 (A11); VASU 010158-301 at 250 (A12); VASU 010455-600 at 546 (A13); VASU 010746-901 at 851 (A20); VASU 010902-1047 at 996 (A21); A51_User_Manual.pdf at 116 (A51); VASU 011197-367 at 315 (A51 5G/A51 5G UW); VASU 011368-531 at 477 (A52 5G); VASU 011853-2015 at 958 (A71 5G); VASU 012016-2186 at 2134 (A71 5G UW); VASU 015086-267 at 209 (Note 10+); VASU 014054-245 at 191 (Note 20 5G/Note 20 Ultra 5G); VASU 017730-891 at 838 (S8), VASU 017568-729 at 676 (S8 Active); VASU 017892-8059 at 8006 (S8+); VASU 018060-236 at 183 (S9/S9+); VASU 018399-571 at 511 (S10/S10e/S10+); VASU 018237-398 at 345 (S10 Lite); VASU 018907-9076 (S20 5G/S20 Ultra 5G/S20+ 5G); VASU 024244-407 at 348 (Z Fold);
--	--

VASU 023090-256 at 199 (XCover 6 Pro); VASU 023257-405 at 358 (XCover FieldPro); VASU 012482-623 at 570 (J2 Pure); VASU 012796-937 at 890 (J3); VASU 013113-257 at 209 (J7 Star).

Advanced Wi-Fi settings

You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by carrier.

1. From Settings, tap  **Connections > Wi-Fi**, and then tap  to turn on Wi-Fi.
2. Tap  **More options > Advanced**.
 - **Sync with Samsung Cloud/account:** Sync Wi-Fi profiles with your Samsung account.
 - **Switch to mobile data:** When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi.
 - **Turn on Wi-Fi automatically:** Turn on Wi-Fi in frequently-used locations.
 - **Detect suspicious networks:** Get notified when suspicious activity is detected on the current Wi-Fi network.

VASU 010455-600 at 546.

The Accused Products include “Intelligent Wi-Fi” feature in “Wi-Fi Settings,” which switches between mobile and Wi-Fi networks depending on the signal strength. VASU 020129-301 at 243 (S24/S24+/S24 Ultra); VASU 024756-929 at 874 (Z Fold4/Z Flip4).

	Wi-Fi settings You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider. 1. From Settings, tap  Connections > Wi-Fi, and then tap  to turn on Wi-Fi. 2. Tap  More options for the following options: • Wi-Fi Direct: Share data directly between devices over Wi-Fi. • Intelligent Wi-Fi: Configure Wi-Fi switching and detection features. • Advanced settings: Configure Wi-Fi connections and Hotspot settings. • Contact us: Contact Samsung support through Samsung Members. VASU 024756-929 at 874 (Z Fold4/Z Flip4). The Accused Products measure signal strength of Wi-Fi networks by Received Signal Strength Indicator (“RSSI”), and its unit of measurement is dBm. The table below provides a point of reference for interpreting the RSSI value.
--	--

Signal Strength	TL;DR		Required for
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWi-Fi, streaming video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

VASU 025540-45 at 43-44.

The screenshot below illustrate that the Accused Products continuously monitor the signal strength.



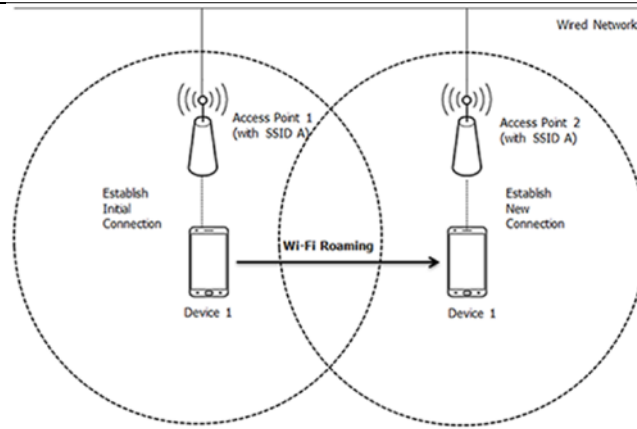
VASU 031389-98 at 96.

The Accused Products include “Auto Wi-Fi,” which turns Wi-Fi on and off depending on locations. VASU 025185-91 at 88. It turns Wi-Fi on when the favorite network is available by user preference and turns off Wi-Fi when this network is unavailable. *Id.* Auto Wi-Fi is triggered based on user’s location by geofencing (a virtual geological fence based on cellular stations). *Id.*

Furthermore, The Wi-Fi network selection functions in the Accused Products continuously

	evaluate the quality of the connected network and assess the quality of available networks. VASU 025102-18 at 02. The Accused Products scan the available networks depending whether the screen of the Accused Products is on or off. <i>Id.</i> If the screen of the Accused Products is on and the Accused Products is connected, the Wi-Fi framework of the Accused Products evaluates whether the current network is good enough to skip network selection when all the following conditions are met: (1) the RSSI is above the required RSSI threshold or sufficient traffic is flowing over the connection; (2) the network is evaluated, or user approved for use without internet access; and (3) the network is unmetered. <i>Id.</i> at 03. If the connection isn't good enough, the connectivity subsystem triggers a scan to detect available networks. <i>Id.</i> Moreover, if the screen is on and the Accused Products are disconnected, the Android connectivity system issues periodic scans (activation of a timer) following an exponential back off schedule (increasing the waiting time between retries). <i>Id.</i> at 02. The module evaluates scan results received by evaluating if the signal level is below a predefined threshold and tries to select the best network to connect to. <i>Id.</i> When the Accused Products' screen is off, the network selection process might occur if scans are initiated by other services such as location services. <i>Id.</i> at 06. When the Accused Products are active in an IMS session, the session transfer procedures provide session continuity between wireless networks using signal strength information. VASU 005654-93 at 62. The Accused Products initiate session transfer procedure based on trigger criteria, including the current operator policy, user preferences, and wireless network conditions for conducting a session continuity operation to the SCC AS (interface server). VASU 005654-93 at 64. A third-party call control function (call function from the Accused Products) is employed for subscriber IMS sessions at the SCC AS upon session establishment for enablement of Session Transfer. <i>Id.</i> <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
--	--

39[c]. when the signal strength drops below a threshold, notifying an interface server and establishing a second communication link between the interface server and the end destination device without disrupting the first communication link;	The Accused Products determine when the signal strength through a wireless communication link drops below a certain signal strength/stability threshold. When this occurs, the Accused Products notify the SCC AS (interface server) to establish a new (second) secondary communication link through a second network through session continuity or Wi-Fi detection functions of the Accused Products. The Android Wi-Fi framework or firmware of the Accused Products periodically monitors the signal strength (or RSSI) of the first communication link to decide if the RSSI is below a certain threshold. VASU 025102-18 at 05. When the screen of the Accused Products is on, and the Wi-Fi service may poll RSSI and link-layer stats every 3 seconds or by other configuration (config_wifiPollRssiIntervalMilliseconds or config_wifiAdjustPollRssiIntervalEnabled for dynamic adjustment based on the device mobility state and RSSI). <i>Id.</i> The polling interval is extended to 6 seconds when the device is stationary and RSSI is above -68 dBm (configured by the config_wifiClientRssiMonitorThresholdDbm and config_wifiClientRssiMonitorHysteresisDb), which is the pre-defined threshold value. <i>Id.</i> The polling interval is reduced back to 3 seconds (the second time window configured by the config_wifiPollRssiIntervalMilliseconds) when the device is non-stationary or RSSI is below -73 dBm, which is another pre-defined threshold value. <i>Id.</i> Once connected, the Wi-Fi service calculate “a connected score” based on the RSSI and determine whether to connect to a Wi-Fi network or another network type, such as a mobile network. <i>Id.</i> at 04-05. the Wi-Fi service may pass the score to the connectivity service, which uses the score to determine whether to connect to a Wi-Fi network or to a mobile network. <i>Id.</i> at 06.
--	---



VASU 025133-44 at 34 (roaming from one Wi-Fi to another Wi-Fi access point is triggered due to weak signal).

Through “Switch to mobile data” or “Switch to better Wi-Fi networks” product features in “Intelligent Wi-Fi” on the Accused Products (shown below), the Accused Products can seamlessly switch to mobile data if there are signal strength issues and “whenever the Wi-Fi connection is unstable.” VASU 019950-20128 at 1070. When the Wi-Fi signal strength is strong, it switches “back to Wi-Fi.” *Id.*

Intelligent Wi-Fi settings

You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider.

1. From Settings, tap  **Connections > Wi-Fi**, and then tap  to turn on Wi-Fi.
2. Tap  **More options > Intelligent Wi-Fi** for the following options:
 - **Switch to mobile data:** When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi.
 - **Switch to better Wi-Fi networks:** Automatically switch to faster or more stable Wi-Fi networks.
 - **Turn Wi-Fi on/off automatically:** Turn on Wi-Fi in frequently-used locations.
 - **Show network quality info:** Display network information (such as speed and stability) in the list of available Wi-Fi networks.
 - **Prioritize real-time data:** Give network priority to games, video calls, and other tasks that are sensitive to lag.
 - **Detect suspicious networks:** Get notified when suspicious activity is detected on the current Wi-Fi network.
 - **Wi-Fi power saving mode:** Enable Wi-Fi traffic analysis to reduce battery usage.
 - **Auto Hotspot connection:** Automatically connect to a Wi-Fi hotspot when detected.
 - **Intelligent Wi-Fi:** View the Intelligent Wi-Fi version.

VASU 019950-20128 at 1070 (intelligent Wi-Fi settings in an exemplary S23+ phone). The Accused Products can also switch to better Wi-Fi networks by “automatically switch[ing] to faster or more stable Wi-Fi networks.” VASU 019950-20128 at 1070.

Session Continuity between Mobile Networks

When the signal strength drops below a predetermined threshold, the Accused Products may also use locally stored data for selecting a second EPC network available for connectivity via the currently selected non-3GPP wireless network to establish a second communication link. VASU 008198-326 at 222. UE shall select a PLMN according to the PLMN selection procedure of the selected non-3GPP wireless network. *Id.*

Signaling and bearer resources are allocated in the transferring-in wireless network and the user's sessions are transferred from the transferring-out wireless network. VASU 005654-93 at 669. The SCC AS executes access transfer procedures and resources in the transferring-out wireless network is released. *Id.*

The Accused Products establish the second communication link (the second call session with the second network, transferred-in network) with the transfer-in network without disrupting the first communication link in the transfer-out network. IMS sessions from and to the Accused Products are anchored at the SCC AS in the home IMS based on initial filtering criteria (“iFC”) to provide service continuity for the user during the transition between two wireless networks. VASU 005654-93 at 62.

For single radio voice call continuity (“SRVCC”), voice call continuity between PLMN/VPLMN over PS and CS are anchored when the UE is capable of transmitting or receiving only one of the access networks at a given time. VASU 005195-214 at 200.

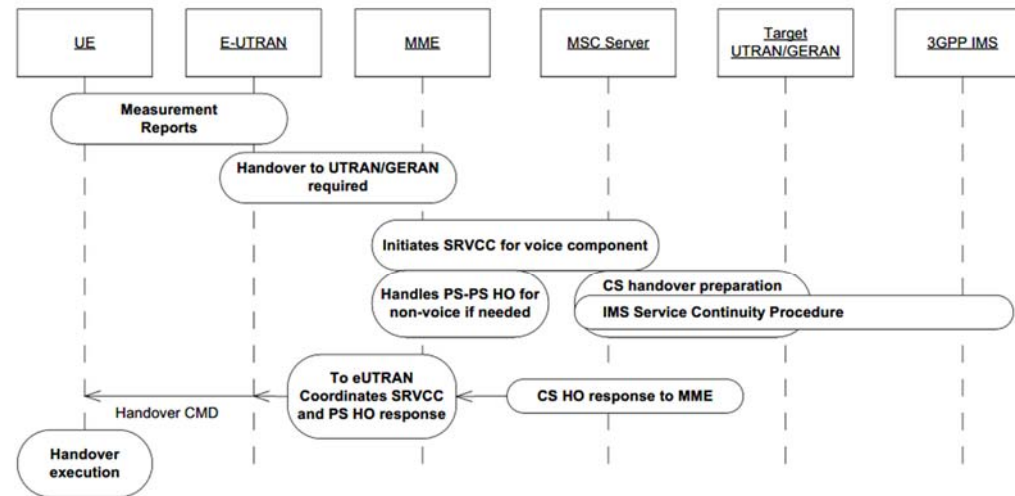


Figure 4.2.2-1: Overall high level concepts for SRVCC from E-UTRAN to UTRAN/GERAN

VASU 005195-214 at 202 (how SRVCC works in E-UTRAN, 4G to UTRAN/GERN, 3G/2G).

A third-party call control function (functions provided by the Accused Products) is employed at the SCC AS to facilitate inter-access network mobility through the user of access transfer between the two wireless networks. *Id.*

PS-CS transfer

IMS session established in CS or PS wireless networks are anchored at the SCC AS. VASU 005654-93 at 662. IMS sessions using CS bearer are established at session setup or upon access transfer. *Id.*

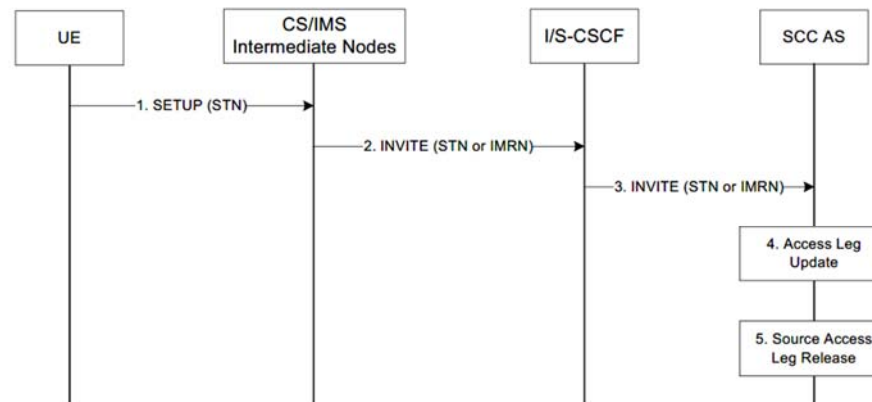


Figure 6.3.2.1.1-1: PS – CS Access Transfer: PS to CS

VASU 005654-93 at 72 (user is active in an IMS originating or terminating session using PS media at the time of transfer).

CS-PS Transfer

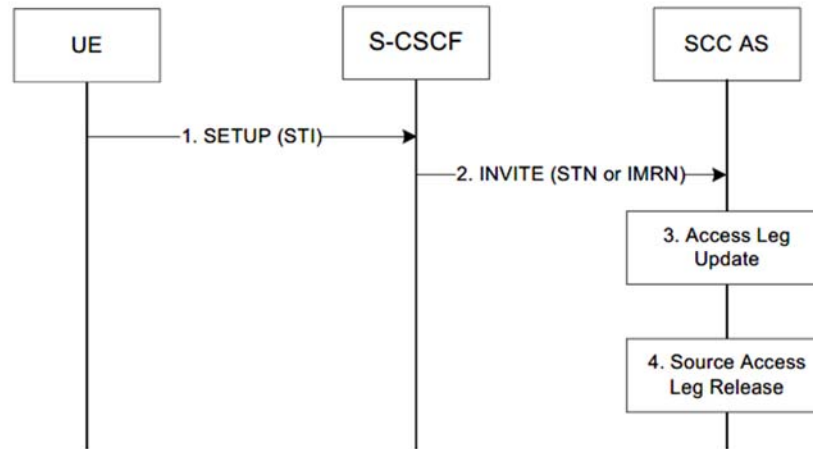


Figure 6.3.2.1.2-1: PS – CS Access Transfer: CS to PS

VASU 005654-93 at 73 (the user is active in the IMS originating or terminating session using CS at the time of transfer).

PS-PS Transfer

US is attached to one IP connectivity access network (“IP-CAN”), and it registers to the S-CSCF. VASU 005654-93 at 75. UE-1 and UE-2 establish an active multimedia session via this IP-CAN. *Id.* After changing to a new IP-CAN, obtaining new signaling and media addresses, and completing the Access Transfer procedures, UE-1 continues the session with UE-2 on the new IP-CAN. *Id.*

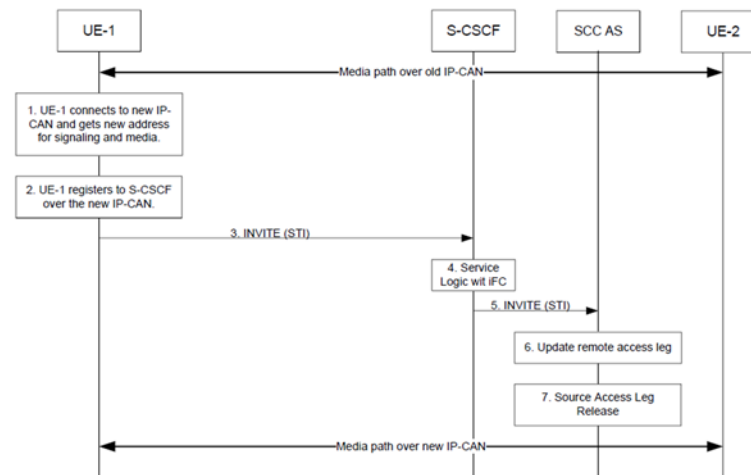


Figure 6.3.2.2.1-1: Information flow for PS-PS Access Transfer

Id.

Session Continuity between Wi-Fi and Mobile Networks

Upon the Accused Products' request, the access network discovery and selection function ("ANDSF") in either HPLMN or VPLMN may provide a list of wireless access networks available in the vicinity of the UE for all the access technology types requested by the UE to establish a second communication link through Wi-Fi. VASU 006232-544 at 293. An ANDSF element located in the HPLMN of a UE is referred to as Home-ANDSF ("H-ANDSF") and an ANDSF element located in the visited PLMN of a UE is referred to as the visited-ANDSF (V-ANDSF) for this UE. VASU 006232-544 at 291. The H-ANDSF in the subscriber's HPLMN may interact with HSS user profile information. *Id.* at 61.

The ANDSF provides information for access networks that are available to the UE including:

- the access technology type (e.g. WLAN, WiMAX).
- the radio access network identifier (e.g. the SSID of a WLAN).
- other technology specific information, e.g. one or more carrier frequencies.
- validity conditions, i.e. conditions indicating when the provided access network discovery information is valid (such conditions may include e.g. a location).

VASU 006232-544 at 293.

ANDSF contains data management and control functionality necessary to provide network discovery and selection assistance data per operator's policy. VASU 006232-544 at 292. ANDSF may provide other information, including access network discovery information, WLAN selection information, and ePDG configuration information. VASU 008198-326 at 252. If the UE is roaming in a VPLMN, the UE may receive Inter-system mobility policies or access network discovery information from H-ANDSF or V-ANDSF or both. *Id.*

Moreover, access network selection and traffic steering between 3GPP access and WLAN is supported using ANDSF and is also supported using radio access network rule procedure without ANDSF. VASU 006232-544 at 290.

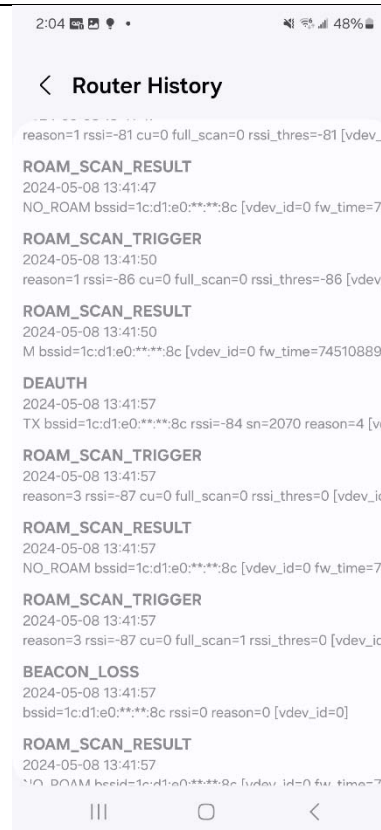
The home network preference may be provided by the Accused Products' HPLMN and include information that assists the UE to select a WLAN network and to select a PLMN for 3GPP-based authentication over WLAN. VASU 006232-544 at 297. Similarly, a visited network preference may be provided by the VPLMN, but UE shall ignore the preference if provided a HPLMN preference. *Id.*

DOE

To the extent that Defendants contend that the Accused Products do not literally satisfy this limitation, Defendants infringe under the doctrine of equivalents because they perform substantially the same function, in substantially the same way, to achieve substantially the same result.

The Accused Products perform substantially the same function because they monitor the second context (signal strength) of the first communication link through "Intelligent Wi-Fi" product feature and switch on-going call or data stream sessions with the end user device to a second communication link through "Switch to Mobile Data" product functions and notifying the interface server without interrupting the call or data streaming sessions. *See, e.g.*, VASU 019244-407 at 351; VASU 013837-4053 at 977; VASU 025185-91 at 187. Moreover, the Accused Products' network switching functions act as an interface server connecting with the Wi-Fi or the mobile network. The Accused Products function in substantially the same way because the "Intelligent Wi-Fi" product feature switch the first communication link to the second communication link when the signal strength (context) of the Wi-Fi network is below a pre-defined

	threshold. <i>See, e.g.</i>, VASU 025185-91 at 187; VASU 025102-18 at 02. The Accused products switch to a second communication link without interrupting the current call or data stream sessions by holding the call or data streaming session after notifying the interface server. <i>See, e.g.</i> VASU 025133-44 at 34; VASU 005654-93 at 69. The Accused Products achieve substantially the same result because the Accused Products switch an on-going call or data streaming sessions to a second communication link seamlessly when the signal strength (context) of the first communication link drops below a threshold value. The Accused Products accomplish this result by notifying an interface server through “Intelligent Wi-Fi” product feature to hold the current session while switching to the second communication link. <i>See, e.g.</i>, VASU 006232-544 at 290; VASU 025102-18 at 1; VASU 005654-93 at 69. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
39[d]. notifying the mobile communication device to terminate transmission over the first communication link; and	The Accused Products will notify them to terminate a wireless communication link when appropriate, according to its connection criteria and signal strength. For example, in the representative Accused Product—the Galaxy S22—screenshot below, the device sent a DEAUTH command when the RSSI value was -84 dBm, thereby terminating the Wi-Fi connection.

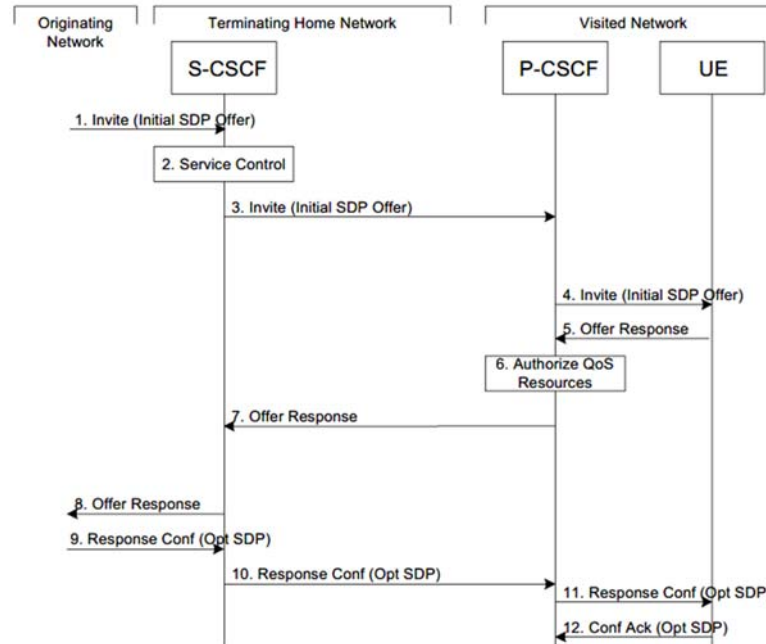


VASU 031389-98 at 97.

The SCC AS notifies the Accused Products through the service control signaling path to terminate transmitting over the first communication link (access leg) with the first wireless network.

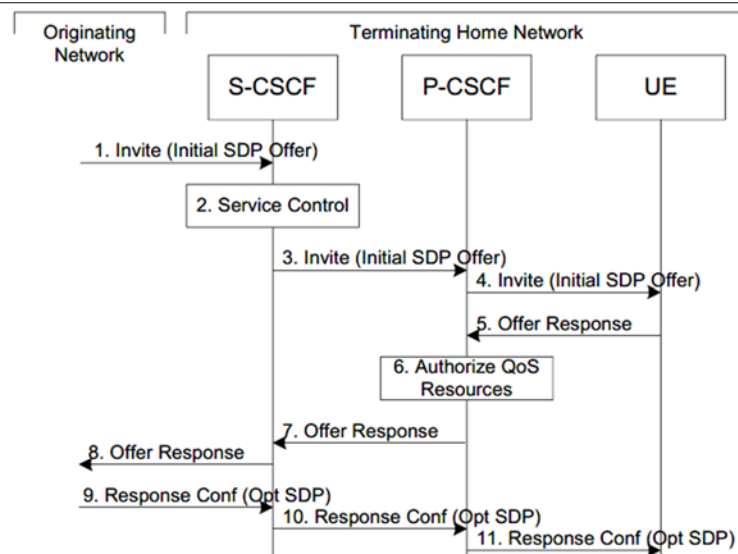
The termination procedures specify the signaling path between the S-CSCF assigned to perform the session termination service and the Accused Products. VASU 005263-653 at 392. The signaling path is determined at the time of UE registration and remains fixed for the life of the registration. *Id.*

When registration is completed in the roaming scenario, S-CSCF knows the name/address of its next hop in the signaling path and the P-CSCF, and P-CSCF knows the name/address of the UE. *Id.*



VASU 005263-653 at 393 (mobile termination procedure during roaming scenario).

When registration is completed in non-roaming scenario, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE. *Id.* at 395.



Id. at 395 (mobile termination procedure during non-roaming scenario).

For detection of conditions requiring session transfer, the Accused Products establish an access leg with the SCC AS via the transferred-in wireless network to request session transfer to the transferred-in wireless network. VASU 005654-93 at 70. When the UE initiates a session transfer request, it includes the session transfer identifier. *Id.* The SCC AS executes the session transfer procedure by replacing the access leg currently communicating to the remote leg (the first communication link) with the access leg established via the transferred-in access (the second communication link). *Id.* The access leg established via the transferred-out wireless network is subsequently released (terminating the first communication link). *Id.* If the SCC AS detects that the Accused Products are not reachable over Service Control Signaling Path, the SCC AS should clear all held sessions related to the user if any are present and update the remote leg if necessary. VASU 005865-953 at 912.

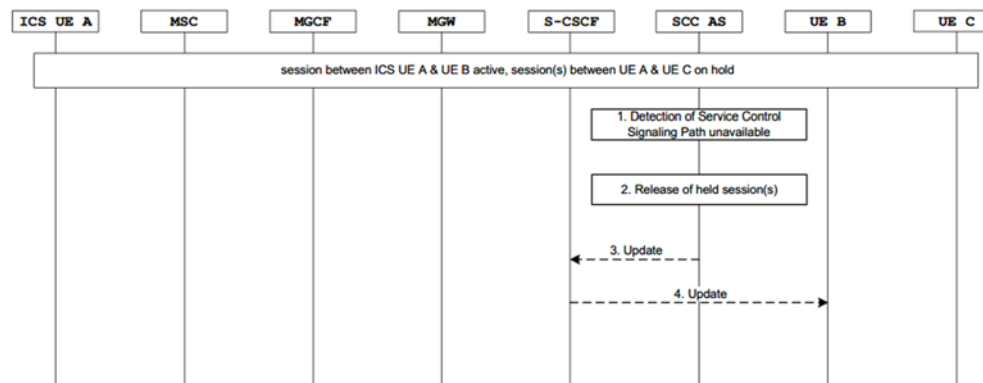


Figure 7.5.1.1.3-1: release of held sessions at SCC AS when Service Control Signaling Path unavailable

VASU 005865-953 at 912.

A delete session request message will notify the Accused Products (UEs) to terminate transmission of the first call session with the first wireless network (transfer-out). The “Delete Session Request” (shown below) is sent over the S2b interface of EPC as part of the following procedure: UE/ePDG initiated detach, UE requested disconnection with packet data network (“PDN”), or HSS/AAA initiated detach. VASU 009199-578 at 307.

	SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)			
32	Create Session Request		X	
33	Create Session Response			X
36	Delete Session Request		X	
37	Delete Session Response			X

VASU 009199-578 at 226.

SOURCE CODE SUPPLEMENTATION

As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.

39[e]. re-directing the second communication link from the interface server to another mobile communication device, thereby establishing a second wireless communication link between the mobile communication device and a second wireless network,	The Accused Products redirect to the second communication link to maintain the connection by the mobile communication device to transparently maintain a connection. For example, in the representative Accused Product—the Galaxy S22—screenshot below, the device shows a connection to both the 5G cellular network and a WiFi network. The screenshot shows the home screen of a Samsung Galaxy S22. At the top, the status bar displays the time 2:10, signal strength, 5G cellular network, Wi-Fi, and 47% battery. The main display features a weather widget for Washington showing 86° and 'Partly Cloudy'. Below the widget is a Google search bar. The app drawer shows icons for the App Store, Play Store, Google, and OneDrive. The bottom dock contains icons for Phone, Messages, Chrome, and Camera. The navigation bar at the very bottom shows the standard Android navigation icons (back, home, recent apps). VASU 031389-98 at 98. The Accused Products, upon receiving a request for execution of session transfer, use the SCC AS (interface server) to perform the access leg update by switching (re-directing) the access leg communicating with the remote leg from transferring-out access to transferring-in access. VASU 005654-
--	---

93 at 70. The SCC AS subsequently coordinates the session control signaling exchange between the access leg and the remote leg associated with a subscriber IMS session, thereby establishing a second wireless communication link between the Accused Products and the second network. *Id.*

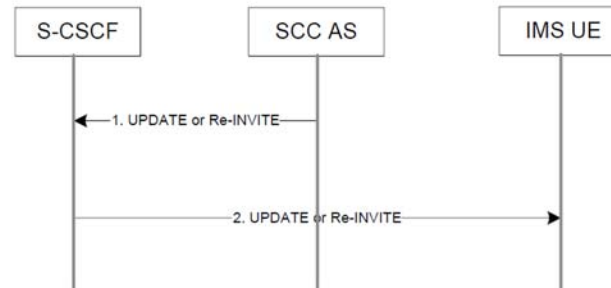


Figure 6.3.1.5-1: Access Leg Update toward the remote end

VASU 005654-93 at 71 (how access leg is updated toward the remote end). The SCC AS updates the access leg by communicating the session description protocol (“SDP”) of the Access leg established in the transferring-in access to the remote end via the user’s S-CSCF. *Id.*

When the Accused Products determine that the access transfer is desirable because the signal strength drops below a pre-determined threshold based on criteria such as operator policy or user preferences, a registration in IMS is performed by the UE via the transferring-in wireless network if the user is not already registered via that network. VASU 005654-93 at 69.

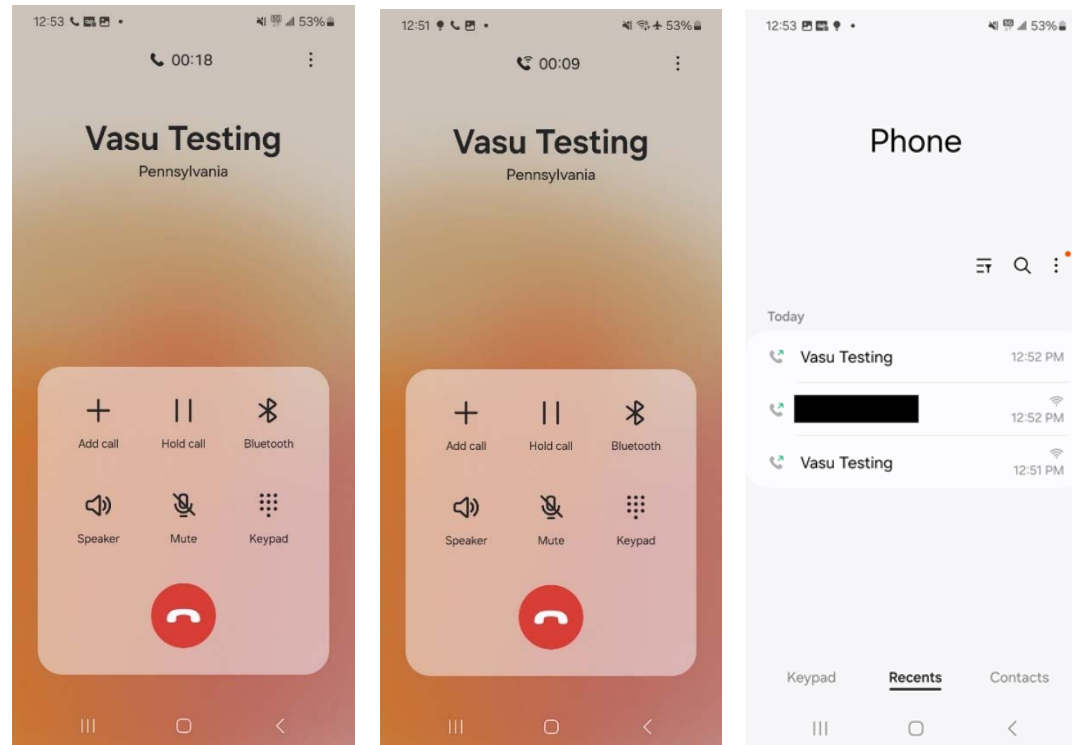
The create session request is part of the procedure to hand over to untrusted or trusted non-3GPP access from ePDG/TWAN to PGW via S2b interface of EPC. VASU 009199-578 at 234. The ePDG/TWAN may include AAA server identifier in the create session request to the PGW through S2a/S2b interface. VASU 009199-578 at 247 (information element in a create session request).

	<table border="1" data-bbox="747 191 1669 376"> <tr> <th data-bbox="747 191 961 253"></th><th data-bbox="961 191 1669 253">SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)</th></tr> <tr> <td data-bbox="747 253 961 282">32</td><td data-bbox="961 253 1669 282">Create Session Request</td></tr> <tr> <td data-bbox="747 282 961 311">33</td><td data-bbox="961 282 1669 311">Create Session Response</td></tr> <tr> <td data-bbox="747 311 961 341">36</td><td data-bbox="961 311 1669 341">Delete Session Request</td></tr> <tr> <td data-bbox="747 341 961 376">37</td><td data-bbox="961 341 1669 376">Delete Session Response</td></tr> </table> VASU 009199-578 at 226 (message types for GRPS Tunneling Protocol in PLMN). The direction of the message is from MME/S4-SGSN to SGW, from SGW to PGW, and from ePDG/TWAN to PGW. VASU 009199-578 at 233. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.		SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)	32	Create Session Request	33	Create Session Response	36	Delete Session Request	37	Delete Session Response
	SGSN/MME/ TWAN/ePDG to PGW (S4/S11, S5/S8, S2a, S2b)										
32	Create Session Request										
33	Create Session Response										
36	Delete Session Request										
37	Delete Session Response										
39[f]. wherein upon activation of a timer, the mobile communication device causes a communication module to change state from a sleep mode to a stand-by mode, and the mobile communication device causes the communication module to change state from the stand-by mode to an active	As described in Element 12[d], the timer (pre-define time window) is activated, and through the switching system (“Switch to mobile data” or “Switch to better Wi-Fi networks”), the Accused Products (mobile communication devices) cause the second communication module to change state from the stand-by to an active mode before the communication (video/voice/data) is switched to the Wi-Fi communication module. The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module.										

mode before a communication is switched to the communication module.	<u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
Claim 41	
41[pre]. A method comprising:	As described in Element 1[pre], the Accused Products (also referred to as user equipment, UEs) perform every step of the method of the claims through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi Settings” or “Wi-Fi preferences,” “Wi-Fi Settings,” or “Advanced Wi-Fi Settings” of the Accused Products.⁷ The feature allows the Accused Products to roam and switch between different wireless networks, such as a WiFi wireless network and cellular networks including General Packet Radio Service (“GPRS,” 2G), Global System for Mobile (“GSM,” 2G), Code-Division Multiple Access (“CDMA,” 3G), Long Term Evolution (“LTE,” 4G), or 5G network. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
41[a]. monitoring a context of a first wireless communication link;	The Accused Products establish a communication link with a destination device and monitor the context of the first communication link. The Accused Products operated as mobile communication devices that establish a voice call or data stream sessions (a first communication link) between the Accused Products and an end destination device (another user equipment) such as a mobile phone, a laptop, the Internet of Things, or server. In the context of a voice call, the call can be over a VoIP or VoWiFi network (“Internet”) or a public land mobile network (“PLMN”), defined by the 3GPP standards. This first communication link is over a first network, either a Wi-Fi network or a PLMN or Cellular Network. For example, with respect to a voice call, it can be initiated within the Wi-Fi network or over the

⁷ These features were previously branded as “Smart Network Switch” and “Adaptive Wi-Fi.”

PLMN/Cellular Network. Compare left screenshot (illustrating a cellular call via 5G by the lack of Wi-Fi symbol in the top ribbon and showing 5G cellular connectivity), with middle screenshot (illustrating a WiFi call by noting the phone is in airplane mode and by bearing a Wi-Fi symbol above the phone symbol); see also right screenshot (showing two calls made to the contact “Vasu Testing” where the earlier call has a Wi-Fi symbol above the time indicating a Wi-Fi call and the later call does not have a Wi-Fi symbol above the time indicating a cellular call).



VASU 031389-98 at 93-95.

The first connection link between the Accused Product and end destination device can be made under at least three scenarios: (1) Wi-Fi to Wi-Fi connection, (2) Wi-Fi to Home PLMN, and (3) Wi-Fi to Visitor

PLMN. The vice versa is also true. Wi-Fi, Home PLMNs, and Visitor PLMNs are type of wireless networks.

Establishing the First Communication Link

The first communication link (voice or video call) uses IP Multimedia Core Network Subsystem (“IMS”), which is the framework for delivering multimedia services using PS and CS bearers (data tunnels between the network gateways and the Accused Products) for the media. VASU 005654-93 at 58. IMS service continuity requires a Service Centralization and Continuity (“SCC”) Application Server (“AS”). VASU 005654-93 at 63. The SCC AS is a home network based IMS application that provides functionality required to enable IMS centralized services. VASU 005865-953 at 77. The screenshot below illustrates the information used for IMS service continuity that may be provided between SCC AS and the Accused Products:

- session transfer indicator to indicate that this new session is for session transfer.
- details about the access and the media components being transferred / kept / released.
- optionally, an IMS Communication Service Identifier defined in 3GPP TS 23.228 [7]
- which session is required to be replaced or updated;
- whether to merge the session(s):

VASU 005654-93 at 63. SCC AS provides an IMS-based mechanism for enabling session continuity. It executes the transfer of the IMS session between different wireless networks and implements third-party call control upon session establishment. VASU 005654-93 at 64.

A Service Control Signaling Path transports service control signaling between the Accused Products and the SCC AS when using CS or PS access. VASU 005865-953 at 79. The access leg is formed by combining the Service Control Signaling Path and the CS Bearer Control Signaling Path. VASU 005865-953 at 80. The SCC AS presents the remote leg to the CSCF as an IMS session using IMS SIP signaling on behalf of the Accused Products. *Id.*

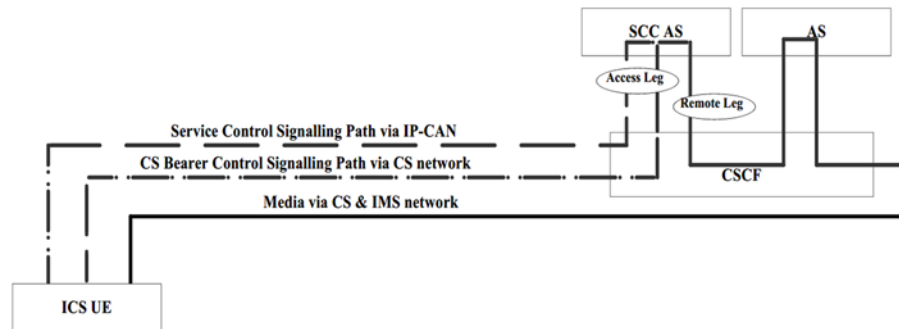


Figure 7.1.1-1: ICS UE session signalling and bearer path using PS network for Service Control Signalling Path

VASU 005865-953 at 80 (Accused Products (or UEs), session signaling and bearer path in access leg and remote leg in PS network).

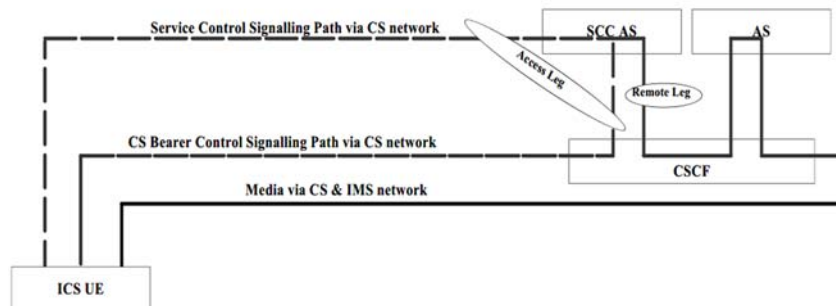


Figure 7.1.1-2: ICS UE session signalling and bearer path using CS network for Service Control Signalling Path

VASU 005865-953 at 80 (Accused Products (or UEs), session signaling and bearer path in access leg and remote leg in CS network).

Moreover, the access transfer control function (“ASCF”) is a function in HPLMN or visitor network (“VPLMN”) may be co-located with the existing functional entities such as P-CSCF. VASU 005694-864 at 720. Based on carrier policy, it shall be allocated a session transfer number (“STN-TR”) and keeps track of sessions (either in alerting state, active, or held) to be able to perform session transfer. *Id.* at 720-21.

	The following implementation method determines if the ASCF should be included during registration: if Accused Products are roaming, based on the roaming agreement; based on local configuration; based on registered communication service of the Accused Products; based on the access type. <i>Id.</i> at 721. Upon session initiation, the Accused Products or the SCC AS establishes the Service Control Signaling Path for communication of service control signaling via the PS network using the Gm reference point. VASU 005865-953 at 80. The Accused Products established the calls via a wireless communication link with PLMN through gateways and interfaces supported by Evolved Packet Core (“EPC”) functions. EPC can be accessed via a trusted or untrusted network. There are differences when accessing these types of networks. However, the differences are not relevant to whether the Accused Products establish a communication link with an end destination device. The Supported EPC Functions <u>Trusted WLAN Access Network (“TWAN”)</u>: For access to PLMN’s EPC via a trusted non-3GPP access network such as trusted TWLAN, a connection shall be established between the Accused Products and TWAN using specific signal procedures. VASU 008198-326 at 230. Access authentication signaling for access to the EPC shall be executed between the Accused Products and the AAA server, which is an interface server, to ensure mutual authentication of the user and the EPC. <i>Id.</i> at 230. <u>Evolved Package Data Gateway (“ePDG”)</u>: ePDG is the local mobility anchor within untrusted non-3GPP access. VASU 006232-544 at 262. The PLMNs included in the ePDG information are the PLMNs that have roaming agreements with HPLMN. VASU 006232-544 at 269. Through a network interface (Swn interface), the ePDG connects with an untrusted non-3GPP access. VASU 005019-113 at 92. The ePDG connects with the Accused Products (through the SWu interface) to establish data tunnels and user data packet transmission within the tunnels. <i>Id.</i> at 93. <u>Call Session Control Function (“CSCF”)</u>: CSCF can act as Proxy CSCF (“P-CSCF”), serving CSCF (“S-CSCF”), emergency CSCF (“E-CSCF”), or Interrogating CSCF (“I-CSCF”). VASU 005019-113 at 56. The P-CSCF is the first contact point for the Accused Products within the International Mobile Subscriber Identity (“IMSI”); the S-CSCF actually handles the session states in the network; the E-CSCF handles
--	---

emergency sessions such as routing an emergency requests to the correct emergency center; the I-CSCF is the contact point within an operator’s network for all IMS connections destined to a subscriber of that network operator or roaming subscriber located within the network operator’s service area. *Id.*

Home Subscriber Server (“HSS”): The HSS supports the authentication procedures to access CS domain, PS domain, and system services by storing the generated data for authentication, integrity, and ciphering and by providing these data to the appropriate entities including AAA server or CSCF. VASU 005019-113 at 41. The diagram below illustrates . . .

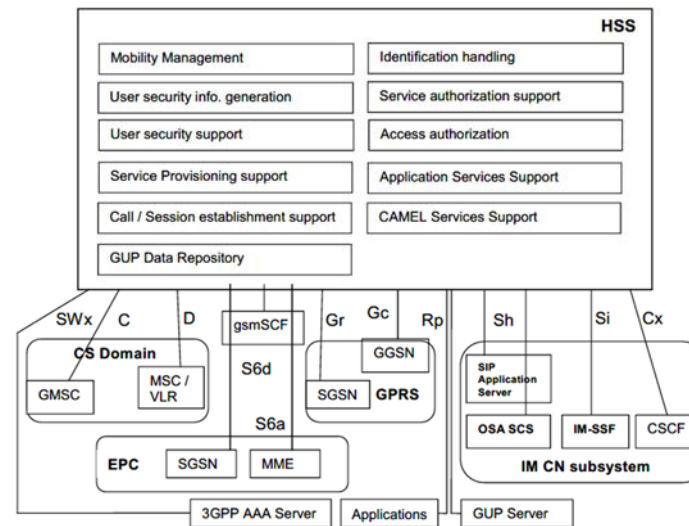


Figure 0.b: HSS logical functions

VASU 005019-113 at 40.

Authentication, Authorization, and Accounting (“AAA”): The Accused Products is authenticated and authorized through AAA to roam between networks. AAA server (interface server) is located at HPLMN and provides support for non-3GPP access users with services like authentication, authorization, and location management services to access evolved packet systems (“EPS”) in mobile networks. VASU 005019-113 at 49. It interacts with HSS to maintain consistent information to support service continuity

between 3GPP (mobile networks) and non-3GPP (Wi-Fi) networks. *Id.* It contains user information to gain access to non-3GPP access. *Id.* Non-3GPP access authentication defines the process to permit or deny a subscriber to attach to and use the sources of a non-3GPP IP access interworked with the EPC network. VASU 006232-544 at 307. Non-3GPP access authentication signaling is executed between the Accused Products and the AAA server/HSS (interface server). *Id.* During the authentication of the Accused Products for accessing the EPC via ePDG, ePDG shall initiate EAP-AKA based authentication between the Accused Products and the AAA server. VASU 006232-544 at 279.

After initiating the call, the Accused Products may roam between Wi-Fi networks and PLMN networks under multiple scenarios.

Exemplary Scenario 1: Wi-Fi to Wi-Fi

- (5) The Accused Products initiate a call within a first Wi-Fi network through VoIP or VoWiFi and roam from a first Wi-Fi network to a second Wi-Fi network.

The Accused Products may go out of range of access points and shift network association to another access point without losing connection. VASU 025133-44 at 134. Weak signals can trigger roaming on the Accused Products. *Id.* The Accused Products support 802.11k and 802.11v standards to reduce the length of time of lost connectivity during basic service set (“BSS”) transition. *Id.* at 138-42.

Exemplary Scenario 2: Wi-Fi to Home PLMN

- (9) The Accused Products initiate a call over a first Wi-Fi network through VoIP or VoWiFi and roam from the first Wi-Fi network to the coverage area of the home PLMN (“HPLMN”) of the Accused Products.
- (10) The Accused Products initiate a call within a first Wi-Fi network, but set up a backend of the call over PLMN network and roam from the first Wi-Fi network to the coverage area of the HPLMN of the Accused Products.

In a non-roaming scenario when the Accused Products establish the communication link with a home network, the trust relationship of Wi-Fi (non-3GPP IP wireless network) is determined by the HPLMN

operators. VASU 008198-326 at 227. The trust relationship is indicated to the Accused Products via either pre-configured policies in the Accused Products by the home PLMN operator or dynamic indication during 3GPP-based access authentication. *Id.*

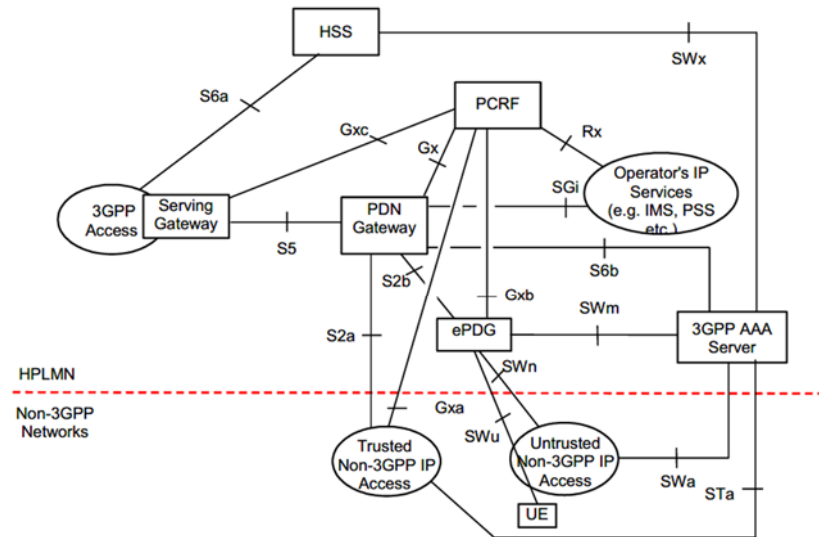
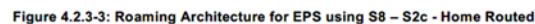


Figure 4.2.2-1: Non-Roaming Architecture within EPS using S5, S2a, S2b

VASU 006232-544 at 254 (non-roaming architecture showing trusted or untrusted non-3PPP wireless network connecting to AAA server in PLMN using the SWa or STa interface to access the trusted or untrusted 3GPP networks).

	Authorization of EPC access shall be performed by the AAA server upon successful user authentication. <i>Id.</i> <u><i>Exemplary Scenario 3: Wi-Fi to Visitor PLMN</i></u> (9) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over VoIP or VoWiFi, and roam from the first Wi-Fi network to the coverage area of a visitor PLMN (“VPLMN”) of the Accused Products. (10) The Accused Products initiate a call within a first Wi-Fi network that resides outside the coverage area of the HPLMN of the Accused Products, but set up a back end of the call over a HPLMN, and roam from the first Wi-Fi network to the coverage area of a VPLMN. In roaming scenario when the Accused Products establish the communication link with a visitor network, the HSS or AAA server (interface server) in HPLMN makes the final decision if a non-3GPP wireless network is trusted or untrusted. VASU 006232-544 at 260. The HSS/AAA server (interface server) may take the visitor PLMN (“VPLMN”) policy and capability returned from the AAA proxy or roaming agreement into account. <i>Id.</i> at 260.
--	--



The session origination procedures specify the signaling path between the Accused Products initiate a session setup attempt and the S-CSCF assigned to perform the session origination service. VASU 005263-653 at 380. The Accused Products initiate a session setup attempt and assigned a S-CSCF to perform the session origination service. VASU 005263-653 at 380. The signaling path between the Accused Products and S-CSCF is determined at the time of the Accused Products registration. *Id.* The S-CSCF to application server interface is used to provide services in the application server in the HPLMN or in a trusted external network (e.g., third-party or VPLMN). VASU 005019-113 at 58.

166

allocates an S-CSCF in the HPLMN. *Id.* at 383. When registration is completed, P-CSCF knows the name/address of S-CSCF. *Id.*

The Accused Products monitor the context (signal strength by Received Signal Strength Indicator, “RSSI” or user preference) of the first communication link with the wireless network. This is performed through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature in “Intelligent Wi-Fi Settings” feature in A Series, S Series, X Cover, and Z Series. VASU 010302-454 at 398 (A13 5G); VASU 010601-745 at 691 (A14 5G); VASU 011048-196 at 143 (A23 5G/A23 5G UW); VASU 011532-691 at 633 (A53 5G/A53 5G UW); VASU 011692-852 at 792 (A54 5G); VASU 018745-906 at 848 (S20 FE 5G); VASU 019244-407 at 351 (S21 5G/ S21 Ultra 5G/ S21+ 5G); VASU 019782-949 at 895 (S22/S22+/S22 Ultra); VASU 019950-20128 at 1070 (S23/S23+/S23 Ultra); VASU 023406-563 at 508 (XCover Pro); VASU 023564-725 at 672 (Z Flip 5G); VASU 023894-4071 at 1014 (Z Fold3 5G/Z Flip3 5G); VASU 024756-929 at 877 (Z Flip4); VASU 024408-577 at 520 (Z Fold2 5G).

“Switch to Mobile Data” monitors network context changes to “automatically switch[] networks based on both network quality and user preferences.” VASU 025185-91 at 187. The connection manager will not be active until it accumulates enough data to determine user preference. *Id.*



Id. at 187 (determining user preference).

Through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature within “Intelligent Wi-Fi settings” on the Accused Products (shown below), the Accused Products can seamlessly switch to mobile data if there are signal strength issues and “whenever the Wi-Fi connection is unstable.” VASU 019950-20128 at 1070. When the Wi-Fi signal strength is strong, it switches “back to Wi-Fi.” *Id.*

	Intelligent Wi-Fi settings You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider. 1. From Settings, tap  Connections > Wi-Fi, and then tap  to turn on Wi-Fi. 2. Tap  More options > Intelligent Wi-Fi for the following options: • Switch to mobile data: When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi. • Switch to better Wi-Fi networks: Automatically switch to faster or more stable Wi-Fi networks. • Turn Wi-Fi on/off automatically: Turn on Wi-Fi in frequently-used locations. • Show network quality info: Display network information (such as speed and stability) in the list of available Wi-Fi networks. • Prioritize real-time data: Give network priority to games, video calls, and other tasks that are sensitive to lag. • Detect suspicious networks: Get notified when suspicious activity is detected on the current Wi-Fi network. • Wi-Fi power saving mode: Enable Wi-Fi traffic analysis to reduce battery usage. • Auto Hotspot connection: Automatically connect to a Wi-Fi hotspot when detected. • Intelligent Wi-Fi: View the Intelligent Wi-Fi version. VASU 019950-20128 at 1070 (intelligent Wi-Fi settings in an exemplary S23+ phone). Similarly, the Accused Products include a “Switch to Mobile Data” feature under “Wi-Fi Preferences.” VASU 012187-372 at 300 (Amp Prime 3); VASU 012624-795 at 737 (J2); VASU 013258-446 at 375 (J7); VASU 013447-617 at 557 (J7 V); VASU 012938-3112 at 1050 (J7 Prime); VASU 017373-567 at 490 (S7); VASU 016965-7166 at 1090 (S7 Active); VASU 017167-372 at 294 (S7 Edge); VASU 013837-4053 at 986 (Note 9).
--	--

	Wi-Fi preferences Customize advanced Wi-Fi services. 1. From  Settings, tap Connections > Wi-Fi, and then tap On/Off to turn on Wi-Fi. 2. Tap  More options > Advanced. To view all network settings, tap View more. • Switch to mobile data: Connect automatically to a mobile network connection when the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi. • Turn on Wi-Fi automatically: Enable Wi-Fi in frequently used locations. • Wi-Fi power saving mode: Reduce battery usage by analyzing Wi-Fi traffic patterns. • Wi-Fi notifications: Receive notifications when open networks in range are detected. • Show Wi-Fi pop-up: When opening apps, indicate when Wi-Fi is available. VASU 013837-4053 at 3977. Moreover, the Accused Products include “Switch to Mobile Data” product feature in “Advanced Wi-Fi Settings” to switch between mobile and Wi-Fi networks. VASU 009579-721 at 669 (A02s); VASU 009855-10011 at 116 (A10e); VASU 010011-157 at 104 (A11); VASU 010158-301 at 250 (A12); VASU 010455-600 at 546 (A13); VASU 010746-901 at 851 (A20); VASU 010902-1047 at 996 (A21); A51_User_Manual.pdf at 116 (A51); VASU 011197-367 at 315 (A51 5G/A51 5G UW); VASU 011368-531 at 477 (A52 5G); VASU 011853-2015 at 958 (A71 5G); VASU 012016-2186 at 2134 (A71 5G UW); VASU 015086-267 at 209 (Note 10+); VASU 014054-245 at 191 (Note 20 5G/Note 20 Ultra 5G); VASU 017730-891 at 838 (S8), VASU 017568-729 at 676 (S8 Active); VASU 017892-8059 at 8006 (S8+); VASU 018060-236 at 183 (S9/S9+); VASU 018399-571 at 511 (S10/S10e/S10+); VASU 018237-398 at 345 (S10 Lite); VASU 018907-9076 (S20 5G/S20 Ultra 5G/S20+ 5G); VASU 024244-407 at 348 (Z Fold);
--	--

VASU 023090-256 at 199 (XCover 6 Pro); VASU 023257-405 at 358 (XCover FieldPro); VASU 012482-623 at 570 (J2 Pure); VASU 012796-937 at 890 (J3); VASU 013113-257 at 209 (J7 Star).

Advanced Wi-Fi settings

You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by carrier.

1. From Settings, tap  **Connections** > **Wi-Fi**, and then tap  to turn on Wi-Fi.
2. Tap  **More options** > **Advanced**.
 - **Sync with Samsung Cloud/account:** Sync Wi-Fi profiles with your Samsung account.
 - **Switch to mobile data:** When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi.
 - **Turn on Wi-Fi automatically:** Turn on Wi-Fi in frequently-used locations.
 - **Detect suspicious networks:** Get notified when suspicious activity is detected on the current Wi-Fi network.

VASU 010455-600 at 546.

The Accused Products include “Intelligent Wi-Fi” feature in “Wi-Fi Settings,” which switches between mobile and Wi-Fi networks depending on the signal strength. VASU 020129-301 at 243 (S24/S24+/S24 Ultra); VASU 024756-929 at 874 (Z Fold4/Z Flip4).

	Wi-Fi settings You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider. 1. From Settings, tap  Connections > Wi-Fi, and then tap  to turn on Wi-Fi. 2. Tap  More options for the following options: • Wi-Fi Direct: Share data directly between devices over Wi-Fi. • Intelligent Wi-Fi: Configure Wi-Fi switching and detection features. • Advanced settings: Configure Wi-Fi connections and Hotspot settings. • Contact us: Contact Samsung support through Samsung Members. VASU 024756-929 at 874 (Z Fold4/Z Flip4). The Accused Products measure signal strength of Wi-Fi networks by Received Signal Strength Indicator (“RSSI”), and its unit of measurement is dBm. The table below provides a point of reference for interpreting the RSSI value.
--	--

Signal Strength	TL;DR		Required for
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWi-Fi, streaming video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

VASU 025540-45 at 43-44.

The screenshot below illustrate that the Accused Products continuously monitor the signal strength.



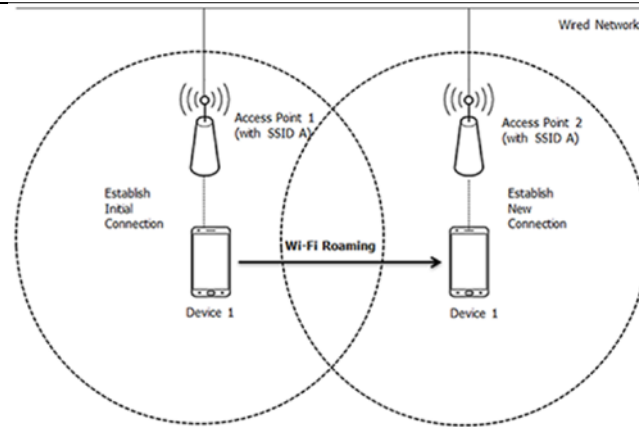
VASU 031389-98 at 96.

The Accused Products include “Auto Wi-Fi,” which turns Wi-Fi on and off depending on locations. VASU 025185-91 at 88. It turns Wi-Fi on when the favorite network is available by user preference and turns off Wi-Fi when this network is unavailable. *Id.* Auto Wi-Fi is triggered based on user’s location by geofencing (a virtual geological fence based on cellular stations). *Id.*

Furthermore, The Wi-Fi network selection functions in the Accused Products continuously

	evaluate the quality of the connected network and assess the quality of available networks. VASU 025102-18 at 02. The Accused Products scan the available networks depending whether the screen of the Accused Products is on or off. <i>Id.</i> If the screen of the Accused Products is on and the Accused Products is connected, the Wi-Fi framework of the Accused Products evaluates whether the current network is good enough to skip network selection when all the following conditions are met: (1) the RSSI is above the required RSSI threshold or sufficient traffic is flowing over the connection; (2) the network is evaluated, or user approved for use without internet access; and (3) the network is unmetered. <i>Id.</i> at 03. If the connection isn't good enough, the connectivity subsystem triggers a scan to detect available networks. <i>Id.</i> Moreover, if the screen is on and the Accused Products are disconnected, the Android connectivity system issues periodic scans (activation of a timer) following an exponential back off schedule (increasing the waiting time between retries). <i>Id.</i> at 02. The module evaluates scan results received by evaluating if the signal level is below a predefined threshold and tries to select the best network to connect to. <i>Id.</i> When the Accused Products' screen is off, the network selection process might occur if scans are initiated by other services such as location services. <i>Id.</i> at 06. When the Accused Products are active in an IMS session, the session transfer procedures provide session continuity between wireless networks using signal strength information. VASU 005654-93 at 62. The Accused Products initiate session transfer procedure based on trigger criteria, including the current operator policy, user preferences, and wireless network conditions for conducting a session continuity operation to the SCC AS (interface server). VASU 005654-93 at 64. A third-party call control function (call function from the Accused Products) is employed for subscriber IMS sessions at the SCC AS upon session establishment for enablement of Session Transfer. <i>Id.</i> <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
--	--

41[b]. when a network is detected as available with a second wireless communication link with a context preferable to the first wireless communication link, notifying an interface and establishing the second communication link between the interface and an end destination device without disrupting the first communication link; and	As described in Element 45[a], the Accused Products monitor the network context (signal strength via RSSI or user preferences) through “Switch to mobile data” or “Switch to better Wi-Fi networks” product feature and other communication modules such as Wi-Fi network selection functions. VASU 025102-18 at 02. When the Accused Products may prefer a second context (signal strength by RSSI in the second network or by user preference) and trigger session transfer when triggering criteria is met (for example, the signal strength is below certain threshold). SCC AS provides IMS-based mechanism for enabling session continuity. It executes the transfer of the IMS session between multiple wireless networks upon session establishment. VASU 005654-93 at 64. The Android Wi-Fi framework or firmware of the Accused Products periodically monitors the signal strength (or RSSI) of the first communication link to decide if the RSSI is below a certain threshold. VASU 025102-18 at 05. When the screen of the Accused Products is on, and the Wi-Fi service may poll RSSI and link-layer stats every 3 seconds or by other configuration (config_wifiPollRssiIntervalMilliseconds or config_wifiAdjustPollRssiIntervalEnabled for dynamic adjustment based on the device mobility state and RSSI). <i>Id.</i> The polling interval is extended to 6 seconds when the device is stationary and RSSI is above -68 dBm (configured by the config_wifiClientRssiMonitorThresholdDbm and config_wifiClientRssiMonitorHysteresisDb), which is the pre-defined threshold value. <i>Id.</i> The polling interval is reduced back to 3 seconds (the second time window configured by the config_wifiPollRssiIntervalMilliseconds) when the device is non-stationary or RSSI is below -73 dBm, which is another pre-defined threshold value. <i>Id.</i> Once connected, the Wi-Fi service calculate “a connected score” based on the RSSI and determine whether to connect to a Wi-Fi network or another network type, such as a mobile network. <i>Id.</i> at 04-05. the Wi-Fi service may pass the score to the connectivity service, which uses the score to determine whether to connect to a Wi-Fi network or to a mobile network. <i>Id.</i> at 06.
---	---



VASU 025133-44 at 34 (roaming from one Wi-Fi to another Wi-Fi access point is triggered due to weak signal).

“Switch to Mobile Data” determines the context changes to “automatically switch[] networks based on both network quality and user preferences.” VASU 025185-91 at 187. The connection manager will not be active until it accumulates enough data to determine user preference. *Id.*



Id. at 187 (determining user preference).

Through “Switch to mobile data” or “Switch to better Wi-Fi networks” product features in “Intelligent Wi-Fi” on the Accused Products (shown below), the Accused Products can seamlessly switch to mobile data if there are signal strength issues and “whenever the Wi-Fi connection is unstable.” VASU 019950-20128 at 1070. When the Wi-Fi signal strength is strong, it switches “back to Wi-Fi.” *Id.*

Intelligent Wi-Fi settings

You can configure connections to various types of Wi-Fi networks and hotspots, manage saved networks and look up your device's network addresses. Options may vary by service provider.

1. From Settings, tap  **Connections > Wi-Fi**, and then tap  to turn on Wi-Fi.
2. Tap  **More options > Intelligent Wi-Fi** for the following options:
 - **Switch to mobile data:** When enabled, your device will switch to mobile data whenever the Wi-Fi connection is unstable. When the Wi-Fi signal is strong, it switches back to Wi-Fi.
 - **Switch to better Wi-Fi networks:** Automatically switch to faster or more stable Wi-Fi networks.
 - **Turn Wi-Fi on/off automatically:** Turn on Wi-Fi in frequently-used locations.
 - **Show network quality info:** Display network information (such as speed and stability) in the list of available Wi-Fi networks.
 - **Prioritize real-time data:** Give network priority to games, video calls, and other tasks that are sensitive to lag.
 - **Detect suspicious networks:** Get notified when suspicious activity is detected on the current Wi-Fi network.
 - **Wi-Fi power saving mode:** Enable Wi-Fi traffic analysis to reduce battery usage.
 - **Auto Hotspot connection:** Automatically connect to a Wi-Fi hotspot when detected.
 - **Intelligent Wi-Fi:** View the Intelligent Wi-Fi version.

VASU 019950-20128 at 1070 (intelligent Wi-Fi settings in an exemplary S23+ phone). The Accused Products can also switch to better Wi-Fi networks by “automatically switch[ing] to faster or more stable Wi-Fi networks.” VASU 019950-20128 at 1070.

Session Continuity between Mobile Networks

When the signal strength drops below a predetermined threshold, the Accused Products may also use locally stored data for selecting a second EPC network available for connectivity via the currently selected non-3GPP wireless network to establish a second communication link. VASU 008198-326 at 222. UE shall select a PLMN according to the PLMN selection procedure of the selected non-3GPP wireless network. *Id.*

Signaling and bearer resources are allocated in the transferring-in wireless network and the user's sessions are transferred from the transferring-out wireless network. VASU 005654-93 at 669. The SCC AS executes access transfer procedures and resources in the transferring-out wireless network is released. *Id.*

The Accused Products establish the second communication link (the second call session with the second network, transferred-in network) with the transfer-in network without disrupting the first communication link in the transfer-out network. IMS sessions from and to the Accused Products are anchored at the SCC AS in the home IMS based on initial filtering criteria (“iFC”) to provide service continuity for the user during the transition between two wireless networks. VASU 005654-93 at 62.

For single radio voice call continuity (“SRVCC”), voice call continuity between PLMN/VPLMN over PS and CS are anchored when the UE is capable of transmitting or receiving only one of the access networks at a given time. VASU 005195-214 at 200.

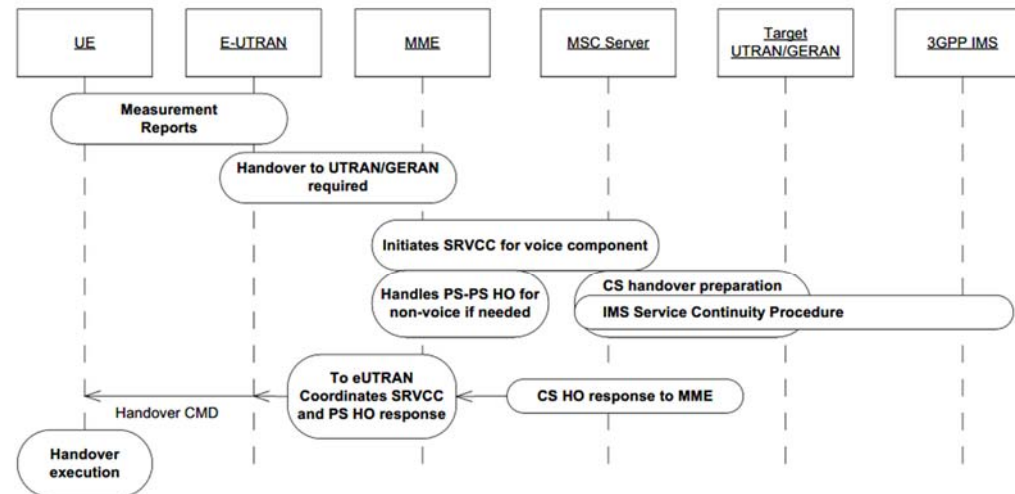


Figure 4.2.2-1: Overall high level concepts for SRVCC from E-UTRAN to UTRAN/GERAN

VASU 005195-214 at 202 (how SRVCC works in E-UTRAN, 4G to UTRAN/GERN, 3G/2G).

A third-party call control function (functions provided by the Accused Products) is employed at the SCC AS to facilitate inter-access network mobility through the user of access transfer between the two wireless networks. *Id.*

PS-CS transfer

IMS session established in CS or PS wireless networks are anchored at the SCC AS. VASU 005654-93 at 662. IMS sessions using CS bearer are established at session setup or upon access transfer. *Id.*

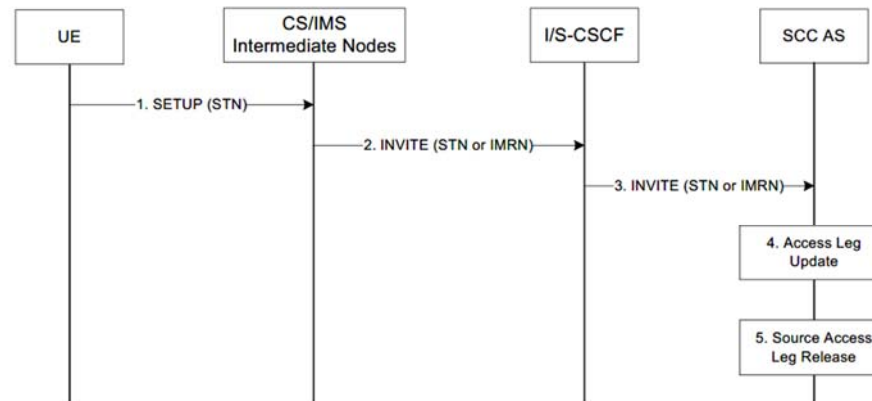


Figure 6.3.2.1.1-1: PS – CS Access Transfer: PS to CS

VASU 005654-93 at 72 (user is active in an IMS originating or terminating session using PS media at the time of transfer).

CS-PS Transfer

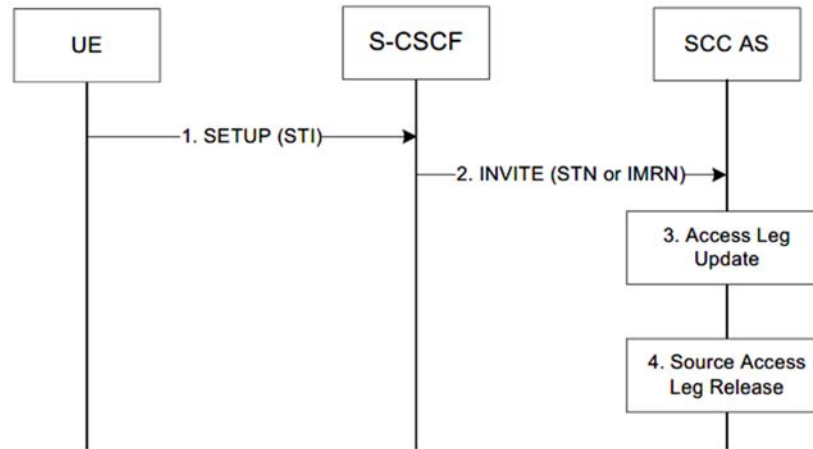


Figure 6.3.2.1.2-1: PS – CS Access Transfer: CS to PS

VASU 005654-93 at 73 (the user is active in the IMS originating or terminating session using CS at the time of transfer).

PS-PS Transfer

US is attached to one IP connectivity access network (“IP-CAN”), and it registers to the S-CSCF. VASU 005654-93 at 75. UE-1 and UE-2 establish an active multimedia session via this IP-CAN. *Id.* After changing to a new IP-CAN, obtaining new signaling and media addresses, and completing the Access Transfer procedures, UE-1 continues the session with UE-2 on the new IP-CAN. *Id.*

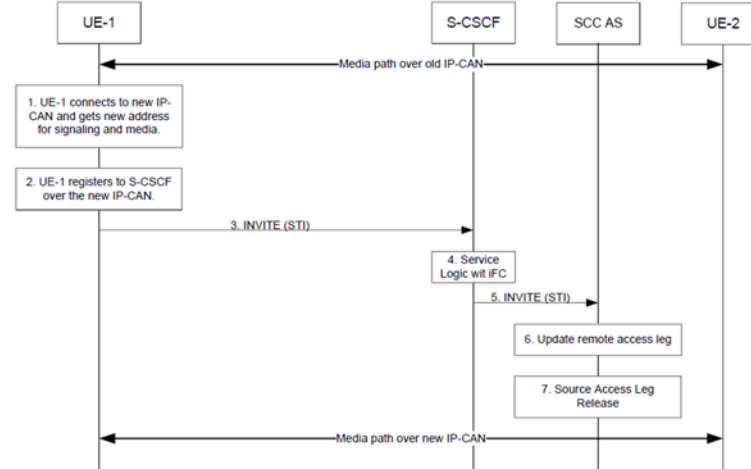


Figure 6.3.2.2.1-1: Information flow for PS-PS Access Transfer

Id.

Session Continuity between Wi-Fi and Mobile Networks

Upon the Accused Products' request, the access network discovery and selection function ("ANDSF") in either HPLMN or VPLMN may provide a list of wireless access networks available in the vicinity of the UE for all the access technology types requested by the UE to establish a second communication link through Wi-Fi. VASU 006232-544 at 293. An ANDSF element located in the HPLMN of a UE is referred to as Home-ANDSF ("H-ANDSF") and an ANDSF element located in the visited PLMN of a UE is referred to as the visited-ANDSF (V-ANDSF) for this UE. VASU 006232-544 at 291. The H-ANDSF in the subscriber's HPLMN may interact with HSS user profile information. *Id.* at 61.

The ANDSF provides information for access networks that are available to the UE including:

- the access technology type (e.g. WLAN, WiMAX).
- the radio access network identifier (e.g. the SSID of a WLAN).
- other technology specific information, e.g. one or more carrier frequencies.
- validity conditions, i.e. conditions indicating when the provided access network discovery information is valid (such conditions may include e.g. a location).

	VASU 006232-544 at 293. ANDSF contains data management and control functionality necessary to provide network discovery and selection assistance data per operator’s policy. VASU 006232-544 at 292. ANDSF may provide other information, including access network discovery information, WLAN selection information, and ePDG configuration information. VASU 008198-326 at 252. If the UE is roaming in a VPLMN, the UE may receive Inter-system mobility policies or access network discovery information from H-ANDSF or V-ANDSF or both. <i>Id.</i> Moreover, access network selection and traffic steering between 3GPP access and WLAN is supported using ANDSF and is also supported using radio access network rule procedure without ANDSF. VASU 006232-544 at 290. The home network preference may be provided by the Accused Products’ HPLMN and include information that assists the UE to select a WLAN network and to select a PLMN for 3GPP-based authentication over WLAN. VASU 006232-544 at 297. Similarly, a visited network preference may be provided by the VPLMN, but UE shall ignore the preference if provided a HPLMN preference. <i>Id.</i> <u>DOE</u> To the extent that Defendants contend that the Accused Products do not literally satisfy this limitation, Defendants infringe under the doctrine of equivalents because they perform substantially the same function, in substantially the same way, to achieve substantially the same result. The Accused Products perform substantially the same function because they monitor the second context (signal strength) of the first communication link through “Intelligent Wi-Fi” product feature and switch on-going call or data stream sessions with the end user device to a preferable second communication link through “Switch to Mobile Data” product functions and notifying the interface server without interrupting the call or data streaming sessions. <i>See, e.g.</i>, VASU 019244-407 at 351; VASU 013837-4053 at 977; VASU 025185-91 at 187. Moreover, the Accused Products’ network switching functions act as an interface server connecting with the Wi-Fi or the mobile network. The Accused Products function in substantially the same way because the “Intelligent Wi-Fi” product feature switch the first communication link to a preferable second communication link when the signal strength (context) of the Wi-Fi network is
--	--

	below a pre-defined threshold. <i>See, e.g.</i>, VASU 025185-91 at 187; VASU 025102-18 at 02. The Accused products switch to a second communication link without interrupting the current call or data stream sessions by holding the call or data streaming session after notifying the interface server. <i>See, e.g.</i> VASU 025133-44 at 34; VASU 005654-93 at 69. The Accused Products achieve substantially the same result because the Accused Products switch an on-going call or data streaming sessions to a preferable second communication link seamlessly when the signal strength (context) of the first communication link drops below a threshold value. The Accused Products accomplish this result by notifying an interface server through “Intelligent Wi-Fi” product feature to hold the current session while switching to the second communication link. <i>See, e.g.</i>, VASU 006232-544 at 290; VASU 025102-18 at 1; VASU 005654-93 at 69. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
41[c]. re-directing the second communication link from the interface to a mobile communication device, thereby establishing the second wireless communication link between the mobile communication device and a second wireless network,	As described in Element 39[e], the Accused Products re-direct the second communication link (through switching access leg for the communication) from the SCC AS (interface server) to the Accused Products. A second wireless communication link is established between the Accused Products and the second wireless network. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element’s functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.

41[d]. wherein upon activation of a timer, the interface causes a communication module to change state from a sleep mode to a stand-by mode, and the interface causes the communication module to change state from the stand-by mode to an active mode before a communication is switched to the communication module.	As described in Element 12[d], the timer (pre-define time window) is activated and the interface on the server (SCC AS or server for Wi-Fi network/Wi-Fi firmware) causes the second communication module to change state from the stand-by to an active mode before the communication (video/voice/data) is switched to the Wi-Fi communication module. The Accused Products also include a first and a second communication module. Depending on the switching of network (Wi-Fi to Wi-Fi, Wi-Fi to mobile, or mobile to Wi-Fi), VoIP user agent, VoWiFi call function, mobile call function can be either the first or the second communication module. The Wi-Fi network selection functions can be either the first communication module or the second communication module, depending on the network switching operation. If the communication network is switch to mobile network, the Wi-Fi network selection functions or the Wi-Fi firmware is the first communication module; if the communication network is switched to Wi-Fi network, the Wi-Fi network selection functions or the Wi-Fi firmware is the second communication module. <u>SOURCE CODE SUPPLEMENTATION</u> As described above, this element's functions may be performed through software in the Accused Products. As such, Vasu reserves the right to supplement its response once Defendants make source code for the Accused Products available for inspection.
---	--