IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

DYNAMIC MESH NETWORKS, INC. DBA MESHDYNAMICS, Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	Case No. 2:25-cv-00783-JRG (Member Case) Jury Trial Demanded

MESHDYNAMICS'S LOCAL PATENT RULES 3-1 AND 3-2 INITIAL DISCLOSURES

MeshDynamics Exhibit 2014
Cisco Systems, Inc. v. Dynamic Mesh Networks, Inc. D/B/A MeshDynamics
IPR2025-01569

Pursuant to Local Patent Rules (L.P.R.) 3-1 and 3-2 of the United States District Court for the Eastern District of Texas, Plaintiff Dynamic Mesh Networks, Inc. ("MeshDynamics" or "Plaintiff") submits the following initial patent disclosures with respect to U.S. Patent Nos. 8,477,762 ("the '762 Patent), 8,514,852 ("the '852 Patent") and 9,049,000 ("the '000 Patent") (collectively, the "MeshDynamics Asserted Patents").

I. INTRODUCTION

This case is in the early stages and discovery and investigation in connection with this lawsuit has not begun. These contentions are thus based on information reasonably available to MeshDynamics to-date. These contentions apply the plain and ordinary meaning to the claim terms and will be supplemented should the Court issue a *Markman* order construing any term of the MeshDynamics Asserted Patents. MeshDynamics has made reasonable assumptions, to the extent necessary and appropriate, with respect to the meaning of patent claim terms for the purpose of preparing these contentions. MeshDynamics reserves the right to rely upon different meanings in the conduct of this litigation, to assert different meanings as appropriate, and revise the factual content of these contentions in light of any such different meanings.

MeshDynamics's contentions are subject to revision, modification and/or supplementation as MeshDynamics's investigation and discovery in the case progresses. Many claim elements are software limitations (as noted in the attached claim charts), and Cisco Systems, Inc. ("Cisco" or "Defendant") has yet to provide access to the relevant source code in this case. Pursuant to Judge Gilstrap's discovery order paragraph 3(a), MeshDynamics will supplement these contentions following the production and review of the relevant source code. MeshDynamics further reserves the right to revise, modify and/or supplement these contentions in response to any invalidity contentions. MeshDynamics further reserves the right to revise, modify, amend and/or supplement these contentions in accordance with the Local Patent Rules, any other applicable Rules, or by

order of this Court.

In addition, MeshDynamics reserves its right to amend, alter, or supplement these contentions at any time and/or as otherwise authorized or permitted by the aforesaid Rules, based on the following:

- Any further investigation;
- Any fact or expert discovery materials, including, but not limited to, documents, source code, reports, guides, communications and deposition testimony, which have not yet been obtained, produced or provided to MeshDynamics;
- Evaluation of the scope and content of the prior art;
- Clarification of Cisco's non-infringement positions;
- Any claim construction order;
- Any claim contentions that Cisco may assert that are different from any assumptions MeshDynamics has made in preparing these contentions;
- Any claim constructions or additional or different allegations that Cisco may assert at a later date; or
- Any other grounds otherwise provided under the Local Patent Rules, any other applicable Rules, upon leave of the Court, and/or any other reason requiring same.

These contentions may be asserted in the alternative and do not constitute any concession by MeshDynamics for purposes of claim construction, non-infringement, or invalidity. *See* Fed. R. Civ. P. 8(d).

Furthermore, these contentions are provided without prejudice to the rights of MeshDynamics to introduce at trial any subsequently-discovered evidence or expert opinions and to produce and introduce at trial all evidence, whenever discovered, relating to the proof of subsequently-discovered facts. Moreover, facts, documents and things now known may be imperfectly understood and, accordingly, such facts, documents and things may not be included in these contentions. In particular, Cisco's publicly available information is unclear and ambiguous as to the operation of its products. MeshDynamics reserves its right to refer to, conduct discovery with reference to, or offer into evidence at the time of trial, any and all facts, expert opinion testimony, documents and things notwithstanding the written statements herein and subject to the

Rules of this Court. MeshDynamics further reserves its right to refer to, conduct discovery with reference to, or offer into evidence at the time of trial, any and all facts, documents and things that are not currently recalled but might be recalled at some time in the future.

MeshDynamics provides these contentions without waiving any claim of attorney-client privilege, attorney work-product immunity, or any other applicable privilege or immunity. To the extent that MeshDynamics inadvertently discloses information that may be protected from discovery under the attorney-client privilege, the attorney work-product immunity, or any other applicable privilege or immunity, such inadvertent disclosure does not constitute a waiver of any such privilege or immunity.

The information set forth below is provided without waiver of (1) the right to object to the use of any statement for any purpose, in this action or in any other action, on the grounds of privilege, relevance, materiality or any other appropriate grounds; (2) the right to object to any request involving or relating to the subject matter of the statements herein; or (3) the right to revise, correct, supplement or clarify any of the statements provided below at any time.

Subject to the foregoing, MeshDynamics hereby submits the following initial disclosures in accordance with L.P.R. 3-1 and L.P.R. 3-2.

II. INFRINGEMENT CONTENTIONS

Pursuant to L.P.R. 3-1, and subject to the reservation of rights outlined above, MeshDynamics provides below, and in the charts attached as Exhibits 1-6, MeshDynamics's infringement contentions.

A. Identification of the Asserted Claims

Pursuant to L.P.R. 3-1(a), the asserted claims of the MeshDynamics Asserted Patents include those claims identified in the attached claim charts. MeshDynamics identified these asserted claims based on its current and preliminary understanding and reserves the right to

supplement its identification of infringed claims as discovery proceeds, including identifying additional claims following review of Cisco's proprietary information.

MeshDynamics accuses Cisco of infringing under 35 U.S.C. § 271(a), 35 U.S.C. § 271(b), and 35 U.S.C. § 271(c) each of the following claims of the MeshDynamics Asserted Patents (hereinafter referred to as the "Asserted Claims"):

- Claims 1-4, 7-9, 10, 12-13, 15-17 of the '762 Patent
- Claims 1, 5, 7 of the '852 Patent
- Claims 1, 6, 7 of the '000 Patent

Cisco has infringed and continues to infringe (literally and/or under the doctrine of equivalents), directly and/or through subsidiaries, agents, representatives, or intermediaries, one or more of the Asserted Claims of the MeshDynamics Asserted Patents by making, using, testing, supplying, causing to be supplied, importing, selling, and/or offering for sale in the United States the Accused Instrumentalities ("Cisco Accused Products") as detailed in the attached claim charts. Cisco has indirectly infringed and continues to indirectly infringe (literally and/or under the doctrine of equivalents) one or more of the Asserted Claims (which were all known to it well before this litigation was commenced) by making, using, offering for sale, selling, and/or importing in or into the United States the Cisco Accused Products, and by actively and intentionally inducing its customers and end users to infringe by making, using, offering for sale, selling, and/or importing the Cisco Accused Products as detailed in the attached claim charts. Cisco has also indirectly infringed and continues to indirectly infringe by offering for sale, selling, and/or importing in or into the United States components that are material parts of the Accused Instrumentalities and are not staple articles of commerce, with knowledge of their infringing use, and without substantial non-infringing uses as detailed in the attached claim charts. *See* Exhibits

1-6. MeshDynamics incorporates fully herein the factual and infringement allegations set forth in its Complaint (*see* Dkt. 1).

B. Identification of the Accused Instrumentalities

Pursuant to L.P.R. 3-1(b), the Accused Instrumentalities ("Cisco Accused Products") include Cisco Webex and Catalyst SD-WAN and related software and hardware made, used, offered for sale, sold and/or imported in or into the United States. Attached as Exhibit 7 is the list of Accused Instrumentalities of which MeshDynamics is currently aware. MeshDynamics asserts that any other Cisco product(s) that operates in the same or similar manner as those specifically identified in Exhibit 7 are also Accused Instrumentalities. MeshDynamics reserves all rights to revise, amend, and/or supplement this list as discovery and its investigation in this case proceeds. MeshDynamics asserts that all Accused Instrumentalities identified on Exhibit 7, and any other Cisco product(s) that operates in the same or similar matter, infringe the Asserted Claims of each MeshDynamics Asserted Patent as identified in Section II.A *supra*. *See* Exhibits 1-6.

Cisco recently announced the availability of "Webex Meetings Survivability."[1] Cisco is marketing it as a solution for outages that is an "[i]solated, secure deployment model in customer's site/ datacenter."[2] Additional information regarding this newly-announced feature is not available publicly. On information and belief, this Webex feature is similar to and infringes for at least the same reasons as detailed in Exhibits 1 and 2, showing infringement by other Webex "Survivability" features. These Exhibits are therefore representative charts for Cisco's new survivability feature. MeshDynamics accuses this new feature of infringement.

---

[1] https://blog.webex.com/collaboration/webex-suite-innovations-at-cisco-live-us-2025/; https://www.webex.com/whats-new.

[2] https://www.webex.com/content/dam/www/us/en/documents/pdf/us-at-a-glance-meeting-survivability.pdf.

C. Infringement Charts

Pursuant to L.P.R. 3-1(c), a chart identifying specifically where each element of each Asserted Claim is found within representative Accused Instrumentalities, including for each element that such party contends is governed by 35 U.S.C. § 112 (¶ 6), the identity of the structure(s), act(s), or material(s) in the Accused Instrumentality that performs the claimed function, is attached for the MeshDynamics Asserted Patents. *See* Exhibits 1-6.

The claim charts are based on public information reasonably available to MeshDynamics, and do not include any confidential or source code information in Cisco's possession, custody or control. MeshDynamics reserves all rights to revise, amend, and/or supplement these charts as discovery proceeds, including but not limited to adding citations to evidence and source code for software limitations, whose operation and structure is not publicly available and cannot be known to MeshDynamics at this time. Accordingly, pursuant to the Court's standing Discovery Order, MeshDynamics reserves the right to supplement these charts once such information is made available to MeshDynamics.

Furthermore, MeshDynamics reserves the right to revise these charts, as appropriate, upon issuance of any Claim Construction Order, including the identification of whether any arguable differences between the Accused Instrumentalities and the claims are insubstantial and/or whether the Accused Instrumentalities read on the claim elements under the doctrine of equivalents.

The claim charts are not intended to be an expert report on infringement or provide detailed analysis of the claim terms or infringement. MeshDynamics will disclose and produce an expert report regarding infringement with appropriate analysis pursuant to Fed. R. Civ. P. 26(a)(2), applicable Federal and Local Rules, and this Court's Orders. These charts include publicly available documentary evidence by way of example and not limitation.

D. Literal Infringement and Infringement Under the Doctrine of Equivalents

Pursuant to L.P.R. 3-1(d), MeshDynamics contends that the Accused Instrumentalities literally infringe or infringed the Asserted Claims of the MeshDynamics Asserted Patents as more specifically explained in the attached claim charts. *See* Exhibits 1-6. With respect to any claim element(s) that may be found not to be literally infringed, MeshDynamics contends in the alternative that the Cisco Accused Products infringed or infringe such claim element(s) under the doctrine of equivalents and that any claim element(s) not found to be literally met is equivalently met because any difference between the claim element(s) and the Accused Instrumentalities is not a substantial difference. In other words, to the extent literal infringement is purportedly absent, the Accused Instrumentalities identified in the attached claim charts perform substantially the same function of the invention recited in the Asserted Claims, in substantially the same way, to achieve substantially the same result. Accordingly, MeshDynamics contends that if any of the Accused Instrumentalities is found not to have infringed any Asserted Claims literally it is nevertheless embodied by the Accused Instrumentalities under at least one operative doctrine of equivalents test (*e.g.*, function-way-result or insubstantial difference). *See* Exhibits 1-6.

MeshDynamics reserves the right to add allegations of infringement under the doctrine of equivalents or amend its doctrine of equivalents allegations in response to discovery, Cisco's claim construction and non-infringement positions, claim construction proceedings, and this Court's claim construction rulings or other rulings by the Court.

E. Priority Dates

Pursuant to L.P.R. 3-1(e), MeshDynamics identifies the priority date to which each Asserted Claim is entitled:[3]

[3] MeshDynamics asserts that each of the MeshDynamics Asserted Patents is entitled to a priority date *as least as early as* the earliest priority date identified in its priority claims to the Patent Office

- Claims 1-4, 7-9, 10, 12-13, 15-17 of the '762 Patent: The asserted claims of the '762 Patent are entitled to a priority date at least as early as November 4, 2005.
- Claims 1, 5, 7 of the '852 Patent: The asserted claims of the '852 Patent are entitled to a priority date at least as early as November 24, 2008.
- Claims 1, 6, 7 of the '000 Patent: The asserted claims of the '000 Patent are entitled to a priority date at least as early as November 24, 2008 (*i.e.*, the priority date of the '852 Patent).

F. MeshDynamics Embodiments

Pursuant to L.P.R. 3-1(f), MeshDynamics reserves its right to rely upon its products as embodying all or some of the Asserted Claims. MeshDynamics reserves the right to revise, amend, or supplement this identification following any claim construction proceedings. MeshDynamics's identification of any embodiments at any time does not constitute any concession regarding the applicability of 35 U.S.C. § 287.

III. DOCUMENT PRODUCTION UNDER L.P.R. 3-2

Pursuant to L.P.R. 3-2 and subject to the reservation of rights outlined above, MeshDynamics is producing concurrently with service of these infringement contentions the following documents:

a) Documents sufficient to evidence each discussion with, disclosure to, or other manner of providing to a third party, or sale of or offer to sell, the claimed invention prior to the date of application for the patent in suit. A party's production of a document as

(*i.e.*, shown on the front of the patent). In the event of any invalidity challenge that raises the issue, either in this litigation or before the Patent Office, MeshDynamics reserves the right to rely on the documentation identified below and/or corroborating testimony supporting earlier dates of conception and/or reduction to practice to establish priority dates earlier than those listed here.

required herein shall not constitute an admission that such document evidences or is prior art under 35 U.S.C. §102. *See* MeshD00052044-63 at MeshD00052048-49.

b) All documents evidencing the conception, reduction to practice, design, and development of each claimed invention, which were created on or before the date of application for the patent in suit or the priority date identified pursuant to L.P.R. 3-1(e), whichever is earlier: MeshD00052044-63 at MeshD00052048-49. Source code available on a standalone computer, which will be made available as specified under the Protective Order to be entered in the case, may also be relied on for evidencing the conception, reduction to practice, design, and development of each claimed invention.

c) A copy of the file history for each patent in suit. *See* MeshD00000001-1848; *see also* MeshD00032748-771.

Dated: November 10, 2025

Respectfully submitted,

/s/ Elizabeth Bernard

Jennifer Parker Ainsworth
TX State Bar No. 00784720
jainsworth@wilsonlawfirm.com
WILSON ROBERTSON &
VANDEVENTER, P.C.
909 ESE Loop 323, Suite 400
Tyler, TX 75701
Telephone: (903) 509-5000

Scott R. Samay* (*pro hac vice*)
Jason S. Charkow* (*pro hac vice*)
Elizabeth Bernard* (admitted DC Bar No. 986675)
Lisa Phillips* (*pro hac vice*)
Taylor Lepore* (*pro hac vice*)
Erin Hadi* (*pro hac vice*)
Louay Meroueh* (*pro hac vice*)
ssamay@daignaultiyer.com
jcharkow@daignaultiyer.com
ebernard@daignaultiyer.com

lphillips@daignaultiyer.com
tlepore@daignaultiyer.com
ehadi@daignaultiyer.com
lmeroueh@daignaultiyer.com
DAIGNAULT IYER LLP
8229 Boone Blvd - Suite 450
Vienna, VA 22182
*Not admitted to practice in Virginia

Attorneys for Plaintiff Dynamic Mesh Networks, Inc. dba MeshDynamics

CERTIFICATE OF SERVICE

I certify that a copy of **MESHDYNAMICS'S LOCAL PATENT RULES 3-1 AND 3-2 INITIAL DISCLOSURES** was served on November 10, 2025 via email at the email addresses indicated below:

Tamir Packin
tpackin@desmaraisllp.com
Lindsey Miller
lmiller@desmaraisllp.com
Michael R Rhodes
mrhodes@desmaraisllp.com
Emily Weber
eweber@desmaraisllp.com
Ryan Thorne
rthorne@dllp.com
Ha Vu Thu Huynh
hhuynh@desmaraisllp.com

Melissa Richards Smith
melissa@gillamsmithlaw.com

Attorneys for Defendant Cisco Systems, Inc.

/s/ Elizabeth Bernard
Elizabeth Bernard
Counsel for MeshDynamics

Exhibit 1 – U.S. Patent No. 8,477,762 (Cisco Webex with Webex Calling – Site Survivability)

Cisco Systems, Inc. ("Cisco") has and continues to make, use, sell, offer for sale, and/or import the Cisco Webex VoIP Network, including but not limited to Cisco's Webex and Webex Calling with related software and hardware (the "Cisco Accused Products," *see* Exhibit 7), and has infringed and infringes at least Claims 1-2 (the "Asserted Claims") of U.S. Patent No. 8,477,762 (the "'762 Patent").[1]

Cisco has and continues to infringe (literally and/or under the doctrine of equivalents), directly and/or through subsidiaries, agents, representatives, or intermediaries, one or more claims of the '762 Patent by making, using, testing, supplying, causing to be supplied, importing, selling, and/or offering for sale in the United States the Cisco Accused Products.

Cisco directly infringes and has infringed under 35 U.S.C. § 271(a) by making, using, selling, offering for sale and importing the Cisco Accused Products. Cisco further directly infringes and has infringed by testing, setting up, and using the Cisco Webex VoIP Network on Cisco's campuses and locations throughout the United States,[2] and/or assisting customers in setting up and servicing their Cisco Webex VoIP Networks. On information and belief, Cisco has partnered with several customers to set up an infringing Cisco Webex VoIP Networks in the United States.[3]

Cisco indirectly infringes and has infringed under 35 U.S.C. § 271(b) by providing specific guidance and instructions to its customers and end users on how to infringe the '762 Patent and make and use the infringing Cisco Webex VoIP Network. Specifically, Cisco's Preferred Architecture guides, deployment guides, Technical Assistance Center, Cisco Tech Talks, technical support, Cisco Community, presentations, and technical documentation on Cisco's website identified in the chart *infra* provide guidelines for the deployment of an infringing Cisco Webex VoIP Network. These guides and instructions specifically teach and describe each and every claim element of Claims 1-2 as demonstrated *infra*, including the necessary components to make and use the infringing Cisco Webex VoIP Network, and the infringing configuration and operation of Webex, Site

---

[1] The identified Accused Products also include Cisco's products, services, and systems that are considered sold or related to the infringement in the United States and subject to a reasonable royalty according to the Federal Circuit's decisions in *Carnegie Mellon Univ. v. Marvell Tech. Group. Ltd.*, 807 F.3d 1283 (Fed. Cir. 2015), *Cal. Inst. of Tech. v. Broadcom Ltd.*, 25 F.4th 976 (Fed. Cir. 2022), and *Brumfield v. IBG LLC*, 97 F.4th 854 (Fed. Cir. 2024).

[2] *See, e.g.*, https://blog.webex.com/collaboration/behind-the-scenes-how-cisco-it-migrated-84000-users-to-webex-calling/ ("With Webex Calling, employees are no longer tied to the corporate WAN. Phones can now be deployed anywhere with internet access — as demonstrated at the Cisco GSX conference, where a temporary network was set up using hotel Wi-Fi, avoiding costly LAN build-outs.").

[3] *See, e.g.*, https://blog.webex.com/customer-stories/why-cloud-calling-is-a-gamechanger-for-broadcom/; https://blog.webex.com/customer-stories/how-att-and-webex-power-hybrid-work-with-world-class-cloud-calling/.

Survivability Gateways, and other software and hardware that comprise the infringing Cisco Webex VoIP Network. These guides and instructions were published and distributed by Cisco for its customers for the sole purpose to instruct and encourage its customers to purchase the Cisco components to make and use the infringing Cisco Webex VoIP Network (and directly infringe literally and/or under the doctrine of equivalents). Cisco has had knowledge of the '762 Patent since 2009 when Cisco executives met with MeshDynamics to discuss partnering opportunities and the application that would result in the '762 Patent. MeshDynamics further put Cisco on actual notice of its infringement by its making, using, selling, offering for sale and importing the Cisco Accused Products that comprise the Cisco Webex VoIP Networks in 2022. Cisco has knowingly and intentionally induced its customers to infringe the '762 Patent, or in the alternative was willfully blind to the '762 Patent and the infringement, following the MeshDynamics meeting in 2009.

Cisco further indirectly infringes and has infringed under 35 U.S.C. § 271(c) by supplying the components used in the infringing Cisco Webex VoIP Network, with knowledge of its infringing use (as discussed *supra*) and without substantial non-infringing uses. Further, the Cisco Accused Products were designed specifically to be used in a manner that infringes the '762 Patent. Cisco Accused Products come enabled as an infringing product, are particularly suited isolated on-premise configuration and operation, and Cisco provides specific instructions and guides on how to make and use the Cisco Webex VoIP Network using the Cisco Accused Products. As a result of Cisco's selling and/or offering for sale of the Cisco Accused Products to other entities, the other entities use these products for their intended purpose and according to their instructions with the result that such entities directly infringe the '762 Patent, literally or under the doctrine of equivalents, for the reasons stated *infra*. Cisco's Accused Products are specially made and adapted for this use in an infringing manner, are not staple articles of commerce, and do not have substantial non-infringing uses.

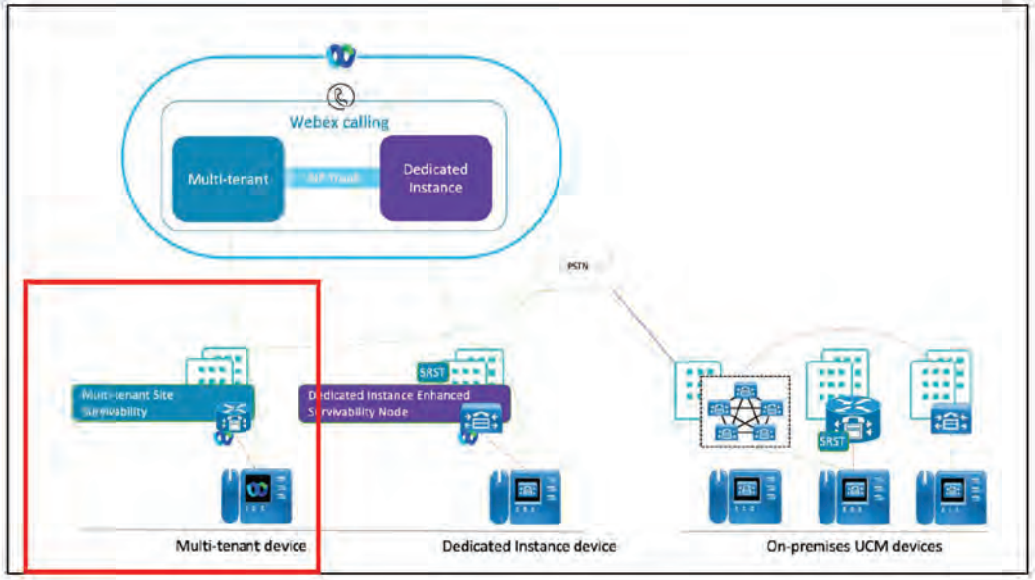
MeshDynamics asserts that the Cisco Accused Products literally infringed and continue to infringe the Asserted Claims of the '762 Patent. With respect to any claim limitation that may be found not to be literally infringed, MeshDynamics contends in the alternative that Cisco Accused Products infringed such claim limitations under the doctrine of equivalents and that any claim element not found to be literally met is equivalently met because any difference between the claim limitation and Cisco Accused Products is not a substantial difference. Accordingly, MeshDynamics contends that if any Cisco Accused Products is found not to have infringed any Asserted Claims literally it is nevertheless embodied by Cisco Accused Products under an operative doctrine of equivalents test (*e.g.*, function-way-result or insubstantial difference).

The below chart presents MeshDynamics's preliminary infringement analysis of Cisco Accused Products based solely on public information. MeshDynamics has not received any discovery from Cisco, including any confidential information or source code demonstrating the operation and

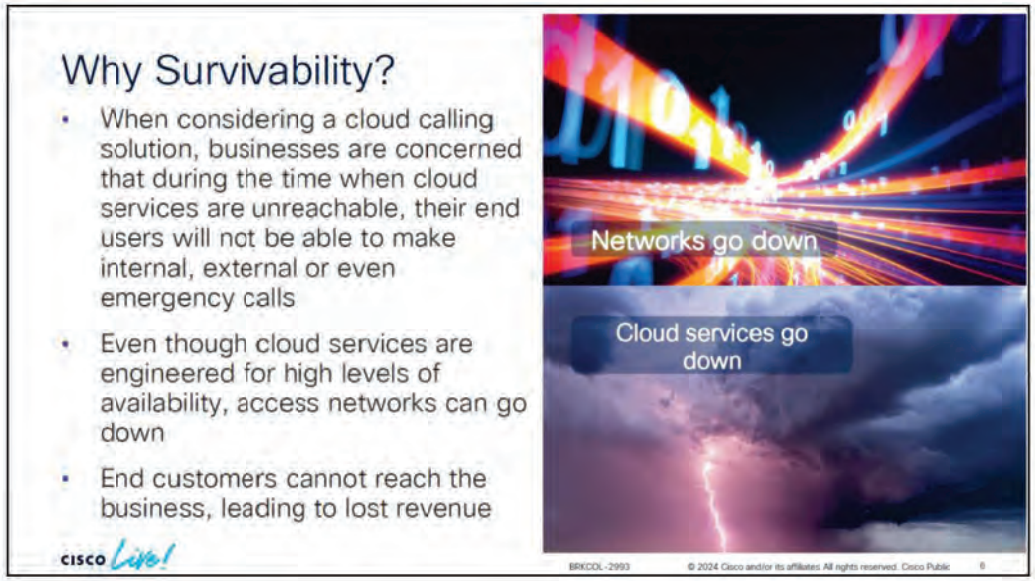
structure of the Cisco Accused Products. All information contained in this disclosure is the result of publicly available information regarding the Cisco Accused Products. Based on these circumstances, MeshDynamics presents these infringement allegations reflecting its analysis of the facts presently known to it. To the best of MeshDynamics's knowledge, information, and belief, formed after an inquiry that is reasonable under the circumstances, the information contained in this disclosure is correct.

Certain information about Cisco Accused Products is not available without discovery, such as proprietary source code, documents, and deposition testimony, from Cisco. Accordingly, MeshDynamics reserves the right to supplement and/or amend this infringement contention claim chart as new information becomes available and as MeshDynamics has the opportunity to review Cisco document productions, including information related to the implementation of Cisco Accused Products, relationships with other parties who participated or contributed to the operation of Cisco Accused Products, and/or elements of Cisco Accused Products that cannot be fully examined based solely on publicly available information. Infringement investigations are ongoing, and MeshDynamics anticipates that additional facts and relevant documents will be uncovered and disclosed that create cause for supplementation and/or amendment.

Claim 1	Cisco Webex (*e.g.*, Cisco Webex Calling)
A VoIP-capable network comprising:	Cisco's Webex, *e.g.*, Webex Calling, is a Voice over Internet Protocol-capable network in which each client or device can communicate with multiple other clients or devices over the Internet using, *e.g.*, a computer or a phone. Voice over Internet Protocol (VoIP) transmits sound as data over the internet. This lets you talk over the internet without using a phone. Webex uses VoIP so users can call into a meeting using a computer. With a paid plan, you can also call into a meeting with your phone. Source: https://www.webex.com/what-is-voip.html. Webex Calling is a cloud calling system offered by Cisco that uses VoIP thereby forming a "VoIP-capable network." Further, with Site Survivability (for multi-tenant), Webex Calling maintains the network connectivity during an outage (*i.e.*, no network or cloud connectivity) and promotes network continuity. Webex Calling with Site Survivability acts as the VoIP-capable network that includes Webex Calling endpoints (*e.g.,* Cisco Desk Phones, Webex App), gateway routers (*e.g.*, Cisco's Catalyst Series 8200/8300 series routers, Catalyst 8000v Edge routers, etc.). and software (*e.g.*, Cisco IOS XE). Source: https://help.webex.com/en-us/article/nk1shtj/Get-started-with-Webex-Calling.



Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability.

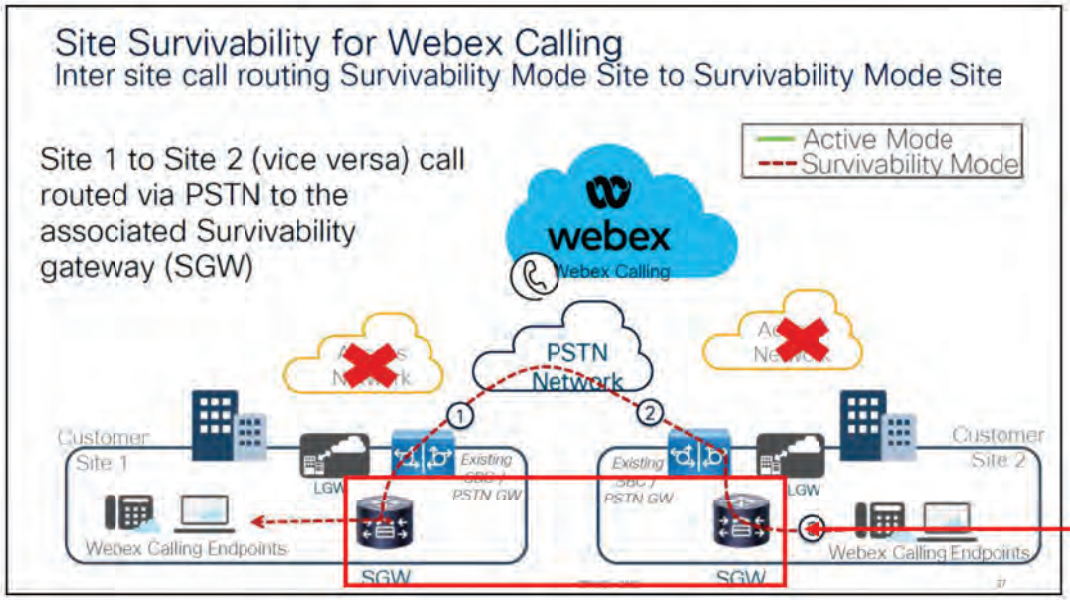


Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKCOL-2993.pdf.

	By default, Webex Calling endpoints operate in Active mode, connecting to the Webex cloud for SIP registration and call control. If the network connection to Webex is lost, endpoints automatically switch to Survivability mode and register with the local Survivability Gateway. In this mode, the gateway provides basic backup calling services. Once the network connection to Webex is restored, call control and registrations switch back to the Webex cloud. The following calls are supported in Survivability mode: • Internal calling (intrasite) between supported Webex Calling endpoints • External calling (incoming and outgoing) using a local PSTN circuit or SIP trunk to external numbers and E911 providers To use this feature, you must configure a Cisco IOS XE router in the local network as a Survivability Gateway. The Survivability Gateway syncs calling information daily from the Webex cloud for endpoints at that location. If the endpoints switch to Survivability mode, the gateway can use this information to take over SIP registrations and provide basic calling services. Source: https://help.webex.com/en-us/article/d68vi1/Site-Survivability-for-Webex-Calling ("If the connection to the Webex cloud breaks, a Survivability Gateway in the local network can provide backup call control for endpoints at that location."). To extent the preamble is limiting, and it is not literally infringed, it is infringed under the doctrine of equivalents. A person skilled in the relevant art would also understand that calling over the PSTN is part of a "VoIP-capable network." SIP (Session Initiation Protocol) calls can go over the PSTN, as SIP trunking provides a connection from a company's Internet-based phone system to the PSTN. This is how Internet-based phones can call traditional landlines and mobile phones, and vice versa, and still have a "VoIP-capable network." A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial. *See* https://www.webex.com/what-is-voip.html ("VoIP can also be used to connect to the PSTN and vice versa. For instance, Webex Calling supports customers with the ability to select PSTN connectivity on a site-by-site basis. Webex customers can use any combination of Cisco Calling Plans, Cloud Connected PSTN, or Local Gateway-based PSTN across different sites.").
one or more VoIP client devices;	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network comprising one or more VoIP client devices. Webex Calling's "one or more VoIP client devices" for making calls can include users calling, for example, from the Webex App on a computer, or Webex phones and devices, including Cisco IP Phones 6800, 7800, 8800 Series desk phones and Cisco IP Conference Phones 7832 and 8832.

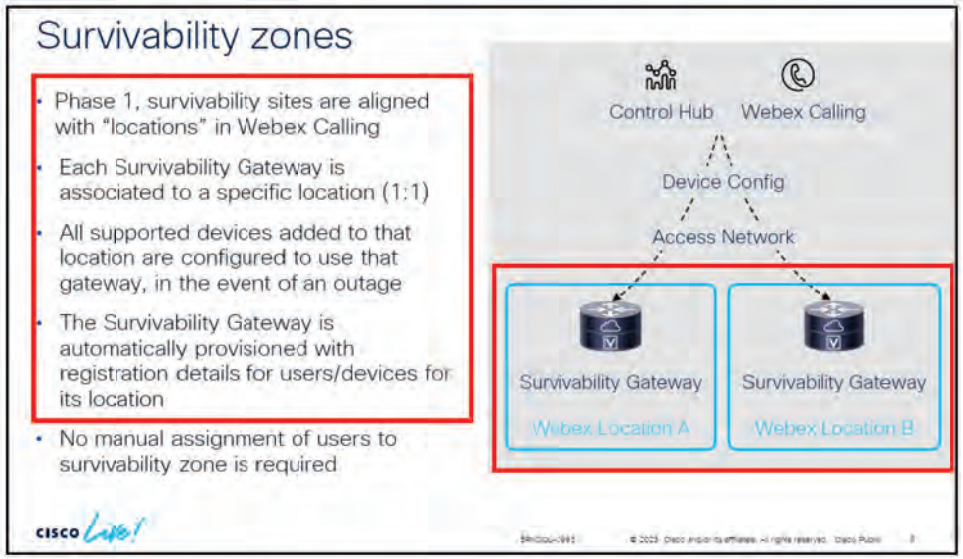
	Webex App (users) Webex App brings everyone together to do exceptional work: One, easy-to-use and secure app to meet, message and make calls. It supports various calling options and we've created several articles to help you make the most out of your calling experience, including how you can set up your own features: **Phones and devices (users)** Webex Calling further provides an integrated user calling experience with Webex devices, including Cisco IP Phones 6800, 7800, 8800 Series desk phones, Cisco IP Conference Phones 7832 and 8832, Cisco IP DECT 6800 Series, Cisco Desk Phone 9800 Series, and analog ATAs. The following articles help you with getting up and running on these devices: Source: https://help.webex.com/en-us/article/nk1shtj/Get-started-with-Webex-Calling. To the extent this claim element is not literally infringed, it is infringed under the doctrine of equivalents. The Cisco VoIP devices perform the same function of making VoIP calls in the same way by using the Internet and larger VoIP system infrastructure that allows calls to bridge to the PSTN when necessary and achieves the same result of connecting a VoIP call during an outage. A person skilled in the relevant art would understand that a "VoIP client device" is any hardware or software (*e.g.*, an "endpoint") that uses VoIP technology to make and receive calls and other communications over an IP network, such as the Internet. A "VoIP client device" can also connect to the PSTN through, *e.g.*, a VoIP gateway. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
two or more VoIP nodes forming an isolated cluster wherein the two or more VoIP nodes in the isolated cluster are in communication with one another; wherein each of the VoIP client devices communicates with at least one VoIP node;	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network comprising two or more VoIP nodes forming an isolated cluster that are in communication with one another, and wherein each of the VoIP client devices communicates with at least one VoIP node. Webex Calling is a VoIP-capable network including Survivability Gateways for Survivability Mode ("SGWs" or "VoIP nodes forming an isolated cluster"). Site Survivability for Webex Calling is designed to ensure users at a site can make/receive calls, both internally and externally, even when they cannot connect to the Webex Calling cloud. SGWs are isolated nodes in the customer's local network (*e.g.*, not in an external datacenter). To use this feature, you must configure a Cisco IOS XE router in the local network as a Survivability Gateway. The Survivability Gateway syncs calling information daily from the Webex cloud for endpoints at that location. If the endpoints switch to Survivability mode, the gateway can use this information to take over SIP registrations and provide basic calling services. Source: https://help.webex.com/en-us/article/d68vi1/Site-Survivability-for-Webex-Calling. SGWs at different sites or branches (*e.g.*, "two or more VoIP nodes forming an isolated cluster") route a call between two endpoints without requiring a connection to Webex. The Webex Calling endpoints (*i.e.*, "VoIP client devices")

communicate with associated SGWs during an outage ("at least one VoIP node"), and the SGWs communicate with one another without the cloud to route and complete the call, for example, from Survivability Mode Site/SGW ("Site 1") to Survivability Mode Site/SGW ("Site 2"), as shown in the inter-site diagram below (other configurations are also shown in the documentation):



Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKCOL-2993.pdf; *see also* https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Collaboration/hybrid/AltDesigns/PA-WbxCall.pdf.

Survivability zones are also defined by on-premise "location" in Webex with SGWs associated with specific locations together forming an "isolated cluster":



Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2023/pdf/BRKCOL-2993.pdf.

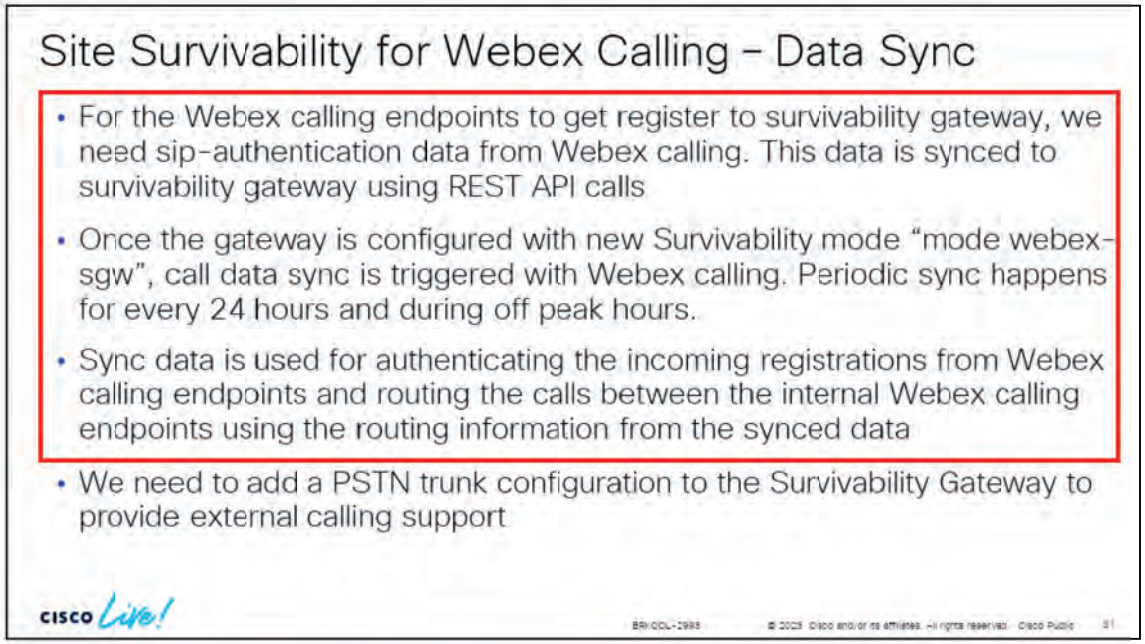
A static SIP routing between two SGWs may also be set up so that branch sites can call each other even during a Webex cloud outage, including when the WAN is still up. This configuration allows direct communication and site-to-site calling between SGWs (*i.e.*, an "isolated cluster" "in communication with one another") during Survivability Mode, using static SIP dial-peers. For example, a Cisco IOS XE router can be configured as an SGW, including setting up static SIP dial-peers to route calls between sites during Survivability Mode. When Site 1 and Site 2 enter Survivability Mode, the endpoints register to local SGWs, SGWs auto-create dynamic dial-peers for local phones or PSTN, and calls to other site extensions are matched to static SIP dial-peers, routed directly to the SGW.

Source: https://help.webex.com/en-us/article/d68vi1/Site-survivability-for-Webex-Calling#task_C988EF9EECEA9D5DCA2A4EC4F07FC095; *see also* https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2023/pdf/BRKCOL-2993.pdf; https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/cube_m_lineside-survivability.pdf; https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2025/pdf/BRKCOL-2312.pdf; https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-border-element/221645-configure-high-availability-ha-on-cube.html (two gateways communicating with each other can be enabled per location for high availability).

	MeshDynamics asserts that these claim elements are software limitations. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If these claim elements are not literally infringed, they are infringed under the doctrine of equivalents. Cisco's Webex Calling with Site Survivability performs the same functions of forming an isolated cluster of nodes communicating with each other and VoIP devices during an outage in the same way by utilizing multiple on-premise gateways and achieves the same result of on-premise (not in the cloud and without an external SIP server) VoIP network for VoIP calling and maintaining device and endpoint communication. Site survivability allows for remote sites and branches to communicate with devices and together form an isolated cluster and VoIP network without an external SIP server for communications. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed elements are insignificant or insubstantial because Cisco's Webex Calling with Site Survivability creates and maintains a VoIP network without an external SIP server. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial. A person skilled in the relevant art would also understand that calling over the PSTN is part of a "VoIP-capable network." SIP (Session Initiation Protocol) calls can go over the PSTN, as SIP trunking provides a connection from a company's Internet-based phone system to the PSTN. This is how Internet-based phones can call traditional landlines and mobile phones, and vice versa, and still have a "VoIP-capable network." A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
wherein each of the VoIP nodes further comprises a local SIP registry built by exchanging SIP information with the remaining VoIP nodes in the isolated cluster;	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network wherein each of the VoIP nodes further comprises a local SIP registry built by exchanging SIP information with the remaining VoIP nodes in the isolated cluster. In the event of a network outage, the SGWs actively take over call routing responsibility. SGWs will process all external and internal calls and properly handle any emergency call routing. (*e.g.*, "each of the VoIP nodes further comprises a local SIP registry"). Endpoints switch to Survivability Mode and registrations fall to the SGW within the local network. Performing a SIP registration means a SIP phone or client registers its current location (*e.g.*, IP address) with the SGW, allowing the network to know where to send incoming calls to that user. The SGW receives the request, authenticates the user, and stores the information. Each SGW is thus configured as a "local SIP registry" for call control during Survivability Mode. SGWs exchange SIP information with the other SGWs for call control and connection during Survivability Mode, including dynamically creating dial peers to route the calls. The SGWs handle registration, the dial peers and exchange of information during the outage to further build the "local SIP registry."

By default, Webex Calling endpoints operate in Active mode, connecting to the Webex cloud for SIP registration and call control. However, if the network connection to Webex breaks, endpoints switch automatically to Survivability mode and registrations fall back to the Survivability Gateway within the local network. While endpoints are in Survivability mode, the Survivability Gateway provides a basic backup calling service for those endpoints. After the network connection to Webex resumes, call control and registrations revert to the Webex cloud.

Source: https://help.webex.com/en-us/article/d68vi1/Site-survivability-for-Webex-Calling.



Site Survivability for Webex Calling – SIP Registration

- When the gateway is enabled with "mode webex-sgw" under voice register global, port 8933 will be opened for listen socket. Webex calling users will establish mTLS connection using this port with survivability gateway while registering
- When the Webex calling Users falls into survivability mode, register message will be sent to survivability gateway with its AOR. Unlike in the Unified-SRST case, here registration will be using AOR instead of DNs.
- Gateway will check the internal database generated using the subscriber data from Webex Calling, if the AOR is a valid entry then Registration is allowed with proper authentication. If the entry is not available in the internal database, 403 response will be sent as the Registration is rejected.
- If the AOR in the subscriber database is valid but the Authentication/password is wrong, then SGW will challenge the authentication with 401. On receiving the proper credentials, endpoint will be registered, else registration gets rejected with 403.
- Dynamic dial-peer will be created on the gateway with dial-peer number 4000x. This will be used while routing calls. Dial-peer will have AOR as its destination pattern.

Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2023/pdf/BRKCOL-2993.pdf.

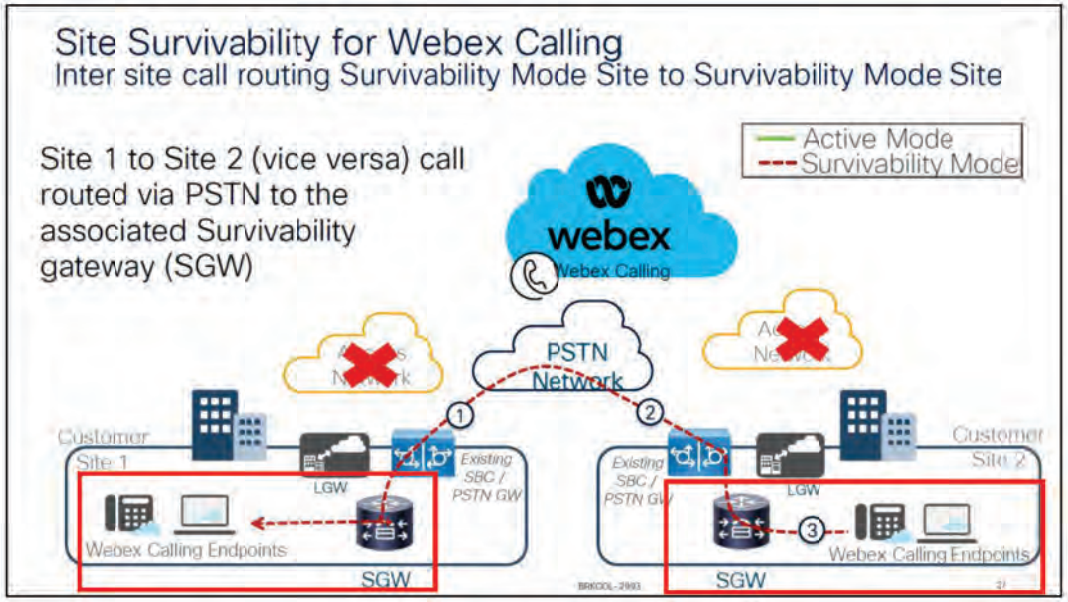
The SGWs log call details (such as the calling number, called number, time, and duration) locally, and through these observations and interactions with the other (*e.g.*, originating or receiving) SGW, create a CDR to further build the "local SIP registry" by logging information, including SIP information.

> The connector automatically configures CDR-related commands to facilitate the collection of call count metrics.

Source: https://help.webex.com/en-us/article/d68vi1/Site-survivability-for-Webex-Calling.

This data includes the SIP information sent and received about the call between sites/SGWs, including when the call was connected and ended (*i.e.*, "local SIP registry built by exchanging SIP information"):

	Understanding CDR Data Call detail records (CDR) detail the called number, the number that placed the call, the date and time that the call was started, the time that it connected, and the time that it ended. Call management records (CMRs, or diagnostic records) detail the jitter, lost packets, the amount of data sent and received during the call, and latency. CDR data comprises CDRs and CMRs collectively. A single call can result in the generation of several CDRs and CMRs. Cisco CallManager records information regarding each call in CDRs and CMRs. CDRs and CMRs, known collectively as CDR data, serve as the basic information source for CAR. You can set service parameters in Cisco CallManager Administration to establish the amount of disk space to allocate to CDRs. For more information, refer to the *Cisco CallManager System Guide*. Source: https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/4_2_1/ccmsrvs/sscar.html; https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/callReportingBillingAdmin/14/cucm_b_reporting-billing-administration-guide-14/cucm_b_reporting-and-billing-administration-guide_chapter_01010.html. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling with Site Survivability performs the same function of building a local SIP registry in the same way by replicating and exchanging SIP information to connect calls and achieves the same result of operating without an external server to connect calls inter-site and maintain endpoint communications during an outage. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the SGWs maintain SIP information and use this information to connect endpoints at different sites or locations. The SGWs function as autonomous SIP servers during an outage, and exchange SIP information, *e.g.*, over the PSTN to complete inter-site calls. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
wherein a first VoIP client device in communication with a first VoIP node establishes a communication with a second VoIP device in communication with a second VoIP node using the local SIP registries of the first VoIP node and the second VoIP node.	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network wherein a first VoIP client device in communication with a first VoIP node establishes a communication with a second VoIP device in communication with a second VoIP node using the local SIP registries of the first VoIP node and the second VoIP node. A call from a "first VoIP client device," *e.g.*, endpoint in Site 2 or Webex Location A, registered and in communication to an SGW, can be routed from the SGW to a "second VoIP client device," *e.g.*, endpoint in Site 1 or Webex Location B, registered and in communication to another SGW, as shown for example in the inter-site Site Survivability for Webex Calling below and Cisco's documentation. Both SGWs comprise "local SIP registries" (as discussed above in Survivability Mode as taking over registration and call control), and are used to establish and connect the call between the endpoint in Site 2 and the endpoint in Site 1.



Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2023/pdf/BRKCOL-2993.pdf.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling with Site Survivability performs the same function of establishing a communication between two endpoints in a VoIP network in the same way by using SIP information at each gateway and achieves the same result establishing a VoIP call between to endpoints. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Webex Calling with Site Survivability will establish a connection between endpoints using on-premise gateways and their SIP registries. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Claim 2	
The VoIP-capable network of claim 1, wherein the local SIP	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein the local SIP registries of the isolated VoIP nodes are updated as the VoIP nodes and the VoIP client devices begin communication with the isolated cluster and end communication with the isolated cluster.

registries of the isolated VoIP nodes are updated as the VoIP nodes and the VoIP client devices begin communication with the isolated cluster and end communication with the isolated cluster	The SGWs log call details (such as the calling number, called number, time, and duration) locally, and through these observations and interactions with the other (*e.g.*, originating or receiving) SGW, create a CDR to further build the "local SIP registry" by logging information, including SIP information that indicates the call is active. The connector automatically configures CDR-related commands to facilitate the collection of call count metrics. Source: https://help.webex.com/en-us/article/d68vi1/Site-survivability-for-Webex-Calling. This data includes all of the SIP information sent and received about the call between sites/SGWs, including when the call was connected and ended (*i.e.*, "local SIP registry built by exchanging SIP information"), and is updated as the device being and end communication: **Understanding CDR Data** Call detail records (CDR) detail the called number, the number that placed the call, the date and time that the call was started, the time that it connected, and the time that it ended. Call management records (CMRs, or diagnostic records) detail the jitter, lost packets, the amount of data sent and received during the call, and latency. CDR data comprises CDRs and CMRs collectively. A single call can result in the generation of several CDRs and CMRs. Cisco CallManager records information regarding each call in CDRs and CMRs. CDRs and CMRs, known collectively as CDR data, serve as the basic information source for CAR. You can set service parameters in Cisco CallManager Administration to establish the amount of disk space to allocate to CDRs. For more information, refer to the *Cisco CallManager System Guide*. Source: https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/4_2_1/ccmsrvs/sscar.html; https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/callReportingBillingAdmin/14/cucm_b_reporting-billing-administration-guide-14/cucm_b_reporting-and-billing-administration-guide_chapter_01010.html. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling with Site Survivability performs the same function of updating the local SIP registry and logs in the same way by exchanging the SIP information from the call and achieves the same result of an updated local SIP registry and logs using the information from the call. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the local SIP registries and logs of each gateway are updated with call information. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Exhibit 2 – U.S. Patent No. 8,477,762 (Cisco Webex with Webex Calling – Enhanced Survivability)

Cisco Systems, Inc. ("Cisco") has and continues to make, use, sell, offer for sale, and/or import the Cisco Webex VoIP Network, including but not limited to Cisco's Webex and Webex Calling with related software and hardware (the "Cisco Accused Products," *see* Exhibit 7), and has infringed and infringes at least Claims 1-4 and 7-9 (the "Asserted Claims") of U.S. Patent No. 8,477,762 (the "'762 Patent").[1]

Cisco has and continues to infringe (literally and/or under the doctrine of equivalents), directly and/or through subsidiaries, agents, representatives, or intermediaries, one or more claims of the '762 Patent by making, using, testing, supplying, causing to be supplied, importing, selling, and/or offering for sale in the United States the Cisco Accused Products.

Cisco directly infringes and has infringed under 35 U.S.C. § 271(a) by making, using, selling, offering for sale and importing the Cisco Accused Products. Cisco further directly infringes and has infringed by testing, setting up, and using the Cisco Webex VoIP Network on Cisco's campuses and locations throughout the United States,[2] and/or assisting customers in setting up and servicing their Cisco Webex VoIP Networks. On information and belief, Cisco has partnered with several customers to set up an infringing Cisco Webex VoIP Network in the United States.[3] Cisco also monitors and manages Enhanced Survivability Nodes like other nodes that are deployed in a Dedicated Instance datacenter.[4]

Cisco indirectly infringes and has infringed under 35 U.S.C. § 271(b) by providing specific guidance and instructions to its customers and end users on how to infringe the '762 Patent and make and use the infringing Cisco Webex VoIP Network. Specifically, Cisco's Preferred Architecture guides, deployment guides, Technical Assistance Center, Cisco Tech Talks, technical support, Cisco Community, presentations, and technical documentation on Cisco's website identified in the chart *infra* provide guidelines for the deployment of an infringing Cisco Webex VoIP Network.

---

[1] The identified Accused Products also include Cisco's products, services, and systems that are considered sold or related to the infringement in the United States and subject to a reasonable royalty according to the Federal Circuit's decisions in *Carnegie Mellon Univ. v. Marvell Tech. Group. Ltd.*, 807 F.3d 1283 (Fed. Cir. 2015), *Cal. Inst. of Tech. v. Broadcom Ltd.*, 25 F.4th 976 (Fed. Cir. 2022), and *Brumfield v. IBG LLC*, 97 F.4th 854 (Fed. Cir. 2024).

[2] *See, e.g.*, https://blog.webex.com/collaboration/behind-the-scenes-how-cisco-it-migrated-84000-users-to-webex-calling/ ("With Webex Calling, employees are no longer tied to the corporate WAN. Phones can now be deployed anywhere with internet access — as demonstrated at the Cisco GSX conference, where a temporary network was set up using hotel Wi-Fi, avoiding costly LAN build-outs.").

[3] *See, e.g.*, https://blog.webex.com/customer-stories/why-cloud-calling-is-a-gamechanger-for-broadcom/; https://blog.webex.com/customer-stories/how-att-and-webex-power-hybrid-work-with-world-class-cloud-calling/; *see also* https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cloud-Calling-Setup-Assist-Add-Ons.pdf.

[4] *See, e.g.*, https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability.

These guides and instructions specifically teach and describe each and every claim element of Claims 1-4 and 7-9 as demonstrated *infra*, including the necessary components to make and use the infringing Cisco Webex VoIP Network, and the infringing configuration and operation of Webex, Unified CM clusters, Local Gateways, Enhanced Survivability Nodes, and other software and hardware that comprise the infringing Cisco Webex VoIP Network. These guides and instructions were published and distributed by Cisco for its customers for the sole purpose to instruct and encourage its customers to purchase the Cisco components to make and use the infringing Cisco Webex VoIP Network (and directly infringe literally and/or under the doctrine of equivalents). Cisco has had knowledge of the '762 Patent since 2009 when Cisco executives met with MeshDynamics to discuss partnering opportunities and the application that would result in the '762 Patent. MeshDynamics further put Cisco on actual notice of its infringement by its making, using, selling, offering for sale and importing the Cisco Accused Products that comprise the Cisco Webex VoIP Networks (including "Mesh" functionality, such as Unified CM clusters and Enhanced Survivability Nodes) in 2022. Cisco has knowingly and intentionally induced its customers to infringe the '762 Patent, or in the alternative was willfully blind to the '762 Patent and the infringement, following the MeshDynamics meeting in 2009.

Cisco further indirectly infringes and has infringed under 35 U.S.C. § 271(c) by supplying the components used in the infringing Cisco Webex VoIP Network, with knowledge of its infringing use (as discussed *supra*) and without substantial non-infringing uses. Further, the Cisco Accused Products were designed specifically to be used in a manner that infringes the '762 Patent. Cisco Accused Products come enabled as an infringing product, are particularly suited for isolated on-premise configuration and operation, and Cisco provides specific instructions and guides on how to make and use the Cisco Webex VoIP Network using the Cisco Accused Products. As a result of Cisco's selling and/or offering for sale of the Cisco Accused Products to other entities, the other entities use these products for their intended purpose and according to their instructions with the result that such entities directly infringe the '762 Patent, literally or under the doctrine of equivalents, for the reasons stated *infra*. Cisco's Accused Products are specially made and adapted for this use in an infringing manner, are not staple articles of commerce, and do not have substantial non-infringing uses.

MeshDynamics asserts that the Cisco Accused Products literally infringed and continue to infringe the Asserted Claims of the '762 Patent. With respect to any claim limitation that may be found not to be literally infringed, MeshDynamics contends in the alternative that Cisco Accused Products infringed such claim limitations under the doctrine of equivalents and that any claim element not found to be literally met is equivalently met because any difference between the claim limitation and Cisco Accused Products is not a substantial difference. Accordingly, MeshDynamics

contends that if any Cisco Accused Products is found not to have infringed any Asserted Claims literally it is nevertheless embodied by Cisco Accused Products under an operative doctrine of equivalents test (*e.g.*, function-way-result or insubstantial difference).

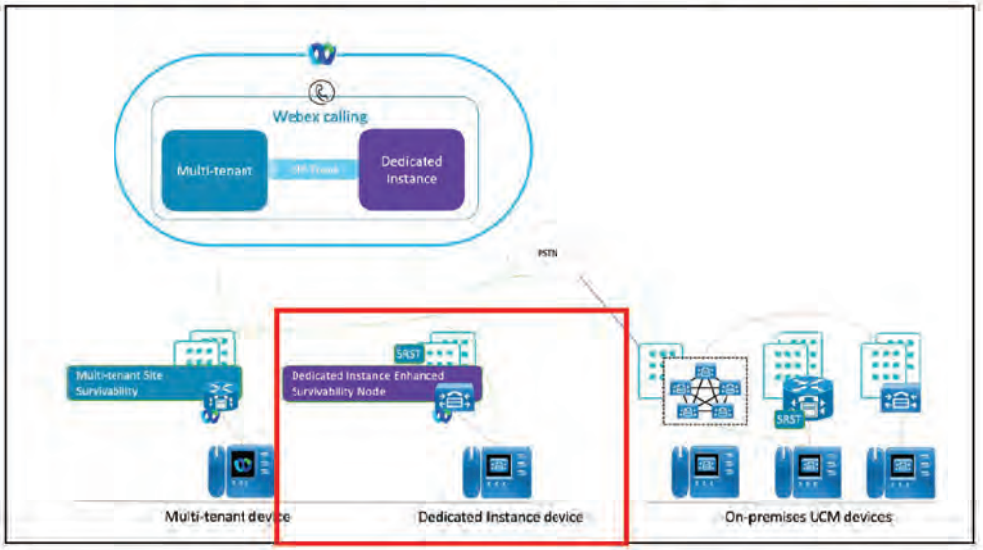
The below chart presents MeshDynamics's preliminary infringement analysis of Cisco Accused Products based solely on public information. MeshDynamics has not received any discovery from Cisco, including any confidential information or source code demonstrating the operation and structure of the Cisco Accused Products. All information contained in this disclosure is the result of publicly available information regarding the Cisco Accused Products. Based on these circumstances, MeshDynamics presents these infringement allegations reflecting its analysis of the facts presently known to it. To the best of MeshDynamics's knowledge, information, and belief, formed after an inquiry that is reasonable under the circumstances, the information contained in this disclosure is correct.

Certain information about Cisco Accused Products is not available without discovery, such as proprietary source code, documents, and deposition testimony, from Cisco. Accordingly, MeshDynamics reserves the right to supplement and/or amend this infringement contention claim chart as new information becomes available and as MeshDynamics has the opportunity to review Cisco document productions, including information related to the implementation of Cisco Accused Products, relationships with other parties who participated or contributed to the operation of Cisco Accused Products, and/or elements of Cisco Accused Products that cannot be fully examined based solely on publicly available information. Infringement investigations are ongoing, and MeshDynamics anticipates that additional facts and relevant documents will be uncovered and disclosed that create cause for supplementation and/or amendment.

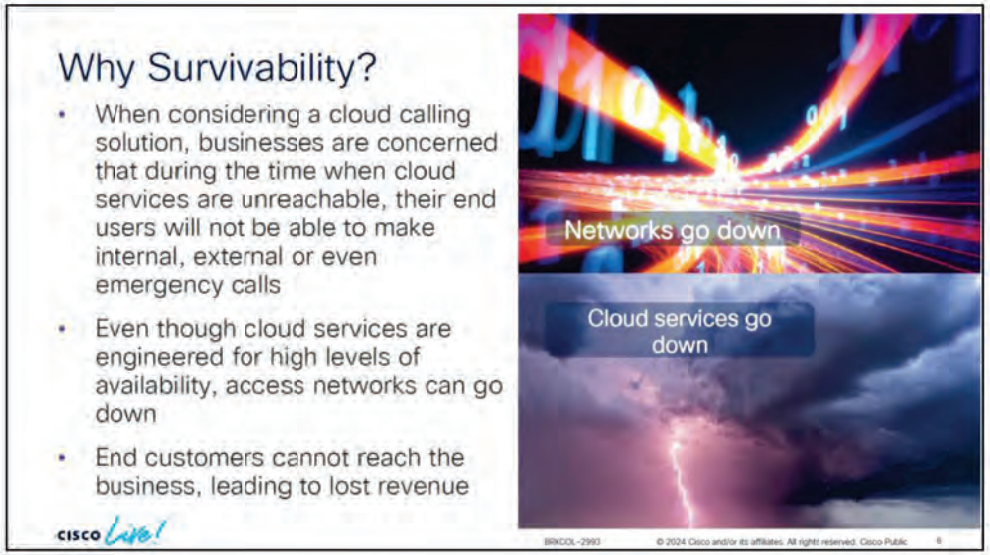
Claim 1	Cisco Webex (*e.g.*, Cisco Webex Calling)
A VoIP-capable network comprising:	Cisco's Webex, *e.g.*, Webex Calling, is a Voice over Internet Protocol-capable network in which each client or device can communicate with multiple other clients or devices over the Internet using, *e.g.*, a computer or a phone. Voice over Internet Protocol (VoIP) transmits sound as data over the internet. This lets you talk over the internet without using a phone. Webex uses VoIP so users can call into a meeting using a computer. With a paid plan, you can also call into a meeting with your phone. Source: https://www.webex.com/what-is-voip.html. Webex Calling is a cloud calling system offered by Cisco that uses VoIP thereby forming a "VoIP-capable network." Further, with Enhanced Survivability (for Dedicated Instance), Webex Calling maintains the network connectivity during an outage (*i.e.*, no network or cloud connectivity) and promotes network continuity. Webex Calling with

Enhanced Survivability acts as the VoIP-capable network that includes Webex Calling Endpoints (*e.g.*, Cisco Desk Phones, Webex App), local gateways, and Enhanced Survivability Nodes.

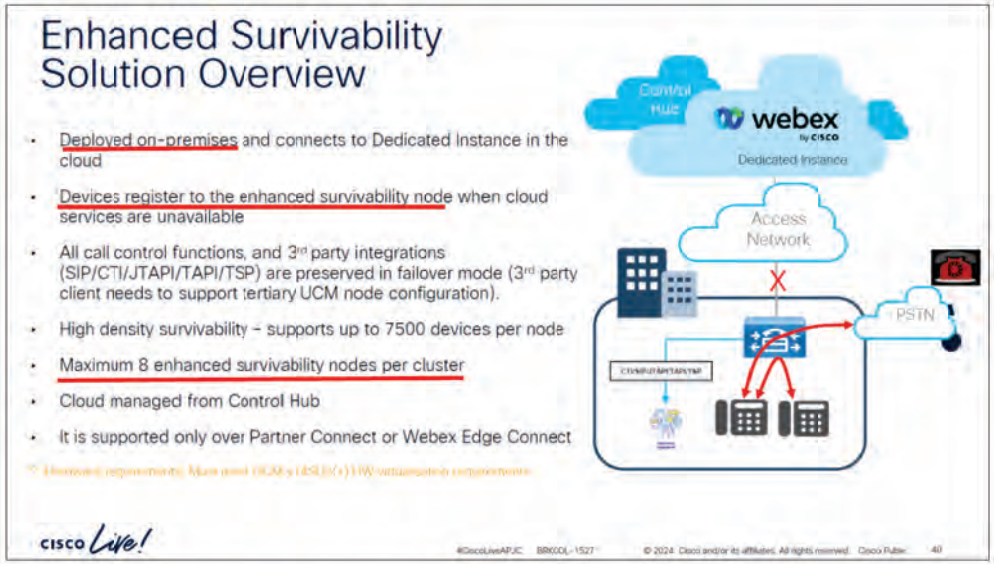
Source: https://help.webex.com/en-us/article/nk1shtj/Get-started-with-Webex-Calling.



Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability.

	 Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKCOL-2993.pdf. To extent the preamble is limiting, and it is not literally infringed, it is infringed under the doctrine of equivalents. A person skilled in the relevant art would also understand that calling over the PSTN is part of a "VoIP-capable network." SIP (Session Initiation Protocol) calls can go over the PSTN, as SIP trunking provides a connection from a company's Internet-based phone system to the PSTN. This is how Internet-based phones can call traditional landlines and mobile phones, and vice versa, and still have a "VoIP-capable network." A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial. *See* https://www.webex.com/what-is-voip.html ("VoIP can also be used to connect to the PSTN and vice versa. For instance, Webex Calling supports customers with the ability to select PSTN connectivity on a site-by-site basis. Webex customers can use any combination of Cisco Calling Plans, Cloud Connected PSTN, or Local Gateway-based PSTN across different sites.").
one or more VoIP client devices;	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network comprising one or more VoIP client devices. Webex Calling VoIP client devices can include users calling, for example, from the Webex App on a computer, or Webex phones and devices, including Cisco IP Phones 6800, 7800, 8800 Series desk phones and Cisco IP Conference Phones 7832 and 8832.

	Webex App (users) Webex App brings everyone together to do exceptional work: One, easy-to-use and secure app to meet, message and make calls. It supports various calling options and we've created several articles to help you make the most out of your calling experience, including how you can set up your own features: **Phones and devices (users)** Webex Calling further provides an integrated user calling experience with Webex devices, including Cisco IP Phones 6800, 7800, 8800 Series desk phones, Cisco IP Conference Phones 7832 and 8832, Cisco IP DECT 6800 Series, Cisco Desk Phone 9800 Series, and analog ATAs. The following articles help you with getting up and running on these devices: Source: https://help.webex.com/en-us/article/nk1shtj/Get-started-with-Webex-Calling. To the extent this claim element is not literally infringed, it is infringed under the doctrine of equivalents. The Cisco VoIP devices perform the same function of making VoIP calls in the same way by using the Internet and larger VoIP system infrastructure that allows calls to bridge to the PSTN when necessary and achieves the same result of connecting a VoIP call during an outage. A person skilled in the relevant art would understand that a "VoIP client device" is any hardware or software (*e.g.*, an "endpoint") that uses VoIP technology to make and receive calls and other communications over an IP network, such as the Internet. A "VoIP client device" can also connect to the PSTN through, *e.g.*, a VoIP gateway. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
two or more VoIP nodes forming an isolated cluster wherein the two or more VoIP nodes in the isolated cluster are in communication with one another; wherein each of the VoIP client devices communicates with at least one VoIP node;	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network comprising two or more VoIP nodes forming an isolated cluster that are in communication with one another wherein each of the VoIP client devices communicates with at least one VoIP node. Webex Calling includes Enhanced Survivability Nodes ("ESNs" or "VoIP nodes") as a part of a Unified Call Manager ("Unified CM") cluster. A Unified CM VoIP node deployed in the customer's data center (*i.e.*, on-premise and isolated) connects to the Dedicated Instance Unified CM cluster as an ESN for operation without the cloud or during network outage. A maximum of 8 ESNs can be deployed on-premise (*e.g.*, each in a building or location) for a single Unified CM cluster ("two or more VoIP nodes forming an isolated cluster"):



Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf; *see also* https://video.cisco.com/detail/video/6330308090112 (June 27, 2023 presentation).

> In Dedicated Instance, the Unified CM cluster's subscribers is deployed across the datacenter within a region, to provide high availability and Geo-redundancy. It allows the devices or client to failover to the subscriber in the other datacenter. But, if there is a network outage between your site and the Dedicated Instance cloud, the Enhanced Survivability Node that deploys within the site can handle the call control and routing functionalities until the connectivity restores. The Enhanced Survivability Node (ESN) provides the call control functionalities of a standard subscriber during an event of outage.

Should a customer's network outage or a cloud outage prevent users at that site(s) from connecting to Webex Calling Dedicated Instance, as shown above, the ESNs actively take over the call routing responsibility and VoIP client devices will communicate with at least one ESN ("each of the VoIP client devices communicates with at least one VoIP node."). The ESNs will communicate to process all intra-site, inter-site, inter-cluster and PSTN calls for the users on that site(s) during the outage.

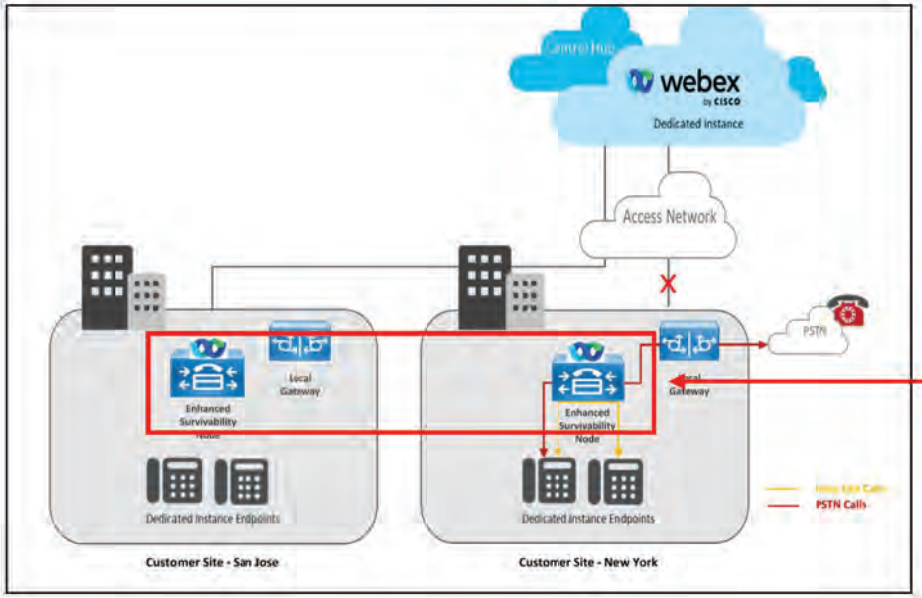
Call Routing

Configure the dial plan for routing intrasite, intersite, inter-cluster, and PSTN calls during the survivability event. In general, the ESN can route calls only for devices that are registered to it. All other calls need to be routed to the Local PSTN GW (configured in every site where ESN is deployed) and from there to the PSTN. Following are few scenarios explained:

- Phone 1 and Phone 2 registered to same ESN – The call is routed within the ESN.
- Phone 1 registered to ESN and Phone 2 registered to Dedicated Instance Unified CM cluster – The dial plan should route the calls from ESN to the local PSTN GW, from there to the DI Unified CM via PSTN. During the survivability event, dial plan should detect the call routing failure and re-route the calls through the local PSTN GW. The same should be applicable for incoming calls to ESN from DI Unified CM devices.
- Phone 1 registered to ESN and Phone 2 is a PSTN device: During survivability event, PSTN calls need to be routed to the local PSTN gateway. You must make sure that the dial plan has the capability to detect call routing failures and reroute the call through the available local PSTN gateway.

Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability; https://help.webex.com/en-us/article/nwb8iyx/How-to-Activate-Enhanced-Survivability.

ESNs can be deployed at each site or across sites, with a total of 8 ESN per Unified CM cluster and two or more ESN's forming an "isolated cluster," *e.g.*, not in an external datacenter:



Isolated Cluster (on-premise)

Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability.

A single ESN can support up to 7,500 endpoints during an outage. On information and belief, multiple ESNs can be deployed within a site (up to 8 per cluster) (*e.g.*, "two or more VoIP nodes forming an isolated cluster") to provide redundancy and share the load of devices within a large site or across multiple sites. Cisco Unified CM (which ESN is a part of) is designed for distributed deployments, allowing multiple nodes to work together. The local network devices (IP phones, gateways, etc.) can be configured to utilize both ESNs and/or, *e.g.*, a SIP trunk can be set up. Cisco's high availability preferred architecture recommends clustering on-premise.

Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf; *see also* https://help.webex.com/en-us/article/nwb8iyx/How-to-Activate-Enhanced-Survivability (confirming more than one ESN can be activated); https://www.cisco.com/c/en/us/td/docs/solutions/PA/overview/12x/clbpa12x.html.

During normal operation, the database replication is fully meshed between all servers including the isolated ESNs within the Unified CM cluster. The ESNs thus communicate with each other.

User Settings

During normal operation, the database replication is fully meshed between all the servers including the Enhanced Survivability Node within the Unified CM cluster. The static configuration data, because it is created through moves, adds, and changes, is always stored on the publisher and replicated one way from the publisher to each subscriber and enhanced survivability node in the cluster.

Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability.

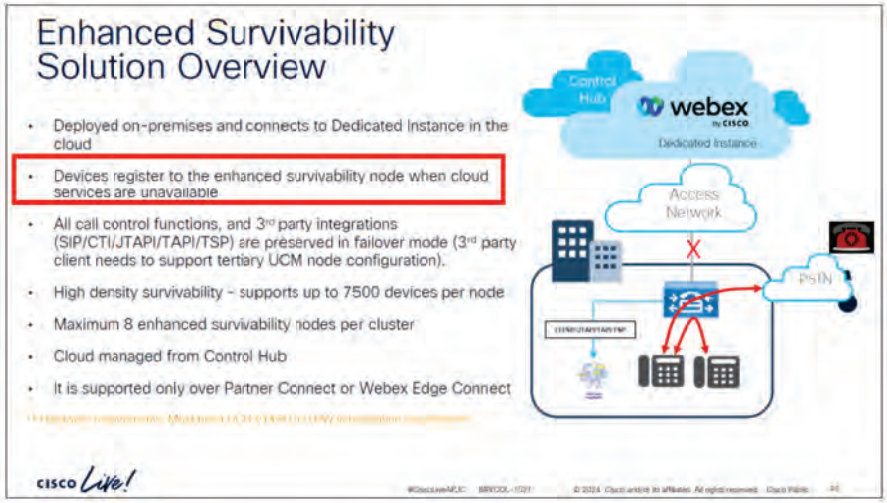
Call routing policies can also be implemented such that calls between VoIP clients over two ESN's are feasible during survivability. On information and belief, this could involve using SIP trunking, a static SIP route, or dial plan between ESNs so that calls can be routed across between ESNs (each with a "local SIP registry," *see infra*) at a large location, for example, and they can communicate directly to route calls.

Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability (ICT or "inter-cluster trunk" is feasible); *see also* https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Collaboration/hybrid/AltDesigns/PA-WbxCallDI.pdf.

MeshDynamics asserts that these claim elements are software limitations. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If these claim elements are not literally infringed, they are infringed under the doctrine of equivalents. Cisco's Webex Calling with Enhanced Survivability performs the same functions of forming an isolated cluster of nodes across sites that communicate with VoIP devices in the same way by utilizing multiple on-premise servers and achieves the same result of an on-premise (not in the cloud and without an external SIP server) VoIP network for maintaining device and endpoint communication. Enhanced Survivability allows for continued communication between devices and a VoIP network without an external SIP server for communications. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed elements are insignificant or insubstantial because Enhanced Survivability creates and maintains a VoIP network without an external SIP server. The ESNs in a cluster are fully meshed and replicated via Unified CM with the registration information. A single isolated ESN can handle the VoIP communications for a single site without any external server or cloud connectivity. ESNs can be set up to communicate directly or through, *e.g.*, a local gateway. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

A person skilled in the relevant art would also understand that calling over the PSTN is part of a "VoIP-capable network." SIP (Session Initiation Protocol) calls can go over the PSTN, as SIP trunking provides a connection from a

	company's Internet-based phone system to the PSTN. This is how Internet-based phones can call traditional landlines and mobile phones, and vice versa, and still have a "VoIP-capable network." A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
wherein each of the VoIP nodes further comprises a local SIP registry built by exchanging SIP information with the remaining VoIP nodes in the isolated cluster;	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network wherein each of the VoIP nodes further comprises a local SIP registry built by exchanging SIP information with the remaining VoIP nodes in the isolated cluster. ESNs act as a backup solution to maintain call control and essential services during network or cloud service disruptions. Devices register to the ESN when the cloud is not available. Each ESN can support up to 7,500 device registrations, and up to 8 ESNs can be enabled for each Dedicated Instance Unified CM cluster. When a cloud connection fails, supported Webex Calling endpoints switch to survivability mode and register with the local ESN. Performing a SIP registration means a SIP phone or client registers its current location (*e.g.*, IP address) with the ESN, allowing the network to know where to send incoming calls to that user.  Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf. Each ESN thus acts as a "local SIP registry" during survivability events. During a network outage, registrations fall to the ESN instead of the main Unified CM cluster or the Webex cloud. This allows for continued internal and external calling within the survivability site without an external SIP server. Source: https://help.webex.com/en-us/article/ntoo2ocb/Enhanced-Survivability-prerequisites. During normal operation, the database replication is fully meshed between all servers including the ESNs within the Unified CM cluster. The ESNs thus communicate with each other and build the "local SIP registry" by communication

with other ESNs (*e.g.*, "each of the VoIP nodes further comprises a local SIP registry built by exchanging SIP information with the remaining VoIP nodes in the isolated cluster"). The ESNs communicate to ensure updated information for call routing (*e.g.*, for local dial plans or SIP trunks):

> ## User Settings
>
> During normal operation, the database replication is fully meshed between all the servers including the Enhanced Survivability Node within the Unified CM cluster. The static configuration data, because it is created through moves, adds, and changes, is always stored on the publisher and replicated one way from the publisher to each subscriber and enhanced survivability node in the cluster.

Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability.

During a survivability event, each ESN stores all of the CDR/CMR data locally:

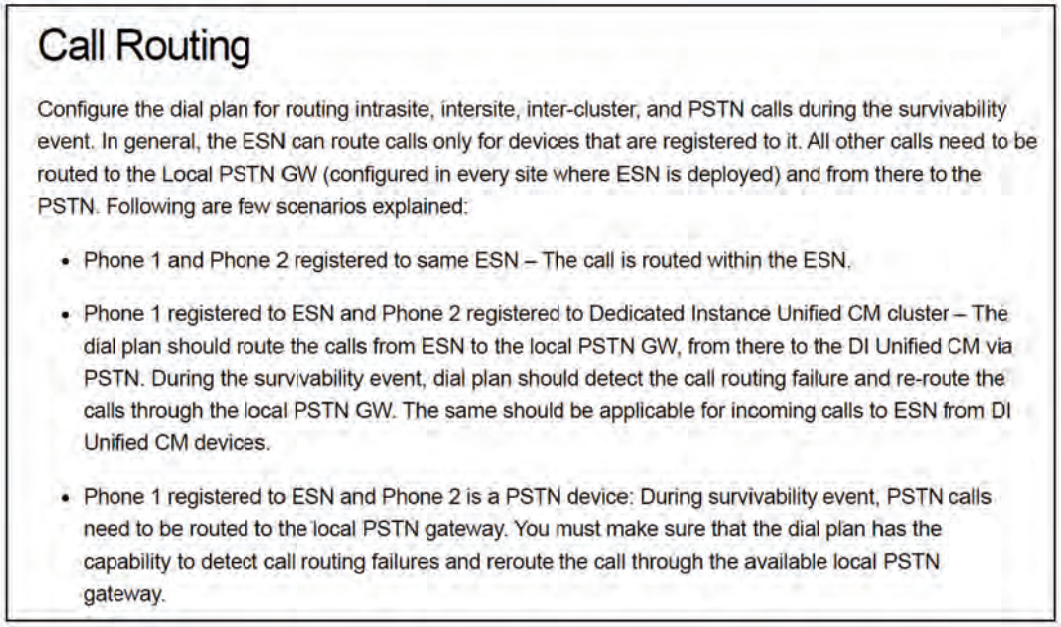
> ## CDR
>
> During the survivability event, the Enhanced Survivability Node stores all the CDR/CMR data locally. When the connectivity is restored, the data will be synced back to the Dedicated Instance Unified CM Publisher. The amount of data that can be stored is based on disk size of then Enhanced Survivability Node. The maximum disk allocation space that can set for CDR is **3328 MB**. This can be with small to large CDR file size based on the CDR interval that is configured. The purge happens based on:

Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability.

This data includes all of the SIP information sent and received about the call between sites/ESNs, including when the call was connected and ended (*i.e.*, "local SIP registry built by exchanging SIP information"):

> **Understanding CDR Data**
>
> Call detail records (CDR) detail the called number, the number that placed the call, the date and time that the call was started, the time that it connected, and the time that it ended. Call management records (CMRs, or diagnostic records) detail the jitter, lost packets, the amount of data sent and received during the call, and latency. CDR data comprises CDRs and CMRs collectively. A single call can result in the generation of several CDRs and CMRs. Cisco CallManager records information regarding each call in CDRs and CMRs. CDRs and CMRs, known collectively as CDR data, serve as the basic information source for CAR.
>
> You can set service parameters in Cisco CallManager Administration to establish the amount of disk space to allocate to CDRs. For more information, refer to the *Cisco CallManager System Guide*.

	Source: https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/4_2_1/ccmsrvs/sscar.html; https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/callReportingBillingAdmin/14/cucm_b_reporting-billing-administration-guide-14/cucm_b_reporting-and-billing-administration-guide_chapter_01010.html. Call routing policies can also be implemented such that calls between VoIP clients over two ESN's are feasible during survivability. On information and belief, this could involve using SIP trunking between ESNs so that calls can be routed across between ESNs (each with a "local SIP registry") at a large location, for example, if necessary. In this way, two ESNs exchange SIP information to further build the "local SIP registry." Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability (ICT or "inter-cluster trunk" is feasible); *see also* https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Collaboration/hybrid/AltDesigns/PA-WbxCallDI.pdf. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling with Enhanced Survivability performs the same function of building a local SIP registry in the same way by replicating and exchanging SIP information to connect calls and achieves the same result of operating without an external server to maintain endpoint communications during an outage. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the nodes maintain SIP information and use this information to connect endpoints at different sites or locations. The ESNs function as autonomous SIP servers during an outage. The ESNs at each site handles the call signaling from the local phone to the local gateway and thus exchanges SIP signaling through the gateway to the PSTN. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
wherein a first VoIP client device in communication with a first VoIP node establishes a communication with a second VoIP device in communication with a second VoIP node using	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network wherein a first VoIP client device in communication with a first VoIP node establishes a communication with a second VoIP device in communication with a second VoIP node using the local SIP registries of the first VoIP node and the second VoIP node. For example, a "first VoIP client device," *e.g.*, Cisco Phone 1 registered and in communication with an ESN, can establish a call with a "second VoIP client device," *e.g.*, Cisco Phone 2 registered to another ESN, via the PSTN. ESNs can route calls for devices that are registered to it during a survivability event, including routing calls within the ESN and from the ESN to the local PSTN gateway. Both ESNs comprise "VoIP nodes" with "local SIP registries" as discussed above, which are used to connect the call.

the local SIP registries of the first VoIP node and the second VoIP node.	 Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability. A single ESN can support up to 7,500 endpoints during an outage. On information and belief, multiple ESNs can be deployed within a site (up to 8 per cluster) (*e.g.*, "two or more VoIP nodes forming an isolated cluster") to provide redundancy and share the load of devices within a large site or across multiple sites. Cisco Unified CM (which ESN is a part of) is designed for distributed deployments, allowing multiple nodes to work together. The local network devices (IP phones, gateways, etc.) can be configured to utilize both ESNs and/or *e.g.*, a SIP trunk can be set up. Cisco's high availability preferred architecture recommends clustering on-premise. Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf; *see also* https://help.webex.com/en-us/article/nwb8iyx/How-to-Activate-Enhanced-Survivability (confirming more than one ESN can be activated); https://www.cisco.com/c/en/us/td/docs/solutions/PA/overview/12x/clbpa12x.html. Call routing policies can also be implemented such that calls between VoIP clients over two ESN's are feasible during survivability. On information and belief, this could involve using SIP trunking between ESNs so that calls can be routed across between ESNs (each with a "local SIP registry") at a large location, for example, if necessary. In this way, two ESNs and their client devices can connect and establish communication to meet this claim element.

	Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability (ICT or "inter-cluster trunk" is feasible); *see also* https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Collaboration/hybrid/AltDesigns/PA-WbxCallDI.pdf. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling with Enhanced Survivability performs the same function of establishing a communication between two endpoints in a VoIP network in the same way by using SIP information at each node, replicated across a Unified CM cluster, and achieves the same result establishing a VoIP call between to endpoints. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Webex Calling with Enhanced Survivability will establish a connection between endpoints using on-premise nodes and their SIP registries. A single "ESN" at a site may be multiple virtual servers or nodes. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial. A person skilled in the relevant art would also understand that calling over the PSTN is part of a "VoIP-capable network." SIP (Session Initiation Protocol) calls can go over the PSTN, as SIP trunking provides a connection from a company's Internet-based phone system to the PSTN. This is how Internet-based phones can call traditional landlines and mobile phones, and vice versa, and still have a "VoIP-capable network." A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 2	
The VoIP-capable network of claim 1, wherein the local SIP registries of the isolated VoIP nodes are updated as the VoIP nodes and the VoIP client devices begin communication with the isolated cluster and end communication with the isolated cluster	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein the local SIP registries of the isolated VoIP nodes are updated as the VoIP nodes and the VoIP client devices begin communication with the isolated cluster and end communication with the isolated cluster. During a survivability event, each ESN stores all of the CDR/CMR data locally: **CDR** During the survivability event, the Enhanced Survivability Node stores all the CDR/CMR data locally. When the connectivity is restored, the data will be synced back to the Dedicated Instance Unified CM Publisher. The amount of data that can be stored is based on disk size of then Enhanced Survivability Node. The maximum disk allocation space that can set for CDR is **3328 MB**. This can be with small to large CDR file size based on the CDR interval that is configured. The purge happens based on:

	Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability. This data includes all of the SIP information sent and received about the call between sites/ESNs, including when the call was connected and ended (*i.e.*, "local SIP registry built by exchanging SIP information"), and is updated as the devices begin and end communication: **Understanding CDR Data** Call detail records (CDR) detail the called number, the number that placed the call, the date and time that the call was started, the time that it connected, and the time that it ended. Call management records (CMRs, or diagnostic records) detail the jitter, lost packets, the amount of data sent and received during the call, and latency. CDR data comprises CDRs and CMRs collectively. A single call can result in the generation of several CDRs and CMRs. Cisco CallManager records information regarding each call in CDRs and CMRs. CDRs and CMRs, known collectively as CDR data, serve as the basic information source for CAR. You can set service parameters in Cisco CallManager Administration to establish the amount of disk space to allocate to CDRs. For more information, refer to the *Cisco CallManager System Guide*. Source: https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/4_2_1/ccmsrvs/sscar.html; https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/callReportingBillingAdmin/14/cucm_b_reporting-billing-administration-guide-14/cucm_b_reporting-and-billing-administration-guide_chapter_01010.html. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling with Enhanced Survivability performs the same function of updating the local SIP registry and logs in the same way by exchanging the SIP information from the call and achieves the same result of an updated local SIP registry and logs using the information from the call. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the local SIP registries and logs of each gateway are updated with call information. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 3	
The VoIP-capable network of claim 1, wherein updates to the local SIP registry of a VoIP node are communicated to	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein updates to the local SIP registry of a VoIP node are communicated to remaining VoIP nodes in the isolated cluster by broadcasting one or more information packets containing local SIP registry information of the VoIP node.

remaining VoIP nodes in the isolated cluster by broadcasting one or more information packets containing local SIP registry information of the VoIP node.	Information in networks is carried in packets. During normal operation, the database replication is fully meshed between all servers including the ESNs within the Unified CM cluster. The ESNs in a cluster thus communicate with each other and update the "local SIP registry" by "by broadcasting one or more information packets containing local SIP registry information of the VoIP node." **User Settings** During normal operation, the database replication is fully meshed between all the servers including the Enhanced Survivability Node within the Unified CM cluster. The static configuration data, because it is created through moves, adds, and changes, is always stored on the publisher and replicated one way from the publisher to each subscriber and enhanced survivability node in the cluster. Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling performs the same function of updating local SIP registries in the same way by database replication and achieves the same result of an updated local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Unified CM shares the directory across nodes to enable VoIP calls. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 4	
The VoIP-capable network of claim 1, wherein the local SIP registry of a VoIP node is updated according to information received from another VoIP node in the isolated cluster in special information packets that each contain	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein the local SIP registry of a VoIP node is updated according to information received from another VoIP node in the isolated cluster in special information packets that each contain local SIP registry information of another VoIP node Information in networks is carried in packets. During normal operation, the database replication is fully meshed between all servers including the ESNs within the Unified CM cluster. The ESNs in a cluster thus communicate with each other and update the "local SIP registry" by "by broadcasting one or more information packets containing local

local SIP registry information of another VoIP node.	SIP registry information of the VoIP node." The "special information packets" including the packets with SIP information. **User Settings** During normal operation, the database replication is fully meshed between all the servers including the Enhanced Survivability Node within the Unified CM cluster. The static configuration data, because it is created through moves, adds, and changes, is always stored on the publisher and replicated one way from the publisher to each subscriber and enhanced survivability node in the cluster. Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling performs the same function of updating the local SIP registry in the same way by database replication and achieves the same result of an updated local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Unified CM shares the directory across nodes to enable VoIP calls. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 7	
The VoIP-capable network of claim 1, further comprising means of connecting the isolated cluster to an external network, wherein upon connection to an external network, the SIP registry of an external SIP server connected to the external network is updated to include SIP registry	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, further comprising means of connecting the isolated cluster to an external network, wherein upon connection to an external network, the SIP registry of an external SIP server connected to the external network is updated to include SIP registry information from the VoIP node. When the outage is over, and network and cloud connectivity restored, the ESN will send all call activity and logs to the Unified CM publisher:

information from the VoIP node.	**CDR** During the survivability event, the Enhanced Survivability Node stores all the CDR/CMR data locally. When the connectivity is restored, the data will be synced back to the Dedicated Instance Unified CM Publisher. The amount of data that can be stored is based on disk size of then Enhanced Survivability Node. The maximum disk allocation space that can set for CDR is 3328 MB. This can be with small to large CDR file size based on the CDR interval that is configured. The purge happens based on: Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability. The Dedicated Instance Unified CM publisher updates SIP information and is integrated with the Webex cloud when there is connectivity: Webex Calling now includes a dedicated cloud instance option based on the Cisco Unified Communications Manager architecture. Dedicated Instance is integrated with Webex Calling and takes advantage of Webex platform services, to bring centralized administration as well as applicable cloud innovation, developed anywhere on the Webex platform, to enhance the calling experience. Dedicated Instance also supports older Cisco endpoints, or existing integrations that are part of critical business workflows. Source: https://help.webex.com/en-us/article/dk3o5r/Introduction-to-Dedicated-Instance; *see also* https://help.webex.com/en-us/article/2vpf1/Dedicated-Instance-for-Webex-Calling---base-configuration. During normal operation, the database replication is fully meshed between all servers including the ESNs within the Unified CM cluster. **User Settings** During normal operation, the database replication is fully meshed between all the servers including the Enhanced Survivability Node within the Unified CM cluster. The static configuration data, because it is created through moves, adds, and changes, is always stored on the publisher and replicated one way from the publisher to each subscriber and enhanced survivability node in the cluster. Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability. To the extent this is considered an element under 35 U.S.C. §112 (¶ 6), in accordance with P.R. 3-1(c), the identity of the structure(s), act(s), or material(s) in the Accused Instrumentality that performs the claimed function include, *e.g.*, ESNs use the communication protocol HTTPs to connect to the Unified CM in the cloud. MeshDynamics's investigation into Cisco's proprietary algorithms remains ongoing and MeshDynamics will supplement or amend its P.R. 3-1(c) identification following discovery and/or claim construction.

	Source: https://help.webex.com/en-us/article/ntoo2ocb/Enhanced-Survivability-prerequisites (TCP port 443). MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling with Enhanced Survivability performs the same function of connecting to the external network to update SIP information and logs in the same way by connecting to the Unified CM when the connectivity is restored and achieves the same result of providing updated information to the external SIP server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the external SIP server is updated with call information that can be used, *e.g.*, to verify the correctness of SIP information. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 8	
The VoIP-capable network of claim 1 wherein said nodes comprise mesh nodes.	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein said nodes comprise mesh nodes. During operation, the database replication is fully meshed between all servers including the ESNs within the Unified CM cluster (each ESN comprising a "mesh node" as a part of the mesh). The ESNs thus communicate with each other and other VoIP nodes within the Unified CM cluster and comprise "mesh nodes." **User Settings** During normal operation, the database replication is fully meshed between all the servers including the Enhanced Survivability Node within the Unified CM cluster. The static configuration data, because it is created through moves, adds, and changes, is always stored on the publisher and replicated one way from the publisher to each subscriber and enhanced survivability node in the cluster. Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability; *see also* Exhibit 3 (demonstrating the Unified CM clusters and communication/replication within a cluster independent of the Webex cloud, incorporated herein).

	MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling with Enhanced Survivability performs the same function of completing VoIP calls without an external server in the same way using nodes in communication with each node and exchanging information locally and achieves the same result a local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Cisco's documents refers to the operation and structure of nodes as "fully meshed." A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 9	
The VoIP-capable network of claim 8 wherein said mesh nodes provide VoIP optimized services within said mesh nodes	Cisco's Webex, *e.g.*, Webex Calling, is a VoIP-capable network, in addition to the elements of claim 1 and claim 8 as shown above, wherein said mesh nodes provide VoIP optimized services within said mesh nodes. Cisco's documentation confirms that the ESNs provide VoIP optimized services during an outage, including preserving all call control functions and third party integrations: • All call control functions, and 3rd party integrations (SIP/CTI/JTAPI/TAPI/TSP) are preserved in failover mode (3rd party client needs to support tertiary UCM node configuration). Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf. User facing features ("VoIP optimized services") are available within the ESNs: User-facing features are any features that can be enabled or disabled by pressing buttons on the phone and include the following: • Call Forward All (CFA) • Privacy Enable or Disable • Do Not Disturb(DND) Enable or Disable • Cisco Extension Mobility Login • Hunt-group Login or Logout • Device Mobility • CTI CAPF status for end users and application users.

	Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Calling with Enhanced Survivability performs the same function of completing VoIP calls without an external server in the same way using nodes in communication with each node and exchanging information locally and achieves the same result a local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Cisco's documents confirm that this network provides benefits and enterprise-calling capabilities. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Exhibit 3 – U.S. Patent No. 8,477,762 (Cisco Webex with Calling in Webex App (Unified CM))

Cisco Systems, Inc. ("Cisco") has and continues to make, use, sell, offer for sale, and/or import the Cisco Webex VoIP Network, including but not limited to Cisco's Webex and Calling in Webex App (Unified CM) with related software and hardware (the "Cisco Accused Products," *see* Exhibit 7), and has infringed and infringes at least Claims 1-4, 8-9, 10, 12-13, and 15-17 (the "Asserted Claims") of U.S. Patent No. 8,477,762 (the "'762 Patent").[1]

Cisco has and continues to infringe (literally and/or under the doctrine of equivalents), directly and/or through subsidiaries, agents, representatives, or intermediaries, one or more claims of the '762 Patent by making, using, testing, supplying, causing to be supplied, importing, selling, and/or offering for sale in the United States the Cisco Accused Products.

Cisco directly infringes and has infringed under 35 U.S.C. § 271(a) by making, using, selling, offering for sale and importing the Cisco Accused Products. Cisco further directly infringes and has infringed by testing, setting up, and using the Cisco Webex VoIP Network on Cisco's campuses and locations throughout the United States,[2] and/or assisting customers in setting up and servicing their Cisco Webex VoIP Networks. On information and belief, Cisco has partnered with several customers to set up an infringing Cisco Webex VoIP Network in the United States.[3]

Cisco indirectly infringes and has infringed under 35 U.S.C. § 271(b) by providing specific guidance and instructions to its customers and end users on how to infringe the '762 Patent and make and use the infringing Cisco Webex VoIP Network. Specifically, Cisco's Preferred Architecture guides, deployment guides, Technical Assistance Center, Cisco Tech Talks, technical support, Cisco Community, presentations, and technical documentation on Cisco's website identified in the chart *infra* provide guidelines for the deployment of an infringing Cisco Webex VoIP Network. These guides and instructions specifically teach and describe each and every claim element of Claims 1-4, 8-9, 10, 12-13, and 15-17 as demonstrated

---

[1] The identified Accused Products also include Cisco's products, services, and systems that are considered sold or related to the infringement in the United States and subject to a reasonable royalty according to the Federal Circuit's decisions in *Carnegie Mellon Univ. v. Marvell Tech. Group. Ltd.*, 807 F.3d 1283 (Fed. Cir. 2015), *Cal. Inst. of Tech. v. Broadcom Ltd.*, 25 F.4th 976 (Fed. Cir. 2022), and *Brumfield v. IBG LLC*, 97 F.4th 854 (Fed. Cir. 2024).

[2] *See, e.g.*, https://blog.webex.com/collaboration/behind-the-scenes-how-cisco-it-migrated-84000-users-to-webex-calling/ ("With Webex Calling, employees are no longer tied to the corporate WAN. Phones can now be deployed anywhere with internet access — as demonstrated at the Cisco GSX conference, where a temporary network was set up using hotel Wi-Fi, avoiding costly LAN build-outs.").

[3] *See, e.g.*, https://blog.webex.com/customer-stories/why-cloud-calling-is-a-gamechanger-for-broadcom/; https://blog.webex.com/customer-stories/how-att-and-webex-power-hybrid-work-with-world-class-cloud-calling/.

infra, including the necessary components to make and use the infringing Cisco Webex VoIP Network, and the infringing configuration and operation of Webex, Unified CM clusters, Intercluster Lookup Service ("ILS"), and other software and hardware that comprise the infringing Cisco Webex VoIP Network. These guides and instructions were published and distributed by Cisco for its customers for the sole purpose to instruct and encourage its customers to purchase the Cisco components to make and use the infringing Cisco Webex VoIP Network (and directly infringe literally and/or under the doctrine of equivalents). Cisco has had knowledge of the '762 Patent since 2009 when Cisco executives met with MeshDynamics to discuss partnering opportunities and the application that would result in the '762 Patent. MeshDynamics further put Cisco on actual notice of its infringement by its making, using, selling, offering for sale and importing the Cisco Accused Products that comprise the Cisco Webex VoIP Networks (including "Mesh" functionality, such as Unified CM clusters and ILS) in 2022. Cisco has knowingly and intentionally induced its customers to infringe the '762 Patent, or in the alternative was willfully blind to the '762 Patent and the infringement, following the MeshDynamics meeting in 2009.

Cisco further indirectly infringes and has infringed under 35 U.S.C. § 271(c) by supplying the components used in the infringing Cisco Webex VoIP Network, with knowledge of its infringing use (as discussed *supra*) and without substantial non-infringing uses. Further, the Cisco Accused Products were designed specifically to be used in a manner that infringes the '762 Patent. Cisco Accused Products come enabled as an infringing product, are particularly suited for isolated on-premise configuration and operation, and Cisco provides specific instructions and guides on how to make and use the Cisco Webex VoIP Network using the Cisco Accused Products. As a result of Cisco's selling and/or offering for sale of the Cisco Accused Products to other entities, the other entities use these products for their intended purpose and according to their instructions with the result that such entities directly infringe the '762 Patent, literally or under the doctrine of equivalents, for the reasons stated *infra*. Cisco's Accused Products are specially made and adapted for this use in an infringing manner, are not staple articles of commerce, and do not have substantial non-infringing uses.

MeshDynamics asserts that the Cisco Accused Products literally infringed and continue to infringe the Asserted Claims of the '762 Patent. With respect to any claim limitation that may be found not to be literally infringed, MeshDynamics contends in the alternative that Cisco Accused Products infringed such claim limitations under the doctrine of equivalents and that any claim element not found to be literally met is equivalently met because any difference between the claim limitation and Cisco Accused Products is not a substantial difference. Accordingly, MeshDynamics contends that if any Cisco Accused Products is found not to have infringed any Asserted Claims literally it is nevertheless embodied by Cisco Accused Products under an operative doctrine of equivalents test (*e.g.*, function-way-result or insubstantial difference).

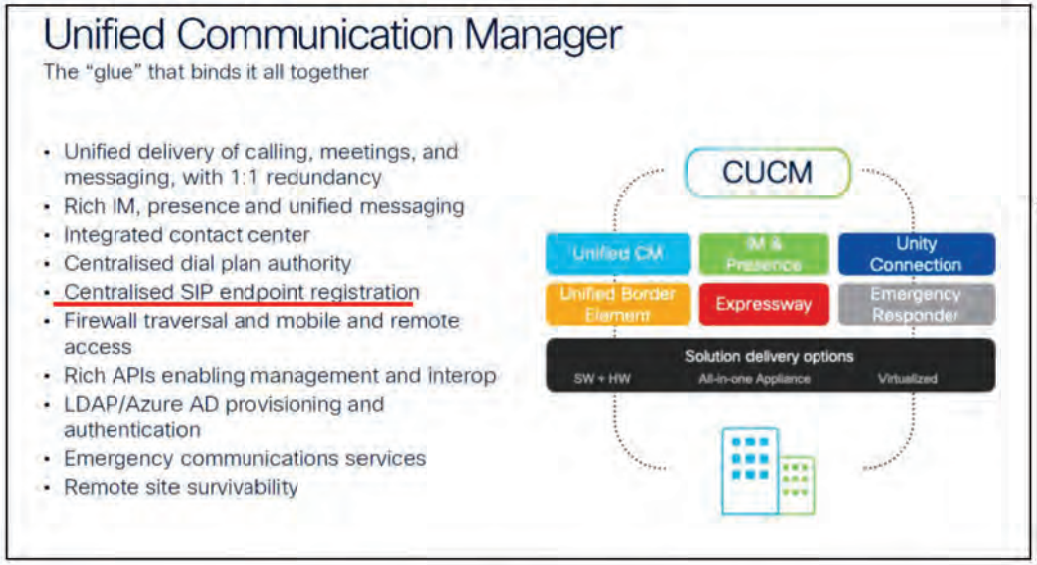
The below chart presents MeshDynamics's preliminary infringement analysis of Cisco Accused Products based solely on public information. MeshDynamics has not received any discovery from Cisco, including any confidential information or source code demonstrating the operation and structure of the Cisco Accused Products. All information contained in this disclosure is the result of publicly available information regarding the Cisco Accused Products. Based on these circumstances, MeshDynamics presents these infringement allegations reflecting its analysis of the facts presently known to it. To the best of MeshDynamics's knowledge, information, and belief, formed after an inquiry that is reasonable under the circumstances, the information contained in this disclosure is correct.

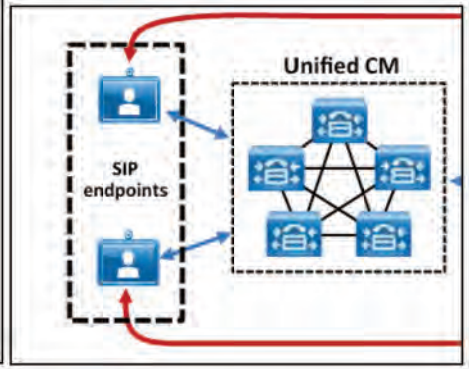
Certain information about Cisco Accused Products is not available without discovery, such as proprietary source code, documents, and deposition testimony, from Cisco. Accordingly, MeshDynamics reserves the right to supplement and/or amend this infringement contention claim chart as new information becomes available and as MeshDynamics has the opportunity to review Cisco document productions, including information related to the implementation of Cisco Accused Products, relationships with other parties who participated or contributed to the operation of Cisco Accused Products, and/or elements of Cisco Accused Products that cannot be fully examined based solely on publicly available information. Infringement investigations are ongoing, and MeshDynamics anticipates that additional facts and relevant documents will be uncovered and disclosed that create cause for supplementation and/or amendment.

Claim 1	Cisco Webex (*e.g.*, Cisco Calling in Webex App (Unified CM))
A VoIP-capable network comprising:	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a Voice over Internet Protocol-capable network in which each client or device can communicate with multiple other clients or devices over the Internet using, *e.g.*, a computer or a phone. Voice over Internet Protocol (VoIP) transmits sound as data over the internet. This lets you talk over the internet without using a phone. Webex uses VoIP so users can call into a meeting using a computer. With a paid plan, you can also call into a meeting with your phone. Source: https://www.webex.com/what-is-voip.html. The Calling in Webex App solution registers the Webex App directly to its Unified Communications Manager (Unified CM) call control environment. The Webex App connects to the Webex cloud to get its service configuration but it also reads configurations from the Unified CM environment to provide specific calling functionality to users, including Intercluster Lookup Service (ILS) in a multi-cluster environment.

	Source: https://help.webex.com/en-us/article/nj8v6wg/Deployment-guide-for-Calling-in-Webex-App-(Unified-CM). In addition, when a connection to the Webex cloud is lost, Calling in Webex App (Unified CM) still works for users who are already signed in, as long as the call type is a Unified CM call and goes through Unified CM infrastructure. **Connection is lost to the Webex cloud** If https://status.webex.com or the health checker show a Webex App cloud full or partial outage, Calling in Webex App (Unified CM) still works for users who are already signed in, as long as the call type is a Unified CM call and goes through Unified CM infrastructure. Source: https://help.webex.com/en-us/article/nj8v6wg/Deployment-guide-for-Calling-in-Webex-App-(Unified-CM). ILS allows a network to further create networks of remote (*e.g.*, "isolated") Unified CM clusters. ILS allows joining additional clusters to the VoIP network. ILS facilitates communication between different clusters, allowing users to dial each other directly using their URIs. Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1_SU7/cucm_b_system-configuration-1151su7-1151su8/cucm_b_system-configuration-guide-1151su1_chapter_011001.html.
one or more VoIP client devices;	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network comprising one or more VoIP client devices. Users are able to directly make calls in the Webex App from their desktop computer or mobile phone (*e.g.*, "one or more VoIP client devices"). **Users** This solution enhances the calling experience for end users, allowing them to directly make calls in Webex App through your Unified CM environment, use midcall features, and control their desk phone from Webex App. When dialing from Webex App, users can use the same dial strings or prefixes as they do on their desk phones; Webex App functions like any other desk phone registered to your Unified CM. Unified CM calls that are established in Webex App use the configuration that's in place for your Unified CM deployment (such as location, bandwidth settings, point to point media, and so on).

	Calling features in Webex App This integration provides the following feature set in Webex App for desktop (Windows and Mac) and for mobile (Android, iPad, and iPhone). Wherever possible, the feature listings in this table include a link to a relevant help article for end users. See **Audio and video calls** for more general information on making a call. See **Supported calling options** for a feature comparison table for end users. Source: https://help.webex.com/en-us/article/nj8v6wg/Deployment-guide-for-Calling-in-Webex-App-(Unified-CM); see also https://help.webex.com/en-us/article/qkwt4j/Supported-devices-for-Webex-Calling.
two or more VoIP nodes forming an isolated cluster wherein the two or more VoIP nodes in the isolated cluster are in communication with one another; wherein each of the VoIP client devices communicates with at least one VoIP node;	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network comprising two or more VoIP nodes forming an isolated cluster that are in communication with one another, and wherein each of the VoIP client devices communicates with at least one VoIP node. VoIP client devices using the Calling in Webex App use the on-premise Unified CM nodes, which can operate in isolation without the need to connect to an external datacenter, for calling, including if the cloud connection is lost. **Connection is lost to the Webex cloud** If https://status.webex.com or the health checker show a Webex App cloud full or partial outage, Calling in Webex App (Unified CM) still works for users who are already signed in, as long as the call type is a Unified CM call and goes through Unified CM infrastructure. Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/ucmcalling/unified-cm-wbx-teams-deployment-guide/unified-cm-wbx-teams-deployment-guide_chapter_0101.html. Unified CM nodes are a networked cluster of remote, isolated nodes (*e.g.*, "two or more VoIP nodes forming an isolated cluster"), including when not connected to the cloud, and the nodes communicate with one another to work as a single call processing unit. This on-premises SIP-based call control system (*e.g.*, Unified CM) manages the SIP registration of VoIP devices using the Webex App and the devices communicate with at least one Unified CM node.





Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf; https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf; *see also* https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/11x/116/collbcvd/control.html ("Unified CM supports the concept of clustering. The Unified CM architecture enables a group of server nodes to work together as a single call processing entity. This grouping of server nodes is known as a cluster.").

Clusters

Clusters provide a mechanism for distributing call processing, presence status, and database replication among multiple servers. They provide transparent sharing of resources and features, and enable system scalability.

Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/install/15/cucm_b_install-guide-cucm-imp-15/cucm_m_planning-the-installation.html.

Using the Intercluster Lookup Service (ILS), the network can create a multi-cluster network of remote Unified CM clusters that are in communication and share data (*e.g.*, "two or more VoIP nodes forming an isolated cluster wherein the two or more VoIP nodes in the isolated cluster are in communication with one another"). ILS is designed to create a

network of interconnected Unified CM clusters, allowing Webex App users to find and dial each other using SIP URIs even if they are on different clusters and even without the cloud.

> The Cisco Intercluster Lookup Service (ILS) makes it easy to create a multi-cluster network of remote Cisco Unified Communications Manager clusters that share data.
>
> ILS eliminates the need for an administrator having to configure connections between clusters manually. Once you have ILS configured on a hub cluster, you can connect new clusters by enabling ILS on the new cluster and pointing the new cluster to an existing hub. ILS connects the clusters automatically and lets both clusters know the topology of the larger ILS network.

Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU4/systemConfig/cucm_b_system-configuration-guide-1251su4/cucm_m_intercluster-lookup-service.pdf; *see also* https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/11x/116/collbcvd/control.html ("In a multi-cluster deployment, interconnect all the individual Unified CM clusters through SIP trunks.").

> Each cluster in an ILS network exchange and update messages, called peer info vectors, that are designed to inform remote clusters of the status of each cluster in the network. The update messages contain information about the known clusters in the network, including:
>
> - Cluster IDs
> - Peer IDs for the publisher
> - Cluster descriptions and versions
> - Fully Qualified Domain Name (FQDN) of the host
> - IP addresses and host names for the cluster nodes that have ILS activated

Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1_SU7/cucm_b_system-configuration-1151su7-1151su8/cucm_b_system-configuration-guide-1151su1_chapter_011001.html.

ILS allows Webex App users in one cluster to call users in another using SIP URI. SIP URI replication using ILS in Unified CM enables different clusters to share and resolve SIP URI addresses—such as user@example.com—across the enterprise, even when those users are registered to different clusters. ILS advertises SIP URIs, while the Unified

CM nodes manage the actual call routing or SIP registration. To dial a SIP URI from one cluster to another, a separate SIP trunk can be configured that routes the call back to the correct cluster.

We can call ILS – Intercluster Lookup Service as Voice Routing Protocol because it behaves like dynamic routing protocol. Just like advertising the local route from one router to another, ILS will advertise the URIs between different CUCM cluster.

Each CUCM cluster node advertises its URIs and "**SIP route string**" to its neighbor's (or Hubs). CUCM cluster later creates a table with URIs and associated SIP route string. Finally, SIP route strings are routed through SIP route patterns.

Source: https://community.cisco.com/t5/collaboration-blogs/cucm-intercluster-lookup-service-ils-configuration-guide-based/ba-p/3358335.

INTER-Cluster URI (URI Dialing across cluster):

To enable intercluster routing of directory URIs, **Unified CM can be provisioned to exchange directory URI catalogs with other clusters through the Intercluster Lookup Service (ILS).** Each cluster configured to exchange directory URI catalogs with other clusters advertises all locally configured directory URIs in a single directory URI catalog together with a location attribute, **the SIP route string**. This location attribute in multi-cluster environments is used to direct calls for directory URIs to the correct cluster when the host portion of the directory URI cannot be used to deterministically route the SIP request. This, for example, is the case when a flat URI scheme such as *<user>@example.com* is use. The host portion "example.com" does not uniquely identify the remote Unified CM cluster that hosts a given URI.

Basically, every cluster would have a catalogue(table) of Directory URI's. Using ILS each and every cluster would share this catalogue with a local attribute i.e SIP ROUTE STRING.

- ***SIP Trunk configuration:***

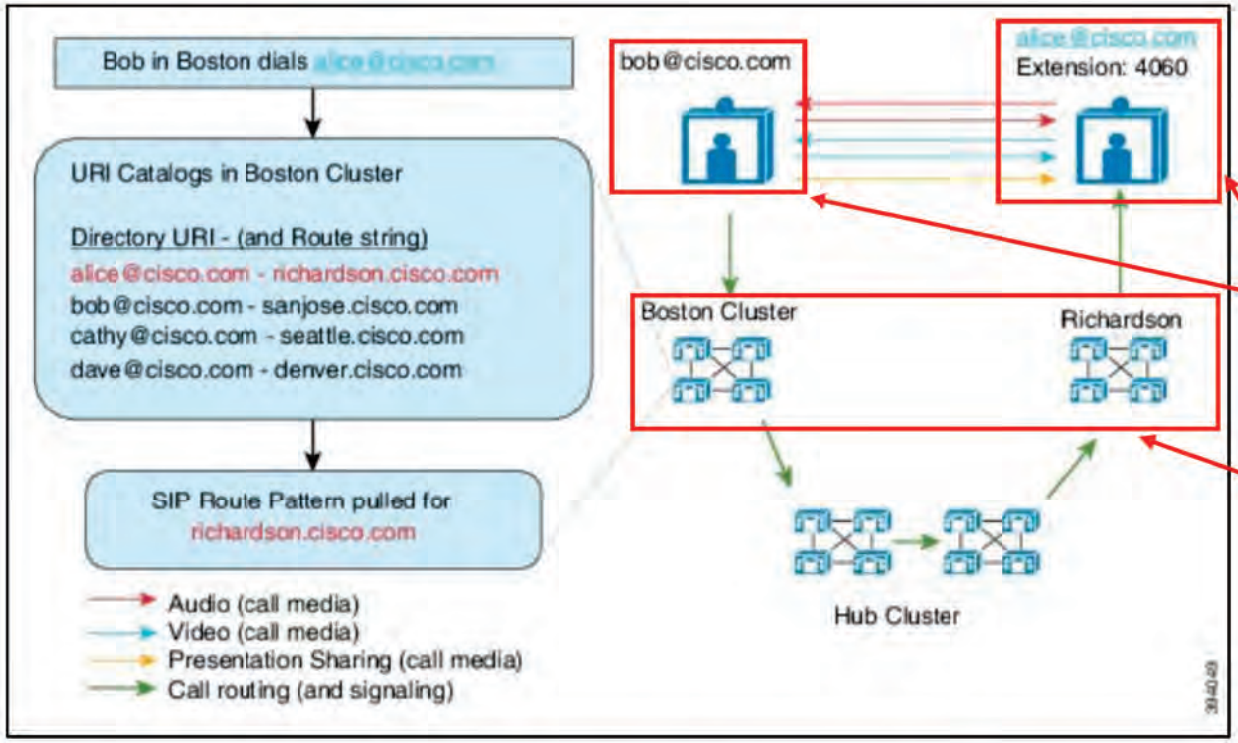
Once all this is configured, now configure a SIP Trunk between the 2 clusters.

Assign the appropriate SIP Profile.

Enter the IP of the other cluster.

Save the trunk.

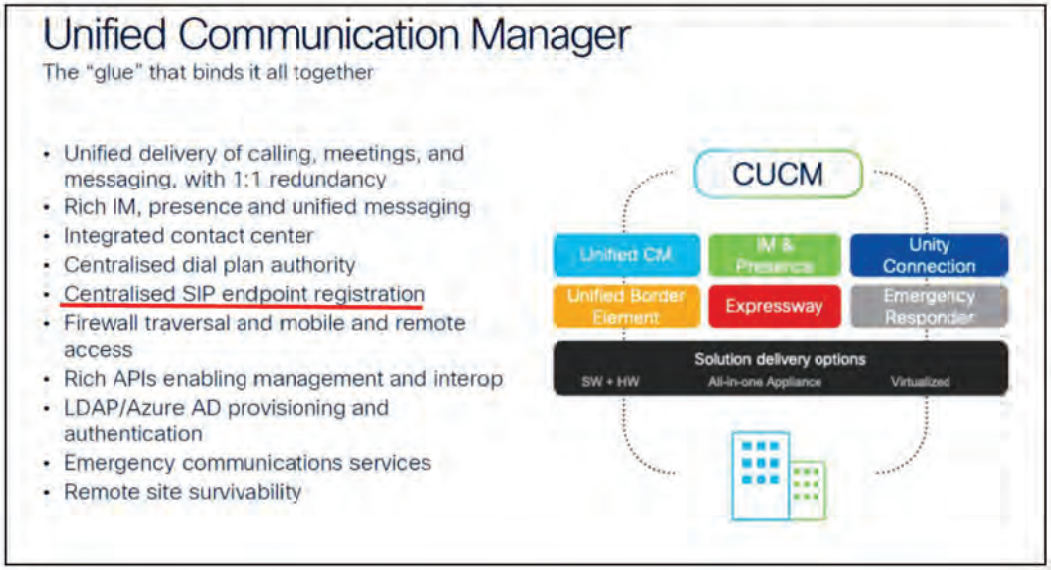
Source: https://community.cisco.com/t5/collaboration-knowledge-base/sip-uri-dialing/ta-p/3157406; *see also* https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/sysConfig/CUCM_BK_SE5DAF88_00_cucm-system-configuration-guide-1151/CUCM_BK_SE5DAF88_00_cucm-system-configuration-guide-1151_chapter_011011.html.



Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/14/systemConfig/cucm_b_system-configuration-guide-14su2/cucm_b_system-configuration-guide-14_chapter_010101.html.

MeshDynamics asserts that these claim elements are software limitations. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If these claim elements are not literally infringed, they are infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same functions of forming an isolated cluster of nodes communicating with each other and VoIP devices in the same way by utilizing on-premise servers that share data and achieves the same result of an on-premise (not in the cloud and without an external SIP server) VoIP network for maintaining device and endpoint

	communication. Unified CM and ILS allow for remote clusters of nodes to communicate with devices and form a VoIP network without an external SIP server for communications. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed elements are insignificant or insubstantial because Unified CM and ILS create a VoIP network without an external SIP Server and provide for remote communication. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
wherein each of the VoIP nodes further comprises a local SIP registry built by exchanging SIP information with the remaining VoIP nodes in the isolated cluster;	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network wherein each of the VoIP nodes further comprises a local SIP registry built by exchanging SIP information with the remaining VoIP nodes in the isolated cluster. Each node within a Unified CM cluster or multi-cluster environment comprises "a local SIP registry built by exchanging SIP information with the remaining VoIP nodes in the isolated cluster."  Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf.

Cluster Recommendations

Cisco Unified CM and IM and Presence support clustering, which is the grouping of nodes that work together as a single logical entity. The publisher node contains the cluster's configuration database, which is replicated to the call processing subscriber nodes and TFTP nodes in the cluster.

Clustering provides an automatic redundancy mechanism for endpoints and for Cisco Unified CM services, such as the ability to receive and process incoming calls. To provide 1:1 redundancy, deploy call processing subscribers and TFTP nodes in pairs. (Figure 6) While the call processing subscribers provide endpoint registration and call processing capabilities, the TFTP nodes provide configuration and firmware updates to endpoints.

Source: https://www.cisco.com/c/en/us/td/docs/solutions/PA/overview/14x/clbpa14x.html.

The "local SIP registry" is built by exchanging SIP information with the other nodes and/or isolated clusters ("VoIP nodes"). Using ILS with SIP URI replication, the Unified CM clusters can share SIP URI reachability data. ILS allows multiple clusters to share user identities (including SIP URIs and directory URIs). Users can then call across clusters using SIP URIs.

INTER-Cluster URI (URI Dialing across cluster):

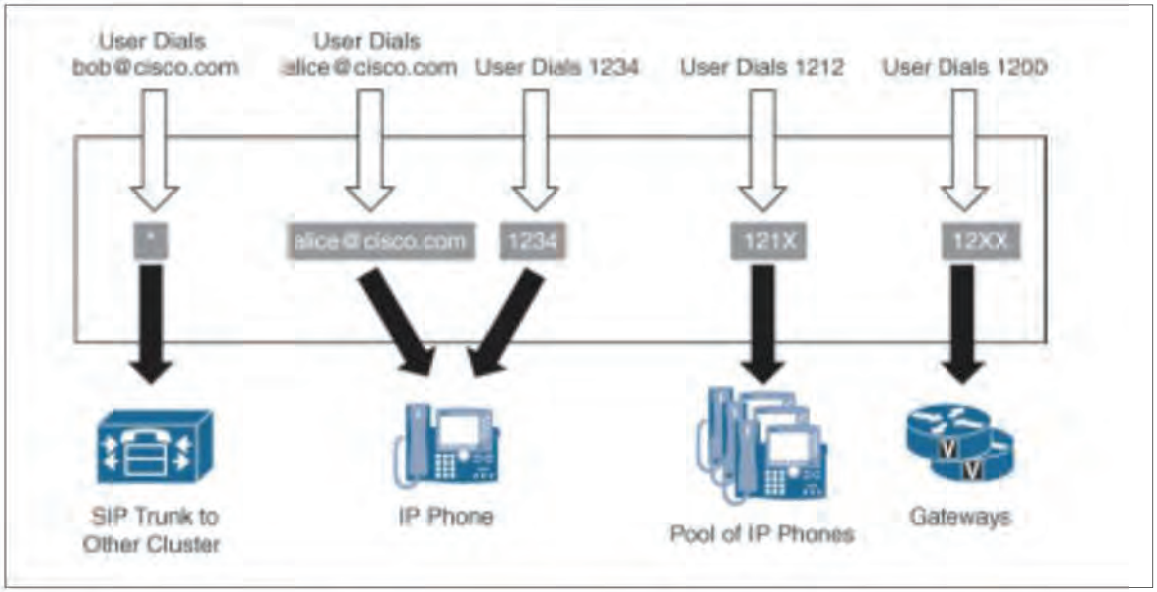
To enable intercluster routing of directory URIs, **Unified CM can be provisioned to exchange directory URI catalogs with other clusters through the Intercluster Lookup Service (ILS).** Each cluster configured to exchange directory URI catalogs with other clusters advertises all locally configured directory URIs in a single directory URI catalog together with a location attribute, **the SIP route string**. This location attribute in multi-cluster environments is used to direct calls for directory URIs to the correct cluster when the host portion of the directory URI cannot be used to deterministically route the SIP request. This, for example, is the case when a flat URI scheme such as *<user>@example.com* is use. The host portion "example.com" does not uniquely identify the remote Unified CM cluster that hosts a given URI.

Basically, every cluster would have a catalogue(table) of Directory URI's. Using ILS each and every cluster would share this catalogue with a local attribute i.e SIP ROUTE STRING.

Source: https://community.cisco.com/t5/collaboration-knowledge-base/sip-uri-dialing/ta-p/3157406.

Using ILS, the Unified CM clusters can create a mesh-like topology. The ILS process exchanges routing updates that contain SIP URI mappings between clusters. Each cluster stores a routing table mapping SIP URIs to cluster locations.

	Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU4/systemConfig/cucm_b_system-configuration-guide-1251su4/cucm_m_intercluster-lookup-service.pdf; *see also* https://www.ciscopress.com/articles/article.asp?p=3089358&seqNum=2 ("The Cisco Unified Communications Manager call-routing table is built using connected devices. The table consists of directory numbers of registered IP phones and of statically entered route patterns that point to external destinations."). MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of building a local SIP registry in the same way by replicating and exchanging SIP information and routing updates between nodes and clusters on-premise and achieves the same result of providing the ability to operate without an external server to maintain endpoint communications at different locations. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the nodes and clusters maintain SIP information and share this information between nodes and clusters on-premise so each has a local SIP registry. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
wherein a first VoIP client device in communication with a first VoIP node establishes a communication with a second VoIP device in communication with a second VoIP node using the local SIP registries of the first VoIP node and the second VoIP node.	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network wherein a first VoIP client device in communication with a first VoIP node establishes a communication with a second VoIP device in communication with a second VoIP node using the local SIP registries of the first VoIP node and the second VoIP node. Each Unified CM cluster comprises multiple nodes, which work together as a single call processing unit. Unified CM nodes can establish a communication between two devices using the local SIP registries on each of the nodes. Source: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/11x/116/collbcvd/control.html. ILS can also be used to establish calls between two different clusters and nodes. For example, a user may be registered to Cluster A with a SIP URI bob@cisco.com (*e.g.*, "a first VoIP client device"). A user registered in Cluster B (*e.g.*, "a second VoIP client device") calls bob@cisco.com using Calling in the Webex App. The Unified CM node in Cluster B (*e.g.*, "a second VoIP node") first looks for a local match in its SIP registry. When no match is found locally, it queries ILS. When ILS finds bob@company.com is hosted on Cluster A's local registry, it routes the call via SIP trunk to that cluster and the Unified CM node in Cluster A (*e.g.*, "a first VoIP node").



Source: https://www.ciscopress.com/articles/article.asp?p=3089358&seqNum=2.

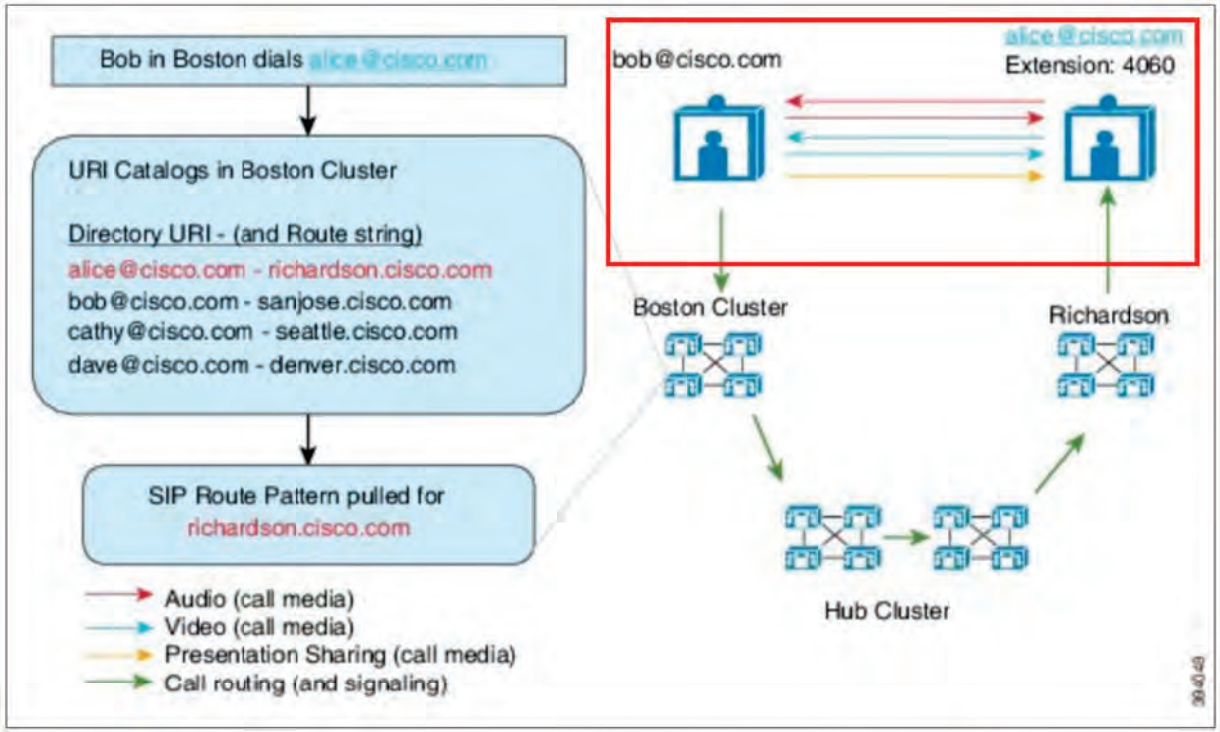
ILS with URIs establishes communication between two VoIP client devices using the local SIP registries of "the first VoIP node" (in one cluster) and "the second VoIP node" (in another cluster).

Advertised Globally via ILS

Global Dial Plan Replication advertises the following dial plan elements to the ILS network, replicating this data in remote clusters:

- **Directory URIs**—In the local cluster, provision email-style directory URIs (e.g. alice@cisco.com). URI dialing provides a user-centric method of placing calls. Global Dial Plan Replication lets you advertise the local catalog of directory URIs to the other clusters in the ILS network to enable intercluster URI dialing.

Intercluster calling uses the cluster route strings that Global Dial Plan Replication advertises to send the call to the called party's home cluster. When a caller places a call to a directory URI or alternate number that is homed in another cluster, the system pulls the associated route string, matches a SIP route pattern for the route string, and sends the call to the destination that the SIP route pattern specifies. For this to work, you must configure SIP route patterns in your remote clusters to route the route string back to its home cluster.



Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/14/systemConfig/cucm_b_system-configuration-guide-14su2/cucm_b_system-configuration-guide-14_chapter_010101.html.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of establishing a communication between two endpoints in a VoIP network in the same way by using on-premise SIP information at each node and cluster and achieves the same result establishing a VoIP call between to endpoints. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Calling for Webex App and Unified CM will establish a connection between endpoints using on-premise nodes or clusters and their SIP registries. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Claim 2	
The VoIP-capable network of claim 1, wherein the local SIP registries of the isolated VoIP nodes are updated as the VoIP nodes and the VoIP client devices begin communication with the isolated cluster and end communication with the isolated cluster.	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein the local SIP registries of the isolated VoIP nodes are updated as the VoIP nodes and the VoIP client devices begin communication with the isolated cluster and end communication with the isolated cluster. When a cluster receives a query for a URI, ILS searches other clusters in the network to find the destination. Once the URI is found, the local Unified CM database ("local SIP registries of the isolated VoIP nodes") is updated, including the URI and associated SIP route string ("as the VoIP nodes and client devices begin communication with the isolated cluster and end communication with the isolated cluster"). This newly learned information is then replicated to all other clusters in the ILS network. This allows subsequent calls to that URI to be routed directly through the local cluster, using the locally stored route string to send the call to the correct remote cluster. **Intercluster Lookup Service Overview** The Intercluster Lookup Service (ILS) allows you to create networks of remote Cisco Unified Communications Manager clusters. When you configure ILS on multiple clusters, it updates Cisco Unified Communications Manager with the current status of remote clusters in the ILS network. In Cisco Unified CM Administration, you can configure ILS on a pair of clusters and then join those clusters to form an ILS network. ILS allows you to join additional clusters to the network without having to configure the connections between each cluster. Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/systemConfig/cucm_b_system-configuration-guide-1251/cucm_b_system-configuration-guide-1251_chapter_011001.html. **Learned Global Dial Plan Data** Unified Communications Manager stores in the local database all global dial plan data that is learned through ILS. In addition to replicating locally configured data, ILS advertises all global dial plan data that the local cluster has learned from other clusters in the ILS network. This ensures that all advertised data reaches each cluster in the ILS network. Learned global dial plan data includes learned directory URIs, learned alternate numbers, learned patterns, learned PSTN failover rules, and learned route strings.

	Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/sysConfig/11_5_1_SU1/cucm_b_system-configuration-guide-1151su1/cucm_b_system-configuration-guide-1151su1_chapter_011010.html. We can call ILS – Intercluster Lookup Service as Voice Routing Protocol because it behaves like dynamic routing protocol. Just like advertising the local route from one router to another, ILS will advertise the URIs between different CUCM cluster. Each CUCM cluster node advertises its URIs and "**SIP route string**" to its neighbor's (or Hubs). CUCM cluster later creates a table with URIs and associated SIP route string. Finally, SIP route strings are routed through SIP route patterns. Source: https://community.cisco.com/t5/collaboration-blogs/cucm-intercluster-lookup-service-ils-configuration-guide-based/ba-p/3358335. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of updating local SIP registries in the same way by exchanging information learned from other clusters and achieves the same result of updated local SIP registries for on-premise calls. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the local SIP registries of each node or cluster on-premise are updated with learned information. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 3	
The VoIP-capable network of claim 1, wherein updates to the local SIP registry of a VoIP node are communicated to remaining VoIP nodes in	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein updates to the local SIP registry of a VoIP node are communicated to remaining VoIP nodes in the isolated cluster by broadcasting one or more information packets containing local SIP registry information of the VoIP node.

the isolated cluster by broadcasting one or more information packets containing local SIP registry information of the VoIP node.	Information in networks is carried in packets. ILS advertises the URIs between different Unified CM clusters and shares the directory URI catalogs across clusters (*e.g.*, "broadcasting one or more information packets containing local SIP registry information of the VoIP node"). We can call ILS - Intercluster Lookup Service as Voice Routing Protocol because it behaves like dynamic routing protocol. Just like advertising the local route from one router to another, ILS will advertise the URIs between different CUCM cluster. Each CUCM cluster node advertises its URIs and "**SIP route string**" to its neighbor's (or Hubs). CUCM cluster later creates a table with URIs and associated SIP route string. Finally, SIP route strings are routed through SIP route patterns. Source: https://community.cisco.com/t5/collaboration-blogs/cucm-intercluster-lookup-service-ils-configuration-guide-based/ba-p/3358335. ***INTER-Cluster URI (URI Dialing across cluster):*** To enable intercluster routing of directory URIs, **Unified CM can be provisioned to exchange directory URI catalogs with other clusters through the Intercluster Lookup Service (ILS).** Each cluster configured to exchange directory URI catalogs with other clusters advertises all locally configured directory URIs in a single directory URI catalog together with a location attribute, **the SIP route string**. This location attribute in multi-cluster environments is used to direct calls for directory URIs to the correct cluster when the host portion of the directory URI cannot be used to deterministically route the SIP request. This, for example, is the case when a flat URI scheme such as *<user>@example.com* is use. The host portion "example.com" does not uniquely identify the remote Unified CM cluster that hosts a given URI. ***Basically, every cluster would have a catalogue(table) of Directory URI's. Using ILS each and every cluster would share this catalogue with a local attribute i.e SIP ROUTE STRING.*** Source: https://community.cisco.com/t5/collaboration-knowledge-base/sip-uri-dialing/ta-p/3157406. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

	If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of updating local SIP registries in the same way by advertising and sharing a directory of URLs and achieves the same result of an updated local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because ILS shares the directory across clusters to enable VoIP calls. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 4	
The VoIP-capable network of claim 1, wherein the local SIP registry of a VoIP node is updated according to information received from another VoIP node in the isolated cluster in special information packets that each contain local SIP registry information of another VoIP node.	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein the local SIP registry of a VoIP node is updated according to information received from another VoIP node in the isolated cluster in special information packets that each contain local SIP registry information of another VoIP node Information in networks is carried in packets. The update messages sent by clusters using ILS are known as "peer info vectors." These are the packets ("special information packets") that allow remote clusters to learn about the status and information of other clusters within the ILS network. These updates include information like cluster IDs, peer IDs, cluster versions, and the IP addresses of activated cluster nodes. The Unified CM cluster also creates a table with URIs and associated SIP route string of advertised directory URI catalogs from ILS ("local SIP registry of a VoIP node is updated according to information received from another VoIP nodes in the isolated cluster in special information packets that each contain local SIP registry information of another VoIP node"). Each cluster in an ILS network exchange and update messages, called peer info vectors, that are designed to inform remote clusters of the status of each cluster in the network. The update messages contain information about the known clusters in the network, including: • Cluster IDs • Peer IDs for the publisher • Cluster descriptions and versions • Fully Qualified Domain Name (FQDN) of the host • IP addresses and host names for the cluster nodes that have ILS activated Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1_SU7/cucm_b_system-configuration-1151su7-1151su8/cucm_b_system-configuration-guide-1151su1_chapter_011001.html.

	We can call ILS - Intercluster Lookup Service as Voice Routing Protocol because it behaves like dynamic routing protocol. Just like advertising the local route from one router to another, ILS will advertise the URIs between different CUCM cluster. Each CUCM cluster node advertises its URIs and "**SIP route string**" to its neighbor's (or Hubs). CUCM cluster later creates a table with URIs and associated SIP route string. Finally, SIP route strings are routed through SIP route patterns. Source: https://community.cisco.com/t5/collaboration-blogs/cucm-intercluster-lookup-service-ils-configuration-guide-based/ba-p/3358335. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of updating the local SIP registry in the same way by advertising and sharing a directory of URLs and other information to complete a call and achieves the same result of an updated local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because ILS shares the directory across clusters to enable VoIP calls. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 8	
The VoIP-capable network of claim 1 wherein said nodes comprise mesh nodes.	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network, in addition to the elements of claim 1 as shown above wherein said nodes comprise mesh nodes. Using ILS, the Unified CM clusters can create a mesh-like topology ("mesh nodes"). The ILS process exchanges routing updates that contain SIP URI mappings between clusters. Each cluster stores a routing table mapping SIP URIs to cluster locations:

ILS Network Components

An ILS network comprises the following components:

- **Hub clusters**—Hub clusters form the backbone of an ILS network using automesh functionality to create a full mesh topology with the other hub clusters. Hub clusters relay and share information across the ILS network for a variety of features.
- **Spoke clusters**—Spoke clusters connect only to their local hub cluster and never contact other hub or spoke clusters directly. Spoke clusters rely on their local hub to share and relay information across the network.
- **Global dial plan imported catalogs**—This optional component applies if you have Global Dial Plan Replication configured, and you are interoperating with a Cisco TelePresence Video Communications Server, or a third-party call control system. Import a directory URI or +E.164 number catalog manually from a CSV file that was exported from the other system, thereby allowing users in the ILS network to call users from the other system.

Source:https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU4/systemConfig/cucm_b_system-configuration-guide-1251su4/cucm_m_intercluster-lookup-service.pdf; *see also* https://www.ciscopress.com/articles/article.asp?p=3089358&seqNum=2 ("The Cisco Unified Communications Manager call-routing table is built using connected devices. The table consists of directory numbers of registered IP phones and of statically entered route patterns that point to external destinations.").

During operation, the database replication is fully meshed between all servers within the Unified CM Cluster.

User Settings

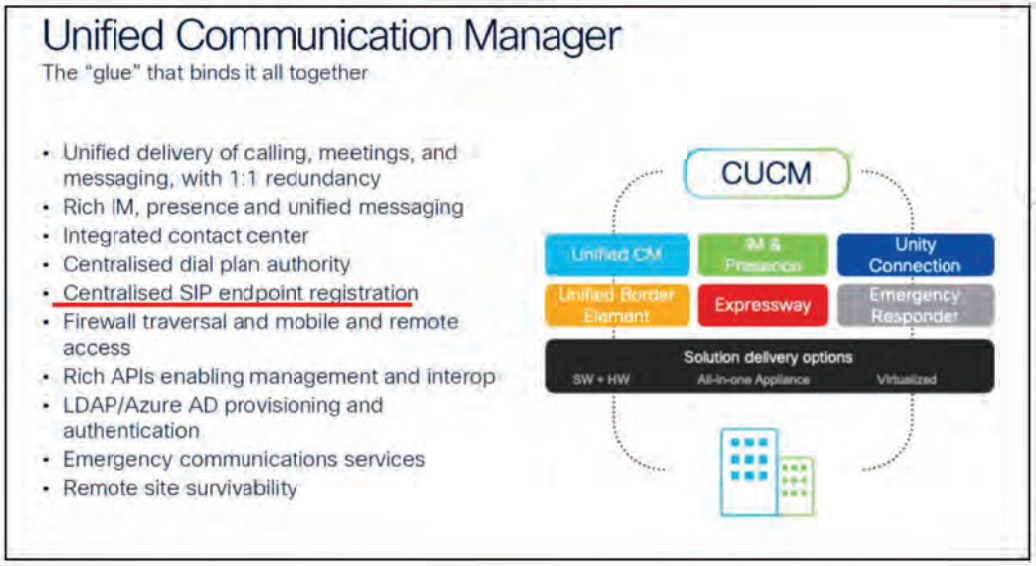
During normal operation, the database replication is fully meshed between all the servers including the Enhanced Survivability Node within the Unified CM cluster. The static configuration data, because it is created through moves, adds, and changes, is always stored on the publisher and replicated one way from the publisher to each subscriber and enhanced survivability node in the cluster.

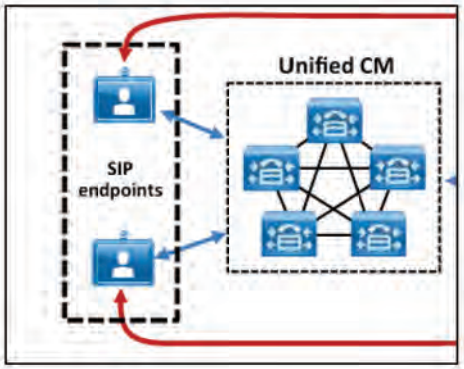
Source: https://help.webex.com/en-us/article/ggaigh/Get-Started-with-Enhanced-Survivability.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

	If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of completing VoIP calls without an external server in the same way by using nodes in communication and exchanging information locally and achieves the same result of a local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Cisco's documents refer to the operation and structure of Unified CM nodes and ILS as "meshed" or "mesh" topology. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 9	
The VoIP-capable network of claim 8 wherein said mesh nodes provide VoIP optimized services within said mesh nodes.	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network, in addition to the elements of claim 1 and 8, as shown above, wherein said mesh nodes provide VoIP optimized services within said mesh nodes. Unified CM cluster ("mesh nodes") provide "VoIP optimized services." These are identified in Cisco's documentation, and include, *e.g.*, direct registration and media, high-quality audio, and media optimization, among other features: When Webex App is registered with Unified CM, the solution provides enterprise calling capabilities—audio/video calls and mid-call features such as mute, consultative transfer, merge/conference, sharing, and so on. Direct access to call settings such as call forwarding (CFA), single number reach (SNR) and visual voicemail is also supported. Webex App app also interfaces with Unified CM-registered desk phones to provide remote call control capabilities in Deskphone Control (DPC) mode. Additionally, direct registration to Unified CM provides these benefits: • Direct connection to Unified CM leading to a faster connect time than Hybrid Call Service • Direct media when Webex App apps are local within enterprise network • Additional calling capabilities with a roadmap towards Jabber calling feature parity • Reuse of existing MRA and Jabber CSF configuration for client-side integration (unlike Hybrid Call Service's server-side integration) Source: https://help.webex.com/en-us/article/nq7yfhbb/Changes-to-Hybrid-Call-Service; *see also* https://help.webex.com/en-us/article/nj8v6wg/Deployment-guide-for-Calling-in-Webex-App-(Unified-CM). MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

	If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of completing VoIP calls without an external server in the same way using nodes in communication with each node and exchanging information locally and achieves the same result a local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Cisco's documents confirm that this network provide benefits and enterprise-calling capabilities. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 10	
A method of maintaining VoIP capabilities within a network comprising:	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a method of maintaining VoIP capabilities within a network. Cisco's Webex is Voice over Internet Protocol-capable network in which each client or device can communicate with multiple other clients or devices over the Internet using, *e.g.*, a computer or a phone. *See supra* preamble Claim 1, incorporated herein by reference.
forming a cluster of two or more initially isolated network nodes	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a method of maintaining VoIP capabilities within a network comprising the step of forming a cluster of two or more initially isolated network nodes. VoIP client devices using the Calling in Webex App use the on-premise Unified CM nodes, which can operate in isolation without the need to connect to an external datacenter, for calling, including if the cloud connection is lost. **Connection is lost to the Webex cloud** If https://status.webex.com or the health checker show a Webex App cloud full or partial outage, Calling in Webex App (Unified CM) still works for users who are already signed in, as long as the call type is a Unified CM call and goes through Unified CM infrastructure. Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/ucmcalling/unified-cm-wbx-teams-deployment-guide/unified-cm-wbx-teams-deployment-guide_chapter_0101.html. Unified CM nodes are a networked cluster of remote, isolated nodes (*e.g.*, "forming a cluster of two or more initially isolated network nodes"), including when not connected to the cloud, and the nodes communicate with one another. This on-premises SIP-based call control system (*e.g.*, Unified CM) manages the SIP registration of VoIP devices using the Webex App and the devices communicate with at least one Unified CM node.





Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf; https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf; *see also* https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/11x/116/collbcvd/control.html ("Unified CM supports the concept of clustering. The Unified CM architecture enables a group of server nodes to work together as a single call processing entity. This grouping of server nodes is known as a cluster.").

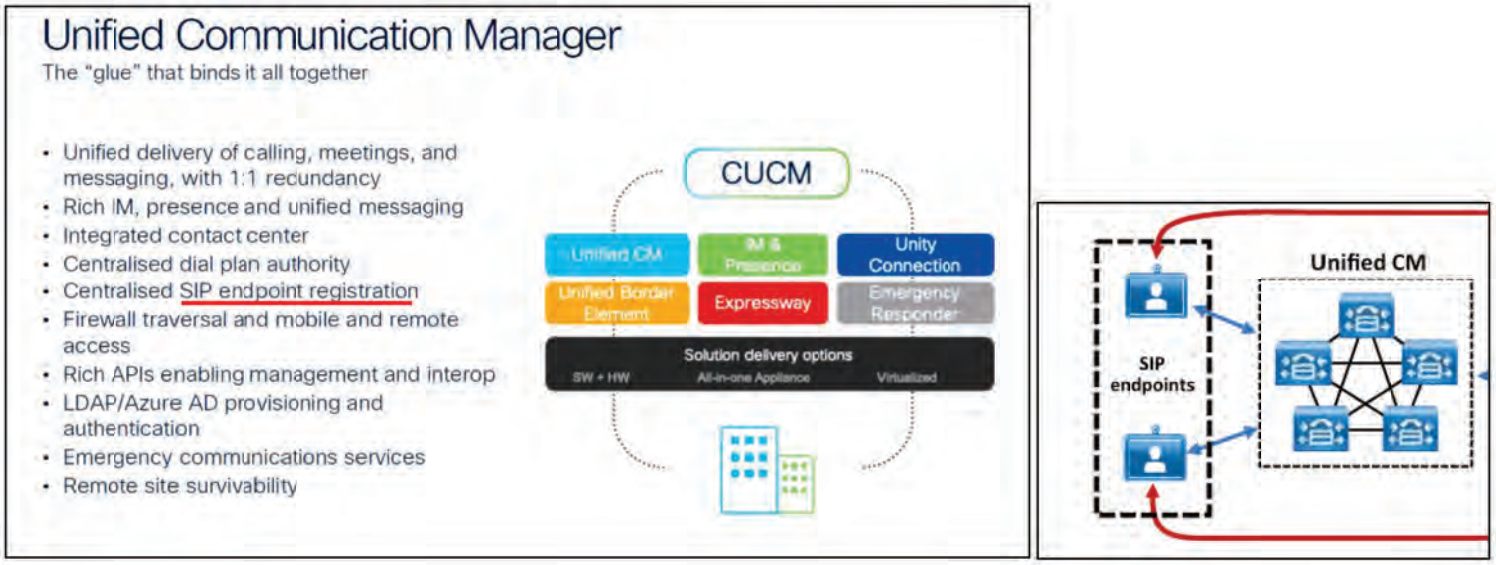
Clusters

Clusters provide a mechanism for distributing call processing, presence status, and database replication among multiple servers. They provide transparent sharing of resources and features, and enable system scalability.

Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/install/15/cucm_b_install-guide-cucm-imp-15/cucm_m_planning-the-installation.html.

Using the Intercluster Lookup Service (ILS), the network can create a multi-cluster network of remote Unified CM clusters that are in communication and share data (*e.g.*, "forming a cluster of two or more initially isolated network

	nodes""). ILS is designed to create a network of interconnected Unified CM clusters, allowing Webex App users to find and dial each other using SIP URIs even if they are on different clusters and even without the cloud. The Cisco Intercluster Lookup Service (ILS) makes it easy to create a multi-cluster network of remote Cisco Unified Communications Manager clusters that share data. ILS eliminates the need for an administrator having to configure connections between clusters manually. Once you have ILS configured on a hub cluster, you can connect new clusters by enabling ILS on the new cluster and pointing the new cluster to an existing hub. ILS connects the clusters automatically and lets both clusters know the topology of the larger ILS network. Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU4/systemConfig/cucm_b_system-configuration-guide-1251su4/cucm_m_intercluster-lookup-service.pdf; *see also* https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/11x/116/collbcvd/control.html ("In a multi-cluster deployment, interconnect all the individual Unified CM clusters through SIP trunks."). *See also* Claim 1 above, incorporated herein by reference. MeshDynamics asserts that these claim elements are software limitations. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of forming a cluster of two or more initially isolated network nodes in the same way by utilizing on-premise servers that share data and achieves the same result of an on-premise (not in the cloud and without an external SIP server) VoIP network for maintaining device and endpoint communication. Unified CM and ILS allow for remote clusters of nodes to communicate with devices and form a VoIP network without an external SIP server for communications. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed elements are insignificant or insubstantial because Unified CM and ILS create a VoIP network without an external SIP Server and provide for remote communication. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
establishing communications between two or more client devices by way of the	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a method of maintaining VoIP capabilities within a network comprising the step of establishing communications between two or more client devices by way of the initially isolated network nodes, wherein in a first configuration, at least two of said initially isolated network nodes are in

initially isolated network nodes, wherein in a first configuration, at least two of said initially isolated network nodes are in communication with each other but not in communication with an external SIP server, and wherein each of said at least two initially isolated network nodes supports VoIP communications based on a local SIP registry contained in each of the said nodes according to the method of:	communication with each other but not in communication with an external SIP server, and wherein each of said at least two initially isolated network nodes supports VoIP communications based on a local SIP registry contained. As shown above, the remote, isolated Unified CM nodes and clusters establish communications between SIP endpoints (*e.g.*, "establishing communications between two or more client devices by way of the initially isolated network nodes"). The Unified CM nodes are in a communications with each other, and do not rely on an external SIP server (*e.g.*, " at least two of said initially isolated network nodes are in communication with each other but not in communication with an external SIP server"), but provide SIP registration and operate as a single call processing entity ("each of said at least two initially isolated network nodes supports VoIP communications based on a local SIP registry contained"):  Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf; https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf; *see also* https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/11x/116/collbcvd/control.html ("Unified CM supports the concept of clustering. The Unified CM architecture enables a group of server nodes to work together as a single call processing entity. This grouping of server nodes is known as a cluster.").

	Clusters Clusters provide a mechanism for distributing call processing, presence status, and database replication among multiple servers. They provide transparent sharing of resources and features, and enable system scalability. Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/install/15/cucm_b_install-guide-cucm-imp-15/cucm_m_planning-the-installation.html. *See also* Claim 1 above, incorporated herein by reference. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of establishing a communication between two VoIP devices in the same way by replicating and exchanging SIP information and routing updates between nodes and clusters on-premise and achieves the same result of providing the ability to operate without an external server to maintain endpoint communications at different locations. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the nodes and clusters maintain SIP information and share this information between nodes and clusters on-premise so each has a local SIP registry to connect endpoints. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial
communicating with at least one other initially isolated node to exchange SIP registry information	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a method of maintaining VoIP capabilities within a network comprising the step of communicating with at least one other initially isolated node to exchange SIP registry information. As shown above, the Unified CM nodes communicate with each other in the cluster to share and replicate their databases of SIP registry information. The "local SIP registry" is built by exchanging SIP information with the other nodes and/or isolated clusters. Using ILS with SIP URI replication, the Unified CM clusters can share SIP URI reachability data. ILS allows multiple clusters to share user identities (including SIP URIs and directory URIs).

Cluster Recommendations

Cisco Unified CM and IM and Presence support clustering, which is the grouping of nodes that work together as a single logical entity. The publisher node contains the cluster's configuration database, which is replicated to the call processing subscriber nodes and TFTP nodes in the cluster.

Clustering provides an automatic redundancy mechanism for endpoints and for Cisco Unified CM services, such as the ability to receive and process incoming calls. To provide 1:1 redundancy, deploy call processing subscribers and TFTP nodes in pairs. (Figure 6) While the call processing subscribers provide endpoint registration and call processing capabilities, the TFTP nodes provide configuration and firmware updates to endpoints.

Source: https://www.cisco.com/c/en/us/td/docs/solutions/PA/overview/14x/clbpa14x.html.

INTER-Cluster URI (URI Dialing across cluster):

To enable intercluster routing of directory URIs, **Unified CM can be provisioned to exchange directory URI catalogs with other clusters through the Intercluster Lookup Service (ILS).** Each cluster configured to exchange directory URI catalogs with other clusters advertises all locally configured directory URIs in a single directory URI catalog together with a location attribute, **the SIP route string**. This location attribute in multi-cluster environments is used to direct calls for directory URIs to the correct cluster when the host portion of the directory URI cannot be used to deterministically route the SIP request. This, for example, is the case when a flat URI scheme such as *<user>@example.com* is use. The host portion "example.com" does not uniquely identify the remote Unified CM cluster that hosts a given URI.

Basically, every cluster would have a catalogue(table) of Directory URI's. Using ILS each and every cluster would share this catalogue with a local attribute i.e SIP ROUTE STRING.

Source: https://community.cisco.com/t5/collaboration-knowledge-base/sip-uri-dialing/ta-p/3157406.

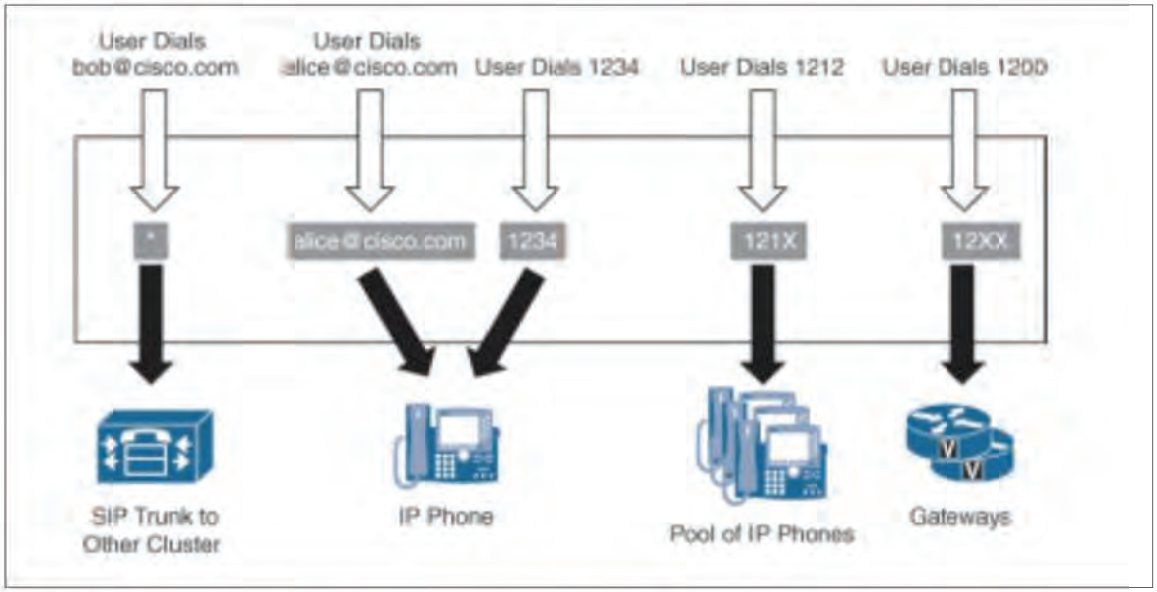
See also Claim 1 above, incorporated herein by reference.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of exchanging SIP registry information in the same way by replicating and

	exchanging SIP information and routing updates between nodes and clusters on-premise and achieves the same result of providing the ability to operate without an external server to maintain endpoint communications at different locations. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the nodes and clusters maintain SIP information and share this information between nodes and clusters on-premise so each has a local SIP registry. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
updating the local SIP registry in said node as new information is acquired	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a method of maintaining VoIP capabilities within a network comprising the step of updating the local SIP registry in said node as new information is acquired. As shown above, the Unified CM nodes in a cluster update the local SIP registries as new information is acquired by replicating the database. Using ILS, tables are updated as new information is learned. **Learned Global Dial Plan Data** Unified Communications Manager stores in the local database all global dial plan data that is learned through ILS. In addition to replicating locally configured data, ILS advertises all global dial plan data that the local cluster has learned from other clusters in the ILS network. This ensures that all advertised data reaches each cluster in the ILS network. Learned global dial plan data includes learned directory URIs, learned alternate numbers, learned patterns, learned PSTN failover rules, and learned route strings. Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/sysConfig/11_5_1_SU1/cucm_b_system-configuration-guide-1151su1/cucm_b_system-configuration-guide-1151su1_chapter_011010.html. We can call ILS – Intercluster Lookup Service as Voice Routing Protocol because it behaves like dynamic routing protocol. Just like advertising the local route from one router to another, ILS will advertise the URIs between different CUCM cluster. Each CUCM cluster node advertises its URIs and "**SIP route string**" to its neighbor's (or Hubs). CUCM cluster later creates a table with URIs and associated SIP route string. Finally, SIP route strings are routed through SIP route patterns. Source: https://community.cisco.com/t5/collaboration-blogs/cucm-intercluster-lookup-service-ils-configuration-guide-based/ba-p/3358335.

	See also Claims 1 and 2 above, incorporated herein by reference. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of updating SIP registry information with newly acquired information in the same way by replicating and exchanging SIP information and routing updates between nodes and clusters on-premise and achieves the same result of providing the ability to operate without an external server to maintain endpoint communications at different locations. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the nodes and clusters maintain SIP information and share this information between nodes and clusters on-premise so each has a local SIP registry. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
sending and receiving VoIP packets from a sender isolated node to one or more recipient isolated nodes based on said local SIP registry functionality when a client device in communication with the sender node establishes communication with a client device in communication with the recipient node.	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a method of maintaining VoIP capabilities within a network comprising the step of sending and receiving VoIP packets from a sender isolated node to one or more recipient isolated nodes based on said local SIP registry functionality when a client device in communication with the sender node establishes communication with a client device in communication with the recipient nodes. Information in networks is carried in packets. A shown above, isolated nodes in a Unified CM cluster can connect SIP endpoints using the directory URI catalog from ILS and the local SIP registry. For example, a user may be registered to Cluster A with a SIP URI bob@cisco.com (*e.g.*, "a first VoIP client device"). A user registered in Cluster B (*e.g.*, "a second VoIP client device") calls bob@cisco.com using Calling in the Webex App. The Unified CM node in Cluster B (*e.g.*, "a second VoIP node") first looks for a local match in its SIP registry. If no match is found locally, it queries ILS. If ILS finds bob@company.com is hosted on Cluster A's local registry, it routes the call via SIP trunk to that cluster and the Unified CM node in Cluster A (*e.g.*, "a first VoIP node").



Source: https://www.ciscopress.com/articles/article.asp?p=3089358&seqNum=2.

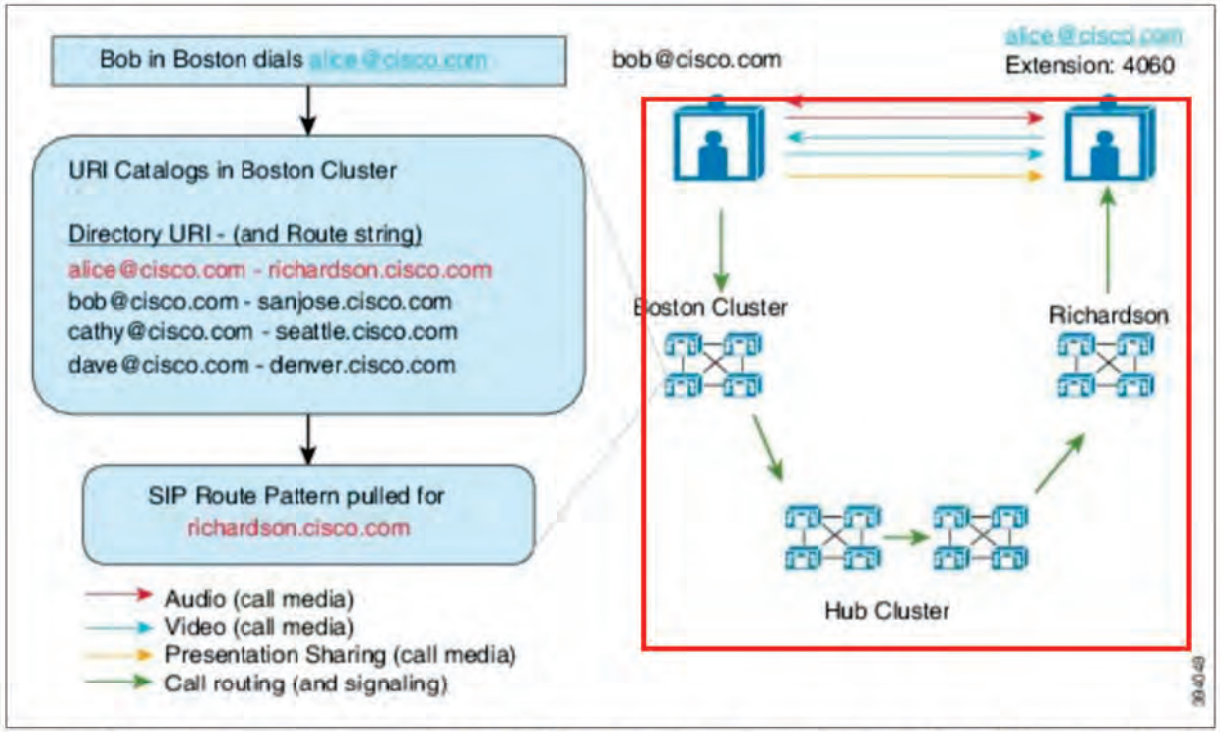
ILS with URIs provides a method of placing calls between two VoIP client devices using the local SIP registries of the sender isolated node (in one cluster) and the recipient isolated node (in another cluster).

Advertised Globally via ILS

Global Dial Plan Replication advertises the following dial plan elements to the ILS network, replicating this data in remote clusters:

- **Directory URIs**—In the local cluster, provision email-style directory URIs (e.g. alice@cisco.com). URI dialing provides a user-centric method of placing calls. Global Dial Plan Replication lets you advertise the local catalog of directory URIs to the other clusters in the ILS network to enable intercluster URI dialing.

Intercluster calling uses the cluster route strings that Global Dial Plan Replication advertises to send the call to the called party's home cluster. When a caller places a call to a directory URI or alternate number that is homed in another cluster, the system pulls the associated route string, matches a SIP route pattern for the route string, and sends the call to the destination that the SIP route pattern specifies. For this to work, you must configure SIP route patterns in your remote clusters to route the route string back to its home cluster.



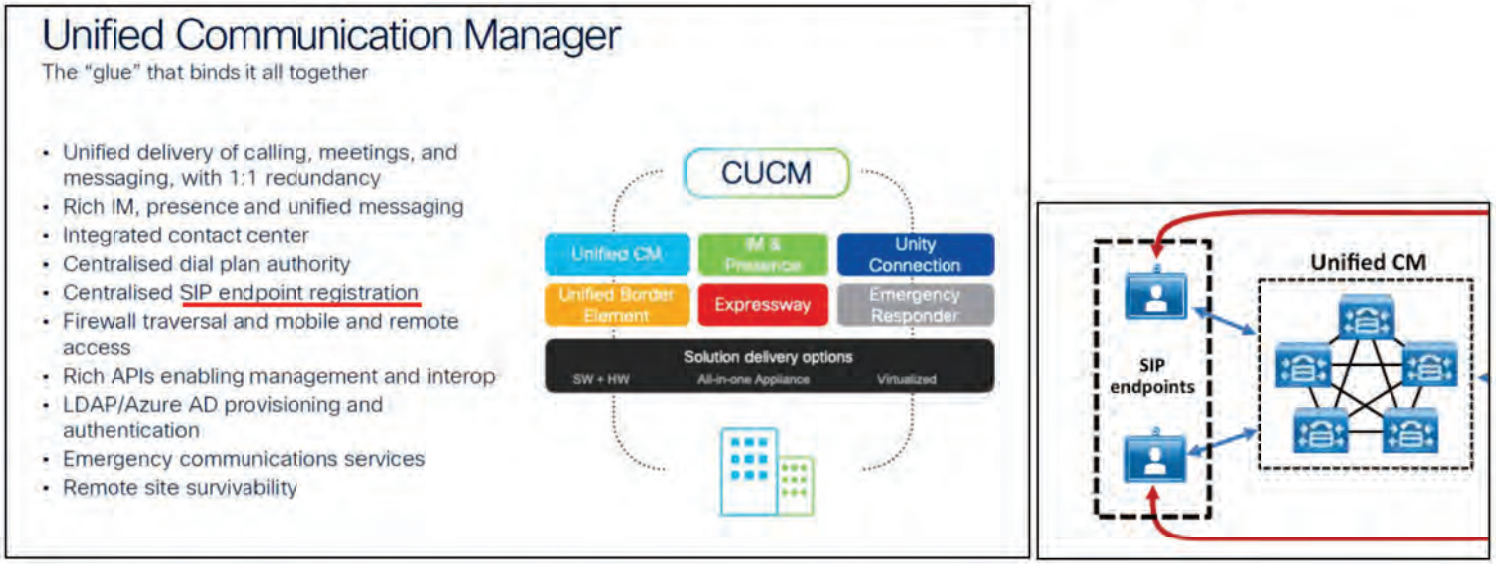
Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/14/systemConfig/cucm_b_system-configuration-guide-14su2/cucm_b_system-configuration-guide-14_chapter_010101.html.

See also Claim 1, above, incorporated herein by reference.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of establishing a communication between two endpoints by sending and receiving packets in a VoIP network on-premise in the same way by using on-premise SIP information at each node and cluster and achieves the same result establishing a VoIP call between two endpoints. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Calling for Webex App and Unified CM will establish a connection between endpoints using on-premise nodes or clusters and their SIP registries. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Claim 12	
The method of claim 10, further comprising updating the local SIP registries of the isolated nodes as nodes and clients join and leave the isolated cluster	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a method of maintaining VoIP capabilities within a network comprising, in addition to the steps of claim 10 as shown above, the step of updating the local SIP registries of the isolated nodes as nodes and clients join and leave the isolated cluster. *See* Claim 2, above, incorporated herein by reference.
Claim 13	
13. The method of claim 10, wherein updates to the local SIP registry of each node is communicated to remaining nodes in the cluster by broadcasting an information packet containing the local SIP registry information.	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a method of maintaining VoIP capabilities within a network comprising, in addition to the steps of claim 10 as shown above, the step of wherein updates to the local SIP registry of each node is communicated to remaining nodes in the cluster by broadcasting an information packet containing the local SIP registry information. *See* Claim 3, above, incorporated herein by reference.
Claim 15	
A VoIP capable network comprising:	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a Voice over Internet Protocol-capable network in which each client or device can communicate with multiple other clients or devices over the Internet using, *e.g.*, a computer or a phone. *See* preamble Claim 1 above, incorporated herein by reference.
a first initially isolated network node in communication with at least two VoIP clients, wherein the first isolated node further comprises a local SIP registry wherein said SIP registry	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network comprising a first initially isolated network node in communication with at least two VoIP clients, wherein the first isolated node further comprises a local SIP registry wherein said SIP registry contains address identifiers for each VoIP client in communication with the first node. A Unified CM cluster is a networked cluster of remote nodes, which can operate in isolation without the need to connect to an external datacenter, including when not connected to the cloud, and the nodes communicate with one another. This on-premises SIP-based call control system (*e.g.*, Unified CM) manages the SIP registration of VoIP

contains address identifiers for each VoIP client in communication with the first node; and	devices using the Webex App and the devices communicate with at least one Unified CM node ("*e.g.*, "first initially isolated network node in communication with at least two VoIP clients" and "a local SIP registry wherein said SIP registry contains address identifiers for each VoIP clients in communication with the first node"):  Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf; https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf; *see also* https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/11x/116/collbcvd/control.html ("Unified CM supports the concept of clustering. The Unified CM architecture enables a group of server nodes to work together as a single call processing entity. This grouping of server nodes is known as a cluster."). MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of providing a local SIP registry in the same way by replicating and exchanging SIP information and routing updates between nodes and clusters on-premise and achieves the same result of providing the ability to operate without an external server to maintain endpoint communications at different locations. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the nodes and clusters maintain SIP information and share this information

	between nodes and clusters on-premise so each has a local SIP registry. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
wherein VoIP communication between said at least two VoIP clients are initiated by utilizing the local SIP registry, wherein the first isolated node further comprises communications means with other isolated nodes wherein the first isolated node broadcasts its SIP registry information to other nodes in communication with the first node.	Cisco's Webex, *e.g.*, Calling for the Webex App, is a VoIP-capable network wherein VoIP communication between said at least two VoIP clients are initiated by utilizing the local SIP registry, wherein the first isolated node further comprises communications means with other isolated nodes wherein the first isolated node broadcasts its SIP registry information to other nodes in communication with the first node. As shown above, Unified CM nodes are a local SIP registry for connecting SIP endpoints (*e.g.*, "VoIP communication between said at least two VoIP clients are initiated by utilizing the local SIP registry"). The remote Unified CM nodes further use Intercluster Lookup Service (ILS) to exchange SIP registry information with other clusters and nodes in communication with the Unified CM node. ***INTER-Cluster URI (URI Dialing across cluster):*** To enable intercluster routing of directory URIs, **Unified CM can be provisioned to exchange directory URI catalogs with other clusters through the Intercluster Lookup Service (ILS).** Each cluster configured to exchange directory URI catalogs with other clusters advertises all locally configured directory URIs in a single directory URI catalog together with a location attribute, **the SIP route string**. This location attribute in multi-cluster environments is used to direct calls for directory URIs to the correct cluster when the host portion of the directory URI cannot be used to deterministically route the SIP request. This, for example, is the case when a flat URI scheme such as *<user>@example.com* is use. The host portion "example.com" does not uniquely identify the remote Unified CM cluster that hosts a given URI. ***Basically, every cluster would have a catalogue(table) of Directory URI's. Using ILS each and every cluster would share this catalogue with a local attribute i.e SIP ROUTE STRING.*** Source: https://community.cisco.com/t5/collaboration-knowledge-base/sip-uri-dialing/ta-p/3157406. Information in networks is carried in packets. ILS advertises the URIs between different Unified CM clusters and shares the directory URI catalogs across clusters (*e.g.*, "broadcasts its SIP registry information to other nodes in communication with the first node").

We can call ILS – Intercluster Lookup Service as Voice Routing Protocol because it behaves like dynamic routing protocol. Just like advertising the local route from one router to another, ILS will advertise the URIs between different CUCM cluster.

Each CUCM cluster node advertises its URIs and "**SIP route string**" to its neighbor's (or Hubs). CUCM cluster later creates a table with URIs and associated SIP route string. Finally, SIP route strings are routed through SIP route patterns.

Source: https://community.cisco.com/t5/collaboration-blogs/cucm-intercluster-lookup-service-ils-configuration-guide-based/ba-p/3358335.

Using ILS, the Unified CM clusters can create a mesh-like topology. The ILS process exchanges routing updates that contain SIP URI mappings between clusters. Each cluster stores a routing table mapping SIP URIs to cluster locations.

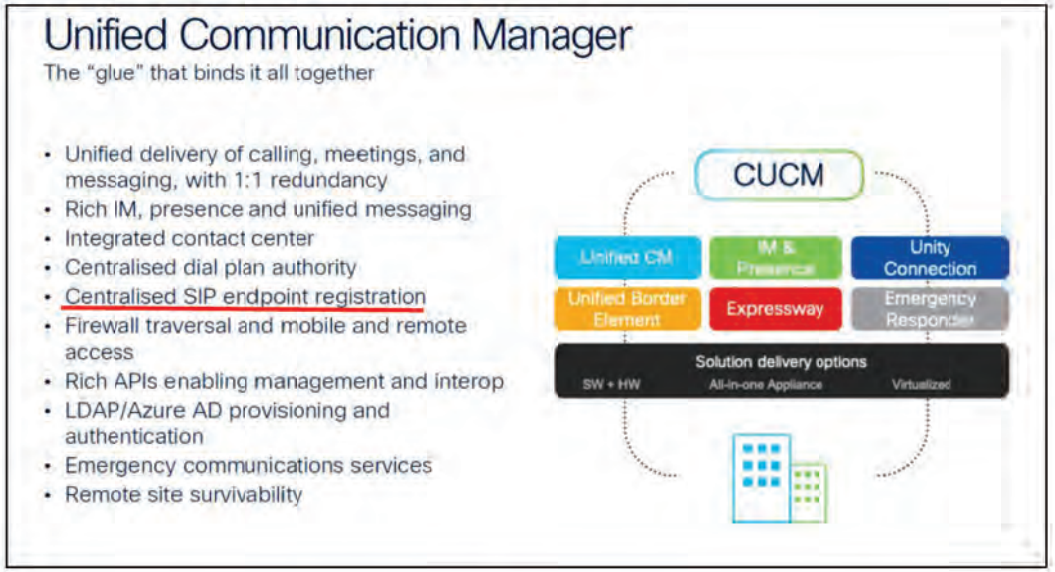
Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU4/systemConfig/cucm_b_system-configuration-guide-1251su4/cucm_m_intercluster-lookup-service.pdf; *see also* https://www.ciscopress.com/articles/article.asp?p=3089358&seqNum=2 ("The Cisco Unified Communications Manager call-routing table is built using connected devices. The table consists of directory numbers of registered IP phones and of statically entered route patterns that point to external destinations.").

To the extent this is considered an element under 35 U.S.C. §112 (¶ 6), in accordance with P.R. 3-1(c), the identity of the structure(s), act(s), or material(s) in the Accused Instrumentality that performs the claimed function include, *e.g.*, ILS uses the communication protocol HTTPS to broadcast SIP registry information to other nodes. MeshDynamics's investigation into Cisco's proprietary algorithms remains ongoing and MeshDynamics will supplement or amend its P.R. 3-1(c) identification following discovery and/or claim construction.

Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/sysConfig/11_5_1_SU1/cucm_b_system-configuration-guide-1151su1/cucm_b_system-configuration-guide-1151su1_chapter_01010101.html (ILS uses HTTPS on TCP port 7501).

	MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of updating local SIP registries in the same way by advertising and sharing a directory of URLs and achieves the same result of an updated local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because ILS shares the directory across clusters to enable VoIP calls. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 16	
The VoIP capable network of claim 15, wherein the local SIP registry of the first isolated node is updated as the VoIP clients establish or terminate a network connection with the first isolated node.	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a VoIP-capable network, in addition to the elements of claim 15 as shown above, wherein the local SIP registry of the first isolated node is updated as the VoIP clients establish or terminate a network connection with the first isolated node. *See* Claim 2 above, incorporated herein by reference.
Claim 17	
The VoIP capable network of claim 15, wherein first isolated node comes into communication with other isolated nodes to form a cluster, and the local SIP registry information of each isolated node in the cluster is updated according to information received from other	Cisco's Webex, *e.g.*, Calling in Webex App (Unified CM), is a VoIP-capable network, in addition to the elements of claim 15 as shown above, wherein first isolated node comes into communication with other isolated nodes to form a cluster, and the local SIP registry information of each isolated node in the cluster is updated according to information received from other isolated nodes in the cluster. Each node within a Unified CM cluster or multi-cluster environment comprises "a local SIP registry" and the "local SIP registry information of each isolated node in the cluster is updated according to information received from other isolated nodes in the cluster":

isolated nodes in the cluster.



Source: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2024/pdf/BRKCOL-1527.pdf.

Cluster Recommendations

Cisco Unified CM and IM and Presence support clustering, which is the grouping of nodes that work together as a single logical entity. The publisher node contains the cluster's configuration database, which is replicated to the call processing subscriber nodes and TFTP nodes in the cluster.

Clustering provides an automatic redundancy mechanism for endpoints and for Cisco Unified CM services, such as the ability to receive and process incoming calls. To provide 1:1 redundancy, deploy call processing subscribers and TFTP nodes in pairs. (Figure 6) While the call processing subscribers provide endpoint registration and call processing capabilities, the TFTP nodes provide configuration and firmware updates to endpoints.

Source: https://www.cisco.com/c/en/us/td/docs/solutions/PA/overview/14x/clbpa14x.html.

The "local SIP registry" is updated with SIP information replicated from the other nodes and/or received from other isolated clusters. Using ILS with SIP URI replication, the Unified CM clusters can share SIP URI reachability data. ILS allows multiple clusters to share user identities (including SIP URIs and directory URIs). Users can then call across clusters using SIP URIs.

INTER-Cluster URI (URI Dialing across cluster):

To enable intercluster routing of directory URIs, **Unified CM can be provisioned to exchange directory URI catalogs with other clusters through the Intercluster Lookup Service (ILS).** Each cluster configured to exchange directory URI catalogs with other clusters advertises all locally configured directory URIs in a single directory URI catalog together with a location attribute, **the SIP route string**. This location attribute in multi-cluster environments is used to direct calls for directory URIs to the correct cluster when the host portion of the directory URI cannot be used to deterministically route the SIP request. This, for example, is the case when a flat URI scheme such as *<user>@example.com* is use. The host portion "example.com" does not uniquely identify the remote Unified CM cluster that hosts a given URI.

Basically, every cluster would have a catalogue(table) of Directory URI's. Using ILS each and every cluster would share this catalogue with a local attribute i.e SIP ROUTE STRING.

Source: https://community.cisco.com/t5/collaboration-knowledge-base/sip-uri-dialing/ta-p/3157406.

Using ILS, the Unified CM clusters can create a mesh-like topology. The ILS process exchanges routing updates that contain SIP URI mappings between clusters. Each cluster stores a routing table mapping SIP URIs to cluster locations.

Source: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU4/systemConfig/cucm_b_system-configuration-guide-1251su4/cucm_m_intercluster-lookup-service.pdf; *see also* https://www.ciscopress.com/articles/article.asp?p=3089358&seqNum=2 ("The Cisco Unified Communications Manager call-routing table is built using connected devices. The table consists of directory numbers of registered IP phones and of statically entered route patterns that point to external destinations.").

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Calling for Webex App performs the same function of updating a local SIP registry in the same way by replicating and exchanging SIP information and routing updates between nodes and clusters on-premise and achieves the same result of providing the ability to operate without an external server to maintain endpoint communications at different locations. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or

	insubstantial because the nodes and clusters maintain SIP information and share this information between nodes and clusters on-premise so each has a local SIP registry. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Exhibit 4 – U.S. Patent No. 8,477,762 (Cisco Webex with Webex Video Mesh)

Cisco Systems, Inc. ("Cisco") has and continues to make, use, sell, offer for sale, and/or import the Cisco Webex VoIP Network, including but not limited to Cisco's Webex and Webex Video Mesh with related software and hardware (the "Cisco Accused Products," *see* Exhibit 7), and has infringed and infringes at least Claims 1-4 and 8-9 (the "Asserted Claims") of U.S. Patent No. 8,477,762 (the "'762 Patent").[1]

Cisco has and continues to infringe (literally and/or under the doctrine of equivalents), directly and/or through subsidiaries, agents, representatives, or intermediaries, one or more claims of the '762 Patent by making, using, testing, supplying, causing to be supplied, importing, selling, and/or offering for sale in the United States the Cisco Accused Products.

Cisco directly infringes and has infringed under 35 U.S.C. § 271(a) by making, using, selling, offering for sale and importing the Cisco Accused Products. Cisco further directly infringes and has infringed by testing, setting up, and using the Cisco Webex VoIP Network on Cisco's campuses and locations throughout the United States,[2] and/or assisting customers in setting up and servicing their Cisco Webex VoIP Networks. On information and belief, Cisco has partnered with several customers to set up an infringing Cisco Webex VoIP Network in the United States.

Cisco indirectly infringes and has infringed under 35 U.S.C. § 271(b) by providing specific guidance and instructions to its customers and end users on how to infringe the '762 Patent and make and use the infringing Cisco Webex VoIP Network. Specifically, Cisco's Preferred Architecture guides, deployment guides, Technical Assistance Center, Cisco Tech Talks, technical support, Cisco Community, presentations, and technical documentation on Cisco's website identified in the chart *infra* provide guidelines for the deployment of an infringing Cisco Webex VoIP Network. These guides and instructions specifically teach and describe each and every claim element of Claims 1-4 and 8-9 as demonstrated *infra*, including the necessary components to make and use the infringing Cisco Webex VoIP Network, and the infringing configuration and operation of Webex, Unified CM clusters, Video Mesh, and other software and hardware that comprise the infringing Cisco Webex VoIP Network. These guides and instructions were published and distributed by Cisco for its customers for the sole purpose to instruct and encourage its customers to purchase the

[1] The identified Accused Products also include Cisco's products, services, and systems that are considered sold or related to the infringement in the United States and subject to a reasonable royalty according to the Federal Circuit's decisions in *Carnegie Mellon Univ. v. Marvell Tech. Group. Ltd.*, 807 F.3d 1283 (Fed. Cir. 2015), *Cal. Inst. of Tech. v. Broadcom Ltd.*, 25 F.4th 976 (Fed. Cir. 2022), and *Brumfield v. IBG LLC*, 97 F.4th 854 (Fed. Cir. 2024).

[2] *See, e.g.*, https://www.cisco.com/c/dam/assets/video-mesh-ebook-cm-5595.pdf ("29M minutes of Cisco's Webex meetings were hosted by Video Mesh.").

Cisco components to make and use the infringing Cisco Webex VoIP Network (and directly infringe literally and/or under the doctrine of equivalents). Cisco has had knowledge of the '762 Patent since 2009 when Cisco executives met with MeshDynamics to discuss partnering opportunities and the application that would result in the '762 Patent. MeshDynamics further put Cisco on actual notice of its infringement by its making, using, selling, offering for sale and importing the Cisco Accused Products that comprise the Cisco Webex VoIP Networks (including "Mesh" functionality, such as Video Mesh nodes) in 2022. Cisco has knowingly and intentionally induced its customers to infringe the '762 Patent, or in the alternative was willfully blind to the '762 Patent and the infringement, following the MeshDynamics meeting in 2009.

Cisco further indirectly infringes and has infringed under 35 U.S.C. § 271(c) by supplying the components used in the infringing Cisco Webex VoIP Network, with knowledge of its infringing use (as discussed *supra*) and without substantial non-infringing uses. Further, the Cisco Accused Products were designed specifically to be used in a manner that infringes the '762 Patent. Cisco Accused Products come enabled as an infringing product, are particularly suited for isolated, on-premise configuration and operation, and Cisco provides specific instructions and guides on how to make and use the Cisco Webex VoIP Network using the Cisco Accused Products. As a result of Cisco's selling and/or offering for sale of the Cisco Accused Products to other entities, the other entities use these products for their intended purpose and according to their instructions with the result that such entities directly infringe the '762 Patent, literally or under the doctrine of equivalents, for the reasons stated *infra*. Cisco's Accused Products are specially made and adapted for this use in an infringing manner, are not staple articles of commerce, and do not have substantial non-infringing uses.

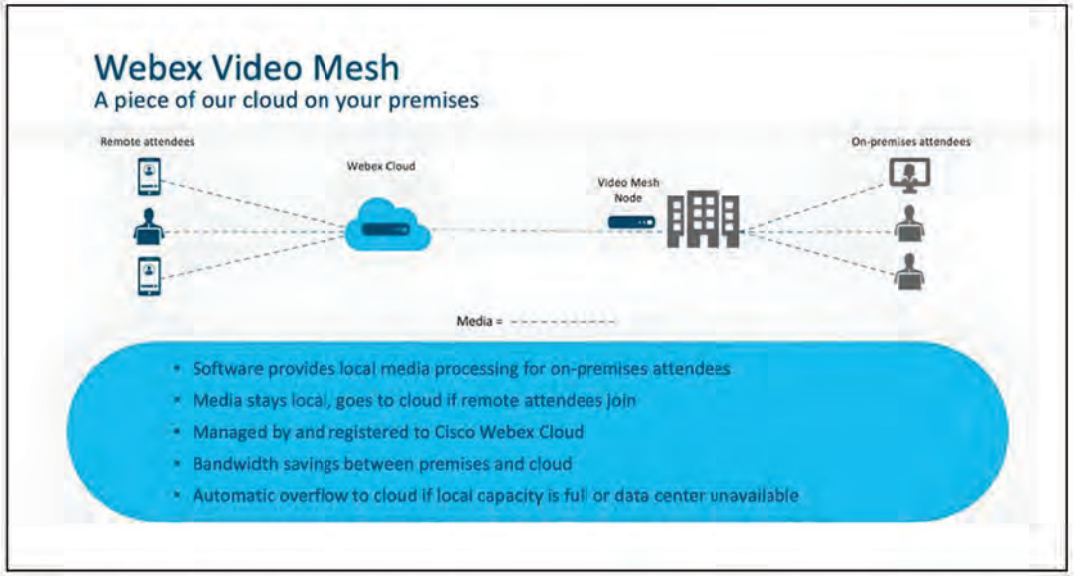
MeshDynamics asserts that the Cisco Accused Products literally infringed and continue to infringe the Asserted Claims of the '762 Patent. With respect to any claim limitation that may be found not to be literally infringed, MeshDynamics contends in the alternative that Cisco Accused Products infringed such claim limitations under the doctrine of equivalents and that any claim element not found to be literally met is equivalently met because any difference between the claim limitation and Cisco Accused Products is not a substantial difference. Accordingly, MeshDynamics contends that if any Cisco Accused Products is found not to have infringed any Asserted Claims literally it is nevertheless embodied by Cisco Accused Products under an operative doctrine of equivalents test (*e.g.*, function-way-result or insubstantial difference).

The below chart presents MeshDynamics's preliminary infringement analysis of Cisco Accused Products based solely on public information. MeshDynamics has not received any discovery from Cisco, including any confidential information or source code demonstrating the operation and structure of the Cisco Accused Products. All information contained in this disclosure is the result of publicly available information regarding the Cisco Accused Products. Based on these circumstances, MeshDynamics presents these infringement allegations reflecting its analysis of the facts

presently known to it. To the best of MeshDynamics's knowledge, information, and belief, formed after an inquiry that is reasonable under the circumstances, the information contained in this disclosure is correct.

Certain information about Cisco Accused Products is not available without discovery, such as proprietary source code, documents, and deposition testimony, from Cisco. Accordingly, MeshDynamics reserves the right to supplement and/or amend this infringement contention claim chart as new information becomes available and as MeshDynamics has the opportunity to review Cisco document productions, including information related to the implementation of Cisco Accused Products, relationships with other parties who participated or contributed to the operation of Cisco Accused Products, and/or elements of Cisco Accused Products that cannot be fully examined based solely on publicly available information. Infringement investigations are ongoing, and MeshDynamics anticipates that additional facts and relevant documents will be uncovered and disclosed that create cause for supplementation and/or amendment.

Claim 1	Cisco Webex (*e.g.*, Cisco Webex Edge with Webex Video Mesh)
A VoIP-capable network comprising:	Cisco's Webex, *e.g.*, Webex Edge with Webex Video Mesh, is a Voice over Internet Protocol-capable network in which each client can communicate with multiple other clients and that allows for optimal routing of media streams depending on network conditions and participant locations. Voice over Internet Protocol (VoIP) transmits sound as data over the internet. This lets you talk over the internet without using a phone. Webex uses VoIP so users can call into a meeting using a computer. With a paid plan, you can also call into a meeting with your phone. Source: https://www.webex.com/what-is-voip.html.



Cisco Webex Video Mesh provides on-premise media processing capabilities for Webex. This includes voice, video, and desktop sharing. This allows users to send and receive audio/video directly within the organization's network.

Source: Preferred Architecture for Cisco Webex Hybrid Services, Design Overview (New Updated – March 10, 2020): https://www.cisco.com/c/en/us/td/docs/solutions/PA/overview/12xy/hybpa12x.html.

Media can be terminated on-premises, instead of sending all media to the cloud.

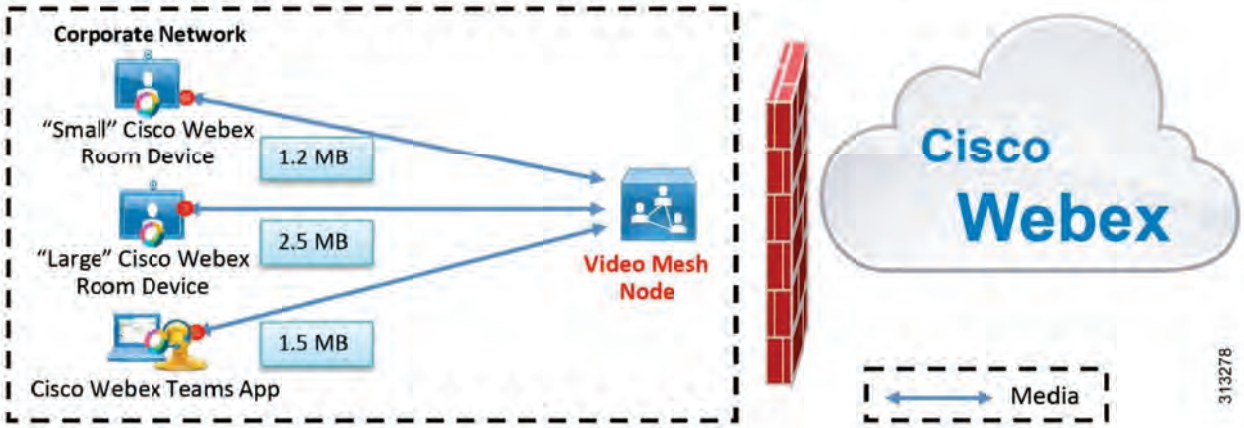
Source: Preferred Architecture for Cisco Webex Hybrid Services, Design Overview (New Updated – March 10, 2020).

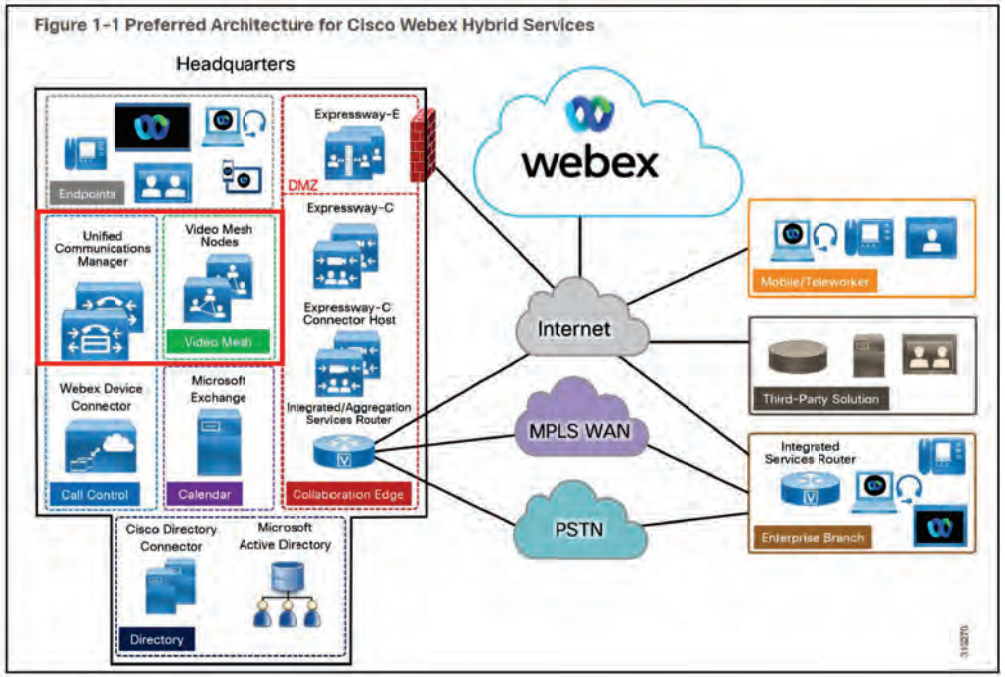
> Deliver the best meeting experience
>
> Webex Video Mesh provides great meeting experiences and enables everyone to connect, share, and collaborate. Video Mesh keeps media on-premises, providing a high-quality user experience, and allows meetings to overflow to the cloud as needed. This optimizes the return on your on-premises investment, minimizes latency, and keeps Internet bandwidth costs down.

Source: https://www.cisco.com/c/en/us/products/conferencing/webex-edge-video-mesh/index.html.

Webex Video Mesh functions without relying on the Webex cloud server by utilizing dedicated on-premises "Video Mesh nodes" within an organization's network. The Video Mesh nodes process meeting media locally instead of

	sending it through the cloud. The node thus acts as a local media server, allowing Webex users to send and receive audio/video directly within the organization's network instead of routing everything through the cloud. Source: Deployment Guide for Video Mesh: https://help.webex.com/en-us/article/2r5gv7/Deployment-Guide-for-Video-Mesh. > Video Mesh Node is software that is installed on an on-premises Cisco UCS server, registered to the cloud, and managed in Control Hub. Webex meetings, Webex Personal Meeting Room, Webex Space Meetings, and Webex App calls between two people can be routed to the local, on-net Video Mesh nodes. Video Mesh selects the most efficient way to use the available resources. Source: Deployment Guide for Video Mesh; Preferred Architecture for Cisco Webex Hybrid Services, Design Overview (New Updated – March 10, 2020); Preferred Architecture for Webex Hybrid Services, Webex Video Mesh, Cisco Validated Design (CVD) April 2023: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Collaboration/hybrid/pa_hybrid_vmn.pdf.
one or more VoIP client devices;	Cisco's Webex, *e.g.*, Webex Edge with Webex Video Mesh, is a VoIP-capable network comprising one or more VoIP client devices. Webex Video Mesh allows participants utilizing VoIP applications (*e.g.*, Webex Meetings) or hardware devices (*e.g.*, "one or more VoIP client devices") connecting to a Webex meeting to have local media processing. These devices can be registered to Webex or to an on-premises call control such as Cisco Unified Communications Manager ("Unified CM") and Cisco Expressway. Source: Cisco Preferred Architecture for the Webex Video Mesh, Design Overview March 2024: https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/WbxEdge/PAEdgeVMN.pdf; Preferred Architecture for Webex Hybrid Services, Webex Video Mesh, Cisco Validated Design (CVD) April 2023; *see also* https://help.webex.com/en-us/article/2r5gv7/Deployment-Guide-for-Video-Mesh. Cisco's Webex Video Mesh uses local media processing when users dial in to a Webex meeting from on-premises standards-based SIP endpoints and clients (*e.g.*, "one or more VoIP client devices"):

	• Uses local media processing when users dial in to a Webex meeting from on-premises standards-based SIP endpoints and clients: ◦ SIP based endpoints and clients (Cisco endpoints, Jabber, 3rd party SIP), registered to on-premises call control (Cisco Unified Communications Manager or Expressway), that call into a Cisco Webex meeting. ◦ Webex App (including paired with room devices) that join a Webex meeting. ◦ Webex room and desk devices that directly join a Webex meeting. Source: Deployment Guide for Video Mesh; Preferred Architecture for Webex Hybrid Services, Webex Video Mesh, Cisco Validated Design (CVD) April 2023.  This figure shows a three-VoIP client device call with the media bridged locally on the Video Mesh node within the enterprise, resulting in no bandwidth utilization for media over the Internet. Source: Preferred Architecture for Cisco Webex Hybrid Services, Design Overview (New Updated – March 10, 2020).
two or more VoIP nodes forming an isolated cluster wherein the two or more VoIP nodes in the isolated cluster are in	Cisco's Webex, *e.g.*, Webex Edge with Webex Video Mesh, is a VoIP-capable network comprising two or more VoIP nodes forming an isolated cluster that are in communication with one another wherein each of the VoIP client devices communicates with at least one VoIP node.

communication with one another; wherein each of the VoIP client devices communicates with at least one VoIP node;	SIP endpoints are registered with a Unified CM cluster on-premise, which operates in isolation without the need to connect to an external datacenter. Unified CM handles certain SIP signaling (call setup, registration, etc.) for these devices. Session Initiation Protocol ("SIP") signaling refers to the communication protocol used to establish a connection, manage media streams, and coordinate the flow of video data between participants, including how to route it efficiently across the mesh nodes. This information includes Session Description Protocol ("SDP") information. The Unified CM nodes (*e.g.*, "VoIP nodes") are a part of the Webex Hybrid Services architecture that includes Webex "Video Mesh Nodes." > Cisco Webex Video Mesh is a component of Webex Hybrid Services that allows organizations to deploy an instance of Webex media processing on-premises. This means that Webex Teams devices and applications can terminate media on-premises instead of sending all media to the cloud. SIP endpoints registered to Cisco Unified Communications Manager (Unified CM) can also use Video Mesh services when dialing into Webex Meetings. Source: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf. Figure 1-1 Preferred Architecture for Cisco Webex Hybrid Services 

Source: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12xy/hybcvd/intro.html.

Each of the VoIP client devices establishes a connection and communicates directly to the Unified CM cluster/nodes (*e.g.*, "wherein each of the VoIP client devices communicates with at least one VoIP node") and designated Video Mesh nodes including for SIP signaling and to send and receive media streams. When a client joins a meeting, the Video Mesh node that first handles the communication gathers information about the client. For example, a Video Mesh node accepts the SIP signaling (*e.g.*, INVITE) and gathers metadata and other SIP information such as device type, media formats, network characteristics, and/or location and organization affiliation.

Deploying Webex Video Mesh for SIP Endpoints

SIP endpoints registered to Cisco Unified CM can send audio, video, and screen share content to a Webex Video Mesh cluster when joining Webex Meetings, provided that the Webex Meetings site is configured to allow Webex Video Mesh.

The following statements describe how Unified CM SIP endpoints can use Webex Video Mesh for Webex Meetings (see Figure 4-11).

- A Unified CM SIP trunk can be pointed to nodes in a Video Mesh Cluster.
- A Unified CM SIP trunk to a Video Mesh cluster may be secured with TLS, and SIP endpoint media through the Video Mesh cluster may be encrypted.
- A Unified CM SIP route pattern can route calls based on a specific domain (for example, sitename.webex.com) via the SIP trunk to a node in the Video Mesh cluster.
- The Video Mesh Node will signal to Webex to set up a meeting, and Webex will determine the cluster node where the meeting will be hosted.
- The Video Mesh Node will then signal to Unified CM to indicate which node in the cluster should be used for media.
- The SIP endpoint will send media to the selected node.

Figure 4-11 SIP Endpoints Sending Media via a Video Mesh Cluster

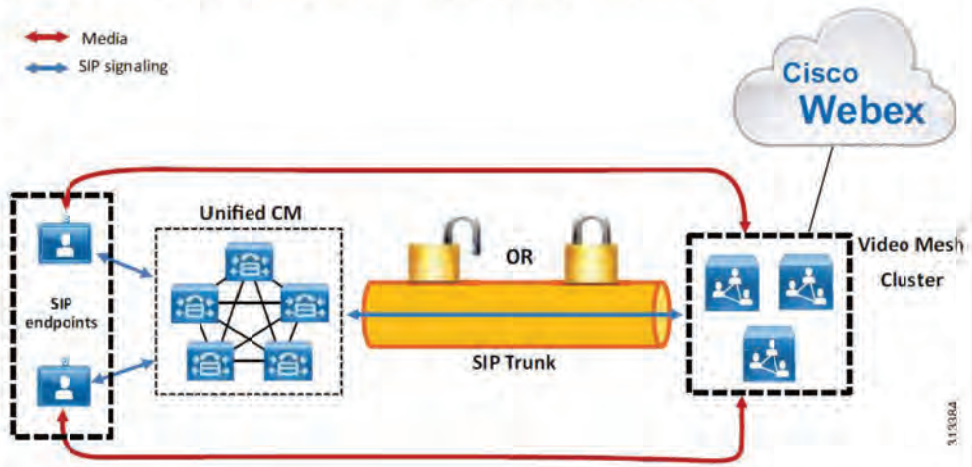


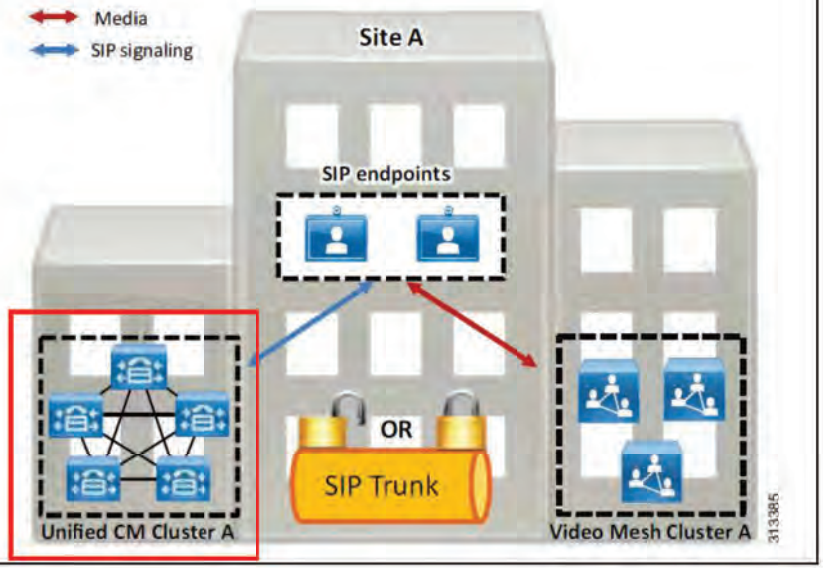
Table 4-5 Port Range Requirements to Allow SIP Endpoints to Use Webex Video Mesh Services

Description	Source IP Address	Destination IP Address	Source Ports	Destination Ports	Protocol
Unified CM SIP signaling to Video Mesh cluster	Unified CM	Video Mesh Node	5060	5060	TCP
SIP endpoint signaling to Video Mesh cluster	SIP Endpoint	Video Mesh Node	5060 to 5062	5060 to 5062	TCP
SIP endpoint media to Video Mesh cluster	SIP Endpoint	Video Mesh Node	ANY	52500 to 62999 for audio 63000 to 65500 for video	UDP

Source: Preferred Architecture for Cisco Webex Hybrid Services, Design Overview (New Updated – March 10, 2020); Preferred Architecture for Webex Hybrid Services, Webex Video Mesh, Cisco Validated Design (CVD) April 2023; Understanding the call flows for the Video Mesh Solution, BRKCOL – 2750 (Cisco Live), https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKCOL-2750.pdf; https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf.

The Unified CM nodes (*e.g.*, "two or more VoIP nodes forming an isolated cluster" (*see* "Cluster A" below)) are set up in an isolated cluster on-premise like the Video Mesh nodes and integrated with the Video Mesh nodes via a SIP trunk. The nodes in the Unified CM cluster are in constant communication with each other:

Figure 4-12 SIP Trunk Configured to Point to a Video Mesh Cluster



Source: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf; *see also* https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/install/15/cucm_b_install-guide-cucm-imp-15/cucm_m_planning-the-installation.html; Exhibit 3 (explaining communication between Unified CM nodes in a cluster, incorporated herein by reference).

The Video Mesh nodes act as relays to efficiently route audio/video media between participants in a Webex call, optimizing bandwidth usage and call quality. The nodes must be accessible from the corporate network. The nodes act as local media servers, allowing Webex users to send and receive audio/video directly within the organization's network instead of routing everything through the cloud.

Deploy Video Mesh Nodes in the enterprise network to provide local media processing. By processing audio and video media locally, the Video Mesh Nodes deliver a better quality experience for audio, video, and content sharing in meetings. A Video Mesh Node can also reduce or eliminate bandwidth consumption from the enterprise network to the Webex cloud. Webex Teams also provides automatic overflow to Media Nodes in the Webex cloud when large meetings/large numbers of meetings exhaust the locally available Video Mesh Node resources.

Source: Webex Teams Tech Ops and Security – Frequently Asked Questions (FAQs): https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Webex-Teams-Security-Frequently-Asked-Questions.pdf; Preferred Architecture for Webex Hybrid Services, Webex Video Mesh, Cisco Validated Design (CVD) April 2023.

The Video Mesh nodes are deployed in isolated clusters on-premise. This provides high availability for internal users in case a single Video Mesh node becomes unavailable. A cluster defines Video Mesh nodes with similar attributes, such as network proximity. The nodes in a Video Mesh cluster require unimpeded communication with one another.

The nodes in a Video Mesh cluster require unimpeded communication with each other. They also require unimpeded communication with the nodes in all your other Video Mesh clusters. Ensure that your firewalls allow all communication between the Video Mesh nodes.

Source: Deployment Guide for Video Mesh; Preferred Architecture for Cisco Webex Hybrid Services, Design Overview (New Updated – March 10, 2020); Cisco Preferred Architecture for the Webex Video Mesh, Design Overview March 2024.

Clustering

Video Mesh Nodes are deployed in clusters and within the cluster the more nodes added increases the capacity to host more Webex devices and applications meeting media. It also provides redundancy in case a single node becomes unavailable for any reason because the Video Mesh Nodes are in an active/active state.

	Source: Preferred Architecture for Webex Hybrid Services, Webex Video Mesh, Cisco Validated Design (CVD) April 2023. Webex Video Mesh nodes communicate with each other directly over a dedicated network, allowing for local media processing of video, audio, and content within an organization's network and creating a "mesh" where data can flow between multiple nodes depending on the participant's location. Source: Preferred Architecture for Webex Hybrid Services, Webex Video Mesh, Cisco Validated Design (CVD) April 2023; https://help.webex.com/en-us/article/npgz5ph/Media-Health-Monitoring-for-Video-Mesh. *Table 4-2 Traffic Signatures for Management of Video Mesh Nodes (continued)* **Source** / **Destination** / **Source Address** / **Source Port** / **Protocol** / **Destination Address** / **Destination Port** Video Mesh Node / Webex cloud media services / Video Mesh Node IP address / ANY / TCP HTTPS / *.docker.io *.wbx2.com *.webex.com / 443 Video Mesh Node #1 / Video Mesh Node #2 / Video Mesh Node #1 IP address / ANY / TCP HTTPS / Video Mesh Node #2 address / 5000 5001 Source:https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf. MeshDynamics asserts that these claim elements are software limitations. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If these claim elements are not literally infringed, they are infringed under the doctrine of equivalents. Cisco's Webex Video Mesh performs the same function of forming an isolated cluster of VoIP nodes in communication with each other and VoIP devices in the same way by utilizing multiple on-premise servers (*e.g.*, Unified CM) that share data and achieves the same result of an on-premise (not in the cloud and without an external SIP server) VoIP network for maintaining device and endpoint communication. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the Unified CM nodes (integrated with the Video Mesh nodes) provide on-premise VoIP communication. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
wherein each of the VoIP nodes further comprises a local SIP registry built by	Cisco's Webex, *e.g.*, Webex Edge with Webex Video Mesh, is a VoIP-capable network wherein each of the VoIP nodes further comprises a local SIP registry built by exchanging SIP information with the remaining VoIP nodes in the isolated cluster.

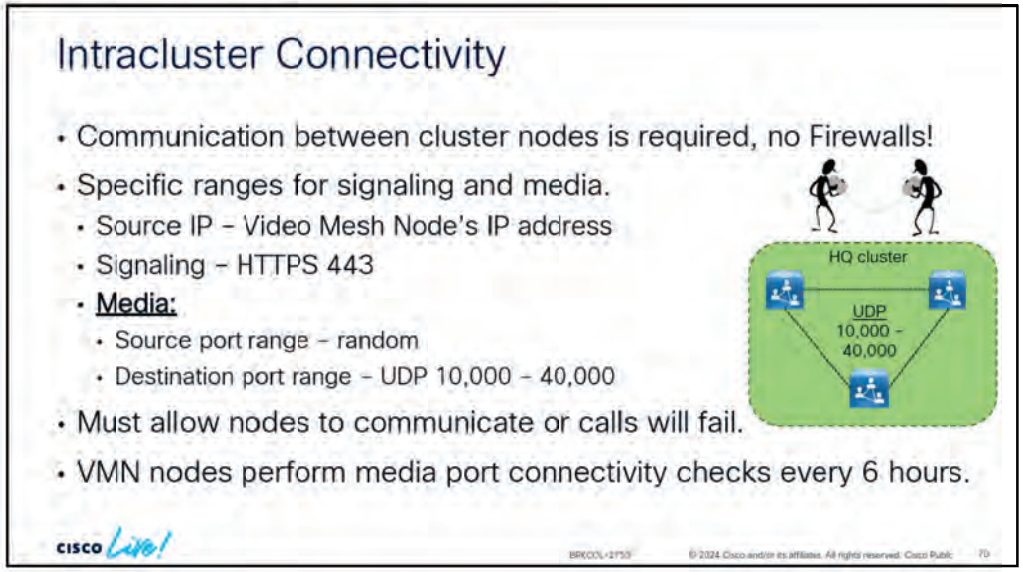
exchanging SIP information with the remaining VoIP nodes in the isolated cluster;	Cisco positions Video Mesh (with Unified CM) as Preferred Architecture for Webex Hybrid Solutions designed to ensure high availability, resilience, local survivability, and efficiency, even in cases of cloud connectivity issues. Source: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12xy/hybcvd/intro.html. **High Availability** The PA for Webex Hybrid Services provides high availability for all deployed on-premises applications by means of the underlying clustering mechanism present in all Cisco Unified Communications applications. Clustering replicates the administration and configuration of deployed applications to backup instances of those applications. Likewise, cloud services are natively redundant by virtue of elastic compute and highly available service distribution within the cloud platform. If an instance of an application or services fails, Cisco on-premises and cloud-based services such as endpoint registration, call processing, messaging, and many others continue to operate on the remaining instance(s) of the application or service. This failover process is transparent to the users. In addition to clustering, the PA for Webex Hybrid Services provides high availability through the use of redundant power, network connectivity, and elastic storage. Source: Preferred Architecture for Cisco Webex Hybrid Services, Design Overview (New Updated – March 10, 2020). The Unified CM clusters ("VoIP nodes") are integrated with and communicate SIP information to the Video Mesh node clusters, and the Unified CM nodes and clusters exchange routing information about SIP endpoints to build a local SIP registry (*e.g.*, "each of the VoIP nodes further comprises a local SIP registry built by exchanging information with the remaining VoIP nodes in the isolated cluster"). The last partition onNetRemote is only used in a multi-cluster environment where routing information is exchanged between Unified CM clusters using Intercluster Lookup Service (ILS) or Global Dialplan Replication (GDPR). Source: https://help.webex.com/en-us/article/nqqzbk7/Configure-Unified-CM-for-Webex-Calling; *see also* Exhibit 3 (explaining the fully meshed Unified CM clusters and ILS for this claim element, showing how each Unified CM node is a local SIP registry built by exchanging information with other Unified CM nodes and cluster, incorporated herein by reference). Video Mesh nodes can also manage SIP signaling locally and can react to network disruptions and changes and route media streams within the local network without relying solely on a remote server, *i.e.*, cloud connectivity.

Source: Preferred Architecture for Webex Hybrid Services, Webex Video Mesh, Cisco Validated Design (CVD) April 2023.

For example, Video Mesh nodes terminate SIP signaling during Webex meetings when a SIP endpoint joins via CVI (Cloud Video Interop), Webex Edge for Devices or Direct SIP dial-in (to @webex.com or internal meeting URI). In these scenarios, the SIP INVITE from the endpoint (routed via Unified CM or direct) reaches the Video Mesh node if the Webex cloud delegates that node to handle the session. The Video Mesh node is listening on standard SIP ports (typically TCP/UDP 5060 or TLS 5061) to accept and respond to these INVITEs.

Source: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf.

On information and belief, the Video Mesh nodes also manage modifications, such as adding or deleting media streams, and are also "two or more VoIP nodes forming an isolated cluster" and meet this claim limitation and the previous claim limitation as "VoIP nodes" (in addition to the Unified CM cluster and nodes). For example, the Video Mesh node may send a re-INVITE when a client turns on or off video or audio. Video Mesh nodes, therefore, do not require continuous external SIP registry access (*i.e.*, cloud connectivity) to maintain and manage calls. If endpoints have already registered with a node, for example, the node can continue to facilitate communication between them without external SIP registry access on the Webex cloud. On information and belief, the Video Mesh nodes exchange session information that assists in call delegation and intra-cluster cascading.



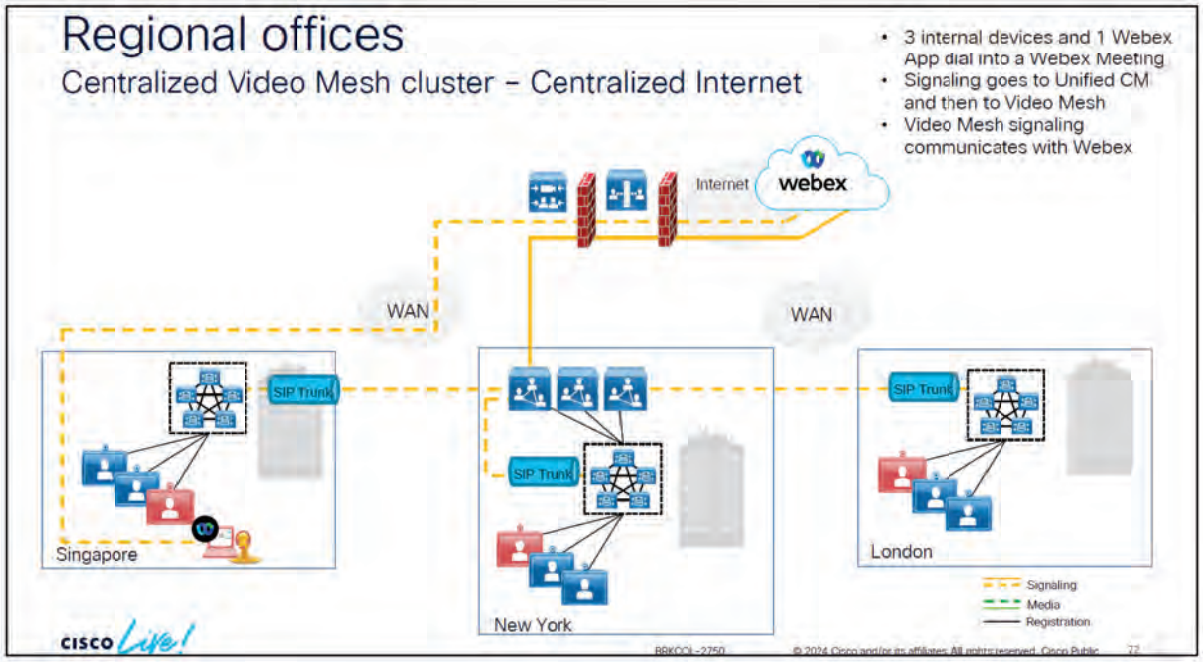
	Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKCOL-2750.pdf. The Video Mesh nodes have a cache. https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/WbxEdge/PAEdgeVMN.pdf ("At the point of startup, network change, or cache expiration which is every 2 hours, the video endpoint or application will ask Webex for a list of media resources that are candidates for the video endpoint or application to use as a media resource."); https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.html ("The cache expiry time for media node discovery is 2 hours. When new Video Mesh Nodes are added to a deployment, it may take Webex endpoints up to 2 hours to recognize this event."). On information and belief, the cached information includes SIP signaling information. The cache at least holds SIP signaling information in memory while an active call is in progress, so that existing sessions can continue. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Video Mesh performs the same function of building a local SIP registry in the same way by replicating and exchanging SIP information between nodes and clusters on-premise and achieves the same result of providing the ability to operate without an external server to maintain endpoint communications and VoIP calls. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the Unified CM clusters perform SIP registration and share this information between nodes and clusters on-premise. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
wherein a first VoIP client device in communication with a first VoIP node establishes a communication with a second VoIP device in communication with a second VoIP node using the local SIP registries of the first VoIP node and the second VoIP node.	Cisco's Webex, *e.g.*, Webex Edge with Webex Video Mesh, is a VoIP-capable network wherein a first VoIP client device in communication with a first VoIP node establishes a communication with a second VoIP device in communication with a second VoIP node using the local SIP registries of the first VoIP node and the second VoIP node. The Unified CM "VoIP nodes" and clusters meet this claim limitation. *See* Exhibit 3 for this claim element, showing that the Unified CM nodes and clusters connect VoIP devices (incorporated herein by reference). In addition, for SIP call handling, SIP endpoints (*e.g.*, Cisco video phones registered to the Unified CM) can continue to place and receive SIP calls that are routed through the Video Mesh node, even if there is no cloud connectivity. If the SIP trunk is configured to route calls through the Video Mesh node as a local media resource, point-to-point or multi-party SIP calls will still work. On-premises media is still processed by the Video Mesh node as long as the SIP trunk to Unified CM is active.

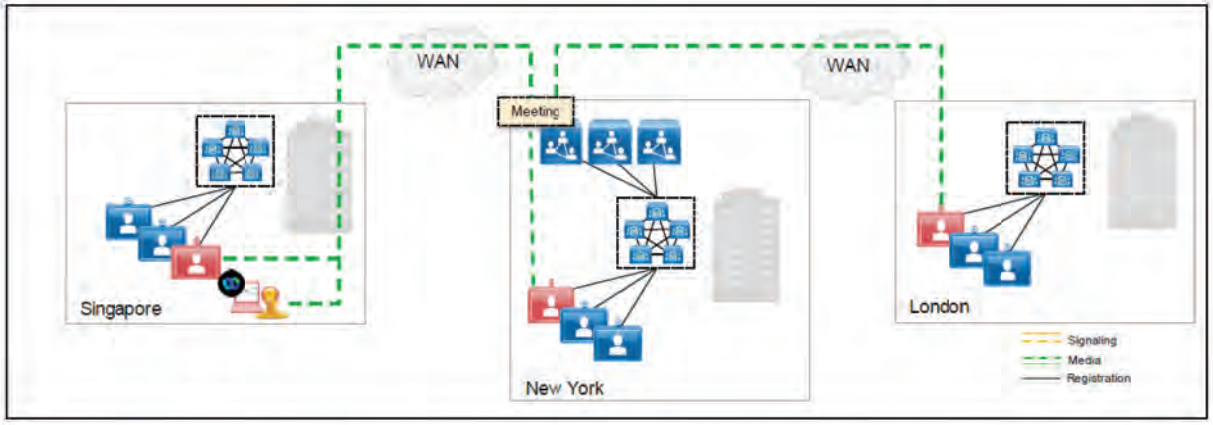
On information and belief, each Video Mesh node also maintains at least a partial SIP registry so that they can make calls in the absence of the cloud server. Webex cloud signaling is not needed, and the SIP endpoints communicate directly with the Video Mesh nodes for media processing. The Video Mesh nodes can host meetings locally.

> **Point to Point call flows**
>
> The Video Mesh is a media resource available for Webex meetings. It is not a standalone bridge and always requires communication to Webex but does not always need to create cascades to Webex for all meetings. The Video Mesh can host meetings locally. For example, a meeting can be two participants in a point-to-point call or many participants in a meeting. Figure 32 shows an example where two cloud registered participants, a video device, and Webex App (without the Full Featured Webex Experience), are calling each other to meet. The media for each participant will be hosted on the Video Mesh and will not go directly between the participants.

Source: https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/WbxEdge/PAEdgeVMN.pdf.

When all participants are on-premises and the Video Mesh node has capacity to host those participants, a cascade (*i.e.*, cloud connectivity) is not needed.



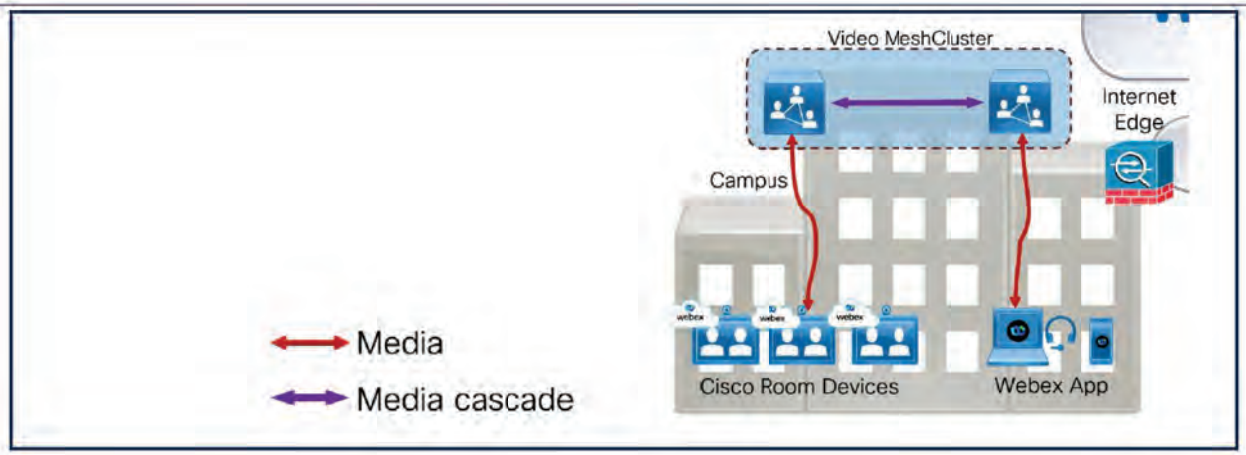


Source: https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/WbxEdge/PAEdgeVMN.pdf.

Meetings are distributed across nodes, and clients land on the most efficient node nearest to them, depending on factors such as network topology, WAN link and resource utilization. When multiple participants in a Webex meeting are connected to different Video Mesh nodes within the same organization, their video and audio data will be exchanged directly between those nodes on the company's internal network.

Source: Deployment Guide for Video Mesh.

At meeting time, Webex directs the endpoint to use a particular node in that cluster. Two Webex endpoints in the same site, attending the same meeting, will typically be assigned to the same Video Mesh Node by Webex. However, Webex endpoints attending the same meeting may be assigned to different nodes in the cluster if one of the nodes becomes full. In that case the meeting will be cascaded across the nodes within the same cluster, as illustrated in Figure 7.



Source: Preferred Architecture for Webex Hybrid Services, Webex Video Mesh, Cisco Validated Design (CVD) April 2023.

On information and belief, as shown in Cisco's proprietary code, Video Mesh nodes (in addition to the Unified CM nodes and cluster) act independently to manage SIP signaling and clients in their respective areas. Video Mesh nodes keep track of where a client can be reached by monitoring network connectivity and use this information to route media streams to the most optimal path, *e.g.*, intracluster cascade, which includes identifying the best available Video Mesh node based on the client's location and network. If the endpoints have already registered with a node, for example, the nodes can continue to facilitate communication between them without external SIP registry access on the Webex cloud. On information and belief, the nodes can share and exchange information of clients in contact with each node to facilitate communications between their respective clients and meet this claim limitation in addition to the Unified CM "VoIP nodes."

> Point to Point call flows
>
> The Video Mesh is a media resource available for Webex meetings. It is not a standalone bridge and always requires communication to Webex but does not always need to create cascades to Webex for all meetings. The Video Mesh can host meetings locally. For example, a meeting can be two participants in a point-to-point call or many participants in a meeting. Figure 32 shows an example where two cloud registered participants, a video device, and Webex App (without the Full Featured Webex Experience), are calling each other to meet. The media for each participant will be hosted on the Video Mesh and will not go directly between the participants.

Preferred Architecture for Cisco Webex Hybrid Services, CVD: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.html ("Webex Teams

	devices and applications can terminate media on-premises instead of sending all media to the cloud"); Keep your media on Video Mesh for all external Webex meetings: https://help.webex.com/en-us/article/nzvixgk/Keep-your-media-on-Video-Mesh-for-all-external-Webex-meetings; Cisco Preferred Architecture for the Webex Video Mesh, Design Overview March 2024 ("The Webex Video Mesh is an extension of Webex Meetings that allows for local media processing of participant's video, audio, and content on a corporate network."); *see also* https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKCOL-2750.pdf. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Video Mesh performs the same function of establishing a communication between two endpoints in a VoIP network on-premise in the same way by using on-premise SIP information at each node and cluster and achieves the same result of establishing a VoIP call between two endpoints. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Unified CM and Video Mesh nodes will establish a connection between endpoints using on-premise nodes and clusters and their SIP registries. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 2	
The VoIP-capable network of claim 1, wherein the local SIP registries of the isolated VoIP nodes are updated as the VoIP nodes and the VoIP client devices begin communication with the isolated cluster and end communication with the isolated cluster.	Cisco's Webex, *e.g.*, Webex Edge with Webex Video Mesh, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein the local SIP registries of the isolated VoIP nodes are updated as the VoIP nodes and the VoIP client devices begin communication with the isolated cluster and end communication with the isolated cluster. *See* Exhibit 3, Claim 2 (incorporated herein by reference for Unified CM nodes and operation). On information and belief, the Video Mesh nodes' cache updates as the client devices begin and end communication, and meets this claim limitation. *See supra* Claim 1. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Video Mesh performs the same function of updating local SIP registries in the same way by exchanging information learned from other nodes and clusters and achieves the same result of updated local SIP registries for on-premise calls.

<table>
<tr><td></td><td>Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the local SIP registries of each node or cluster on-premise are updated. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.</td></tr>
<tr><th>Claim 3</th><th></th></tr>
<tr><td>The VoIP-capable network of claim 1, wherein updates to the local SIP registry of a VoIP node are communicated to remaining VoIP nodes in the isolated cluster by broadcasting one or more information packets containing local SIP registry information of the VoIP node.</td><td>Cisco's Webex, e.g., Webex Edge with Webex Video Mesh, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein updates to the local SIP registry of a VoIP node are communicated to remaining VoIP nodes in the isolated cluster by broadcasting one or more information packets containing local SIP registry information of the VoIP node.

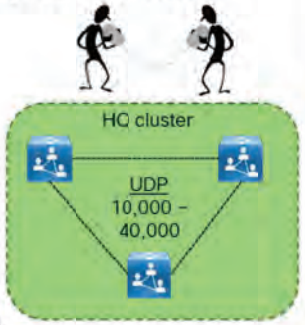
See Exhibit 3, Claim 3 (incorporated herein by reference for Unified CM nodes and operation).

The Webex Video Mesh nodes communicate via packet-based TCP protocol and HTTPS, including for SIP signaling and maintaining calls. On information and belief, tis includes updates to the local SIP registry. See supra Claim 1.

Table 4-2 Traffic Signatures for Management of Video Mesh Nodes (continued)
<table><tr><th>Source</th><th>Destination</th><th>Source Address</th><th>Source Port</th><th>Protocol</th><th>Destination Address</th><th>Destination Port</th></tr><tr><td>Video Mesh Node</td><td>Webex cloud media services</td><td>Video Mesh Node IP address</td><td>ANY</td><td>TCP
HTTPS</td><td>*.docker.io
*.wbx2.com
*.webex.com</td><td>443</td></tr><tr><td>Video Mesh Node #1</td><td>Video Mesh Node #2</td><td>Video Mesh Node #1 IP address</td><td>ANY</td><td>TCP
HTTPS</td><td>Video Mesh Node #2 address</td><td>5000
5001</td></tr></table>
Source:https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf.</td></tr>
</table>

Intracluster Connectivity

- Communication between cluster nodes is required, no Firewalls!
- Specific ranges for signaling and media.
  - Source IP – Video Mesh Node's IP address
  - Signaling – HTTPS 443
  - **Media:**
    - Source port range – random
    - Destination port range – UDP 10,000 – 40,000
- Must allow nodes to communicate or calls will fail.
- VMN nodes perform media port connectivity checks every 6 hours.



cisco Live!

BRKCOL-2750 ©2024 Cisco and/or its affiliates. All rights reserved. Cisco Public 70

Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKCOL-2750.pdf.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

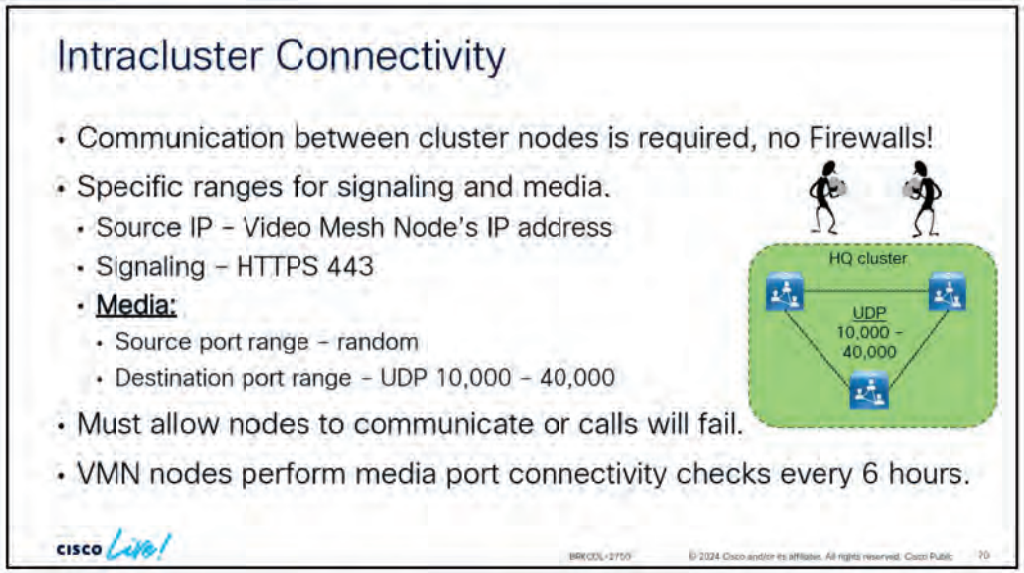
If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Video Mesh performs the same function of updating local SIP registries in the same way by sharing signaling between nodes, and achieves the same result of an updated local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the mesh nodes shares information to enable VoIP calls. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Claim 4	
The VoIP-capable network of claim 1, wherein the local SIP registry of a VoIP node is updated according to information received from another VoIP nodes in the isolated cluster in special information packets that each contain local SIP registry information of another VoIP node.	Cisco's Webex, *e.g.*, Webex Edge with Webex Video Mesh, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein the local SIP registry of a VoIP node is updated according to information received from another VoIP nodes in the isolated cluster in special information packets that each contain local SIP registry information of another VoIP node. *See* Exhibit 3, Claim 4 (incorporated herein by reference for Unified CM nodes and operation). The Webex Video Mesh nodes communicate via packet-based TCP protocol and HTTPs, including for SIP signaling and maintaining calls. The packets are "special information packets" for communicating solely between cluster nodes. On information and belief, tis includes updates to the local SIP registry. *See supra* Claim 1.

Table 4-2 Traffic Signatures for Management of Video Mesh Nodes (continued)

Source	Destination	Source Address	Source Port	Protocol	Destination Address	Destination Port
Video Mesh Node	Webex cloud media services	Video Mesh Node IP address	ANY	TCP HTTPS	*.docker.io *.wbx2.com *.webex.com	443
Video Mesh Node #1	Video Mesh Node #2	Video Mesh Node #1 IP address	ANY	TCP HTTPS	Video Mesh Node #2 address	5000 5001

Source:https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.pdf.



Source: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKCOL-2750.pdf.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Video Mesh performs the same function of updating local SIP registries in the same way by sharing signaling between nodes, and achieves the same result of an updated local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the mesh nodes shares information to enable VoIP calls. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Claim 8	
The VoIP-capable network of claim 1 wherein said nodes comprise mesh nodes.	Cisco's Webex, *e.g.*, Webex Edge with Webex Video Mesh, in addition to the elements of claim 1 as shown above, is a VoIP-capable network wherein said nodes comprise mesh nodes. *See* Exhibit 3, Claim 8 (incorporated herein by reference for Unified CM nodes and operation).

	Webex Video Mesh nodes are on-premises servers that create a mesh by processing media locally for on-site users. Multiple nodes can be deployed in different locations to create a distributed network that "meshes" with the Unified CM. Webex Video Mesh leverages a piece of Webex's cloud services and is deployed within a customer's premises. This localized setup facilitates media processing within the corporate network and decreases dependency on internet bandwidth, and results in minimizing latency, ensuring enhanced privacy, regulatory compliance, and delivering a superior user experience for meetings and collaborations. Customers can set up Video Mesh nodes in multiple locations, optimizing media quality within each site and efficiently managing bandwidth between locations. If the on-premises nodes reach capacity, the system seamlessly uses cloud nodes to handle additional demand. Additionally, the Video Mesh nodes receive automatic updates to ensure they're running the latest version. Source: https://blog.webex.com/collaboration/hybrid-work/business-class-experience-with-video-mesh-and-thousandeyes/. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Video Mesh performs the same function of completing VoIP calls without an external server in the same way using nodes in communication and exchanging information locally and achieves the same result a local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Cisco's own documentation refers to the nodes as "Mesh" nodes. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 9	
The VoIP-capable network of claim 8 wherein said mesh nodes	Cisco's Webex, *e.g.*, Webex Edge with Webex Video Mesh, is a VoIP-capable network, in addition to the elements of claim 1 as shown above, wherein said mesh nodes provide VoIP optimized services within said mesh nodes.

provide VoIP optimized services within said mesh nodes.	*See* Exhibit 3, Claim 9 (incorporated herein by reference for Unified CM nodes and operation). Webex Video Mesh nodes provide VoIP optimized services by keeping video media processing on-premises, which reduces latency, packet loss, and internet bandwidth consumption for improved call quality. Video Mesh nodes also provide simplified, centralized management through cloud-based control, seamless overflow to the cloud when on-premises capacity is exceeded, and automated updates. **Deliver the best meeting experience** Webex Video Mesh provides great meeting experiences and enables everyone to connect, share, and collaborate. Video Mesh keeps media on-premises, providing a high-quality user experience, and allows meetings to overflow to the cloud as needed. This optimizes the return on your on-premises investment, minimizes latency, and keeps Internet bandwidth costs down. Source: https://www.cisco.com/c/en/us/products/conferencing/webex-edge-video-mesh/index.html. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's Webex Video Mesh performs the same function of completing VoIP calls without an external server in the same way using nodes in communication with each node and exchanging information locally and achieves the same result a local SIP registry so VoIP calls can be made without an external server. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because Cisco's documents confirm that the Webex Video Mesh optimizes on-premise communications. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Exhibit 5 – U.S. Patent No. 8,514,852 (Cisco SD-WAN with Forward Error Correction)

Cisco Systems, Inc. ("Cisco") has and continues to make, use, sell, offer for sale, and/or import the Cisco Software-Defined Wide Area Network (SD-WAN), including but not limited to Cisco's Catalyst SD-WAN with Forward Error Correction (FEC) and related software and hardware (the "Cisco Accused Product," *see* Exhibit 7), and infringed at least Claims 1, 5 and 7 (the "Asserted Claims") of U.S. Patent No. 8,514,852 (the "'852 Patent").[1]

Cisco has and continues to infringe (literally and/or under the doctrine of equivalents), directly and/or through subsidiaries, agents, representatives, or intermediaries, one or more claims of the '852 Patent by making using, testing, supplying, causing to be supplied, importing, selling, and/or offering for sale in the United States the Cisco Accused Products.

Cisco directly infringes and has infringed under 35 U.S.C. § 271(a) by making, using, selling, offering for sale and importing the Cisco Accused Products. Cisco further directly infringes and has infringed by testing, setting up, and using the Cisco SD-WAN on Cisco's campuses and locations throughout the United States, and/or assisting customers in setting up and servicing their Cisco SD-WANs. On information and belief, Cisco has partnered with several customers to set up an infringing Cisco SD-WAN in the United States.[2]

Cisco indirectly infringes and has infringed under 35 U.S.C. § 271(b) by providing specific guidance and instructions to its customers and end users on how to infringe the '852 Patent and make and use the infringing Cisco SD-WAN. Specifically, Cisco's SD-WAN deployment guides, Technical Assistance Center, Cisco Tech Talks, technical support, Cisco Community, presentations, and technical documentation on Cisco's website identified in the chart *infra* provide design and deployment guidelines for the deployment of an infringing Cisco SD-WAN. These guides and instructions were published and distributed by Cisco for its customers for the sole purpose to instruct and encourage its customers to purchase the Cisco components to make and use the infringing Cisco SD-WAN (and directly infringe literally and/or under the doctrine of equivalents). Cisco has had knowledge of the '852 Patent since 2009 when Cisco executives met with MeshDynamics to discuss partnering opportunities and the application that would result in the '852 Patent. MeshDynamics further put Cisco on actual notice of its infringement by its making, using, selling, offering for sale and importing the Cisco Accused Products that comprise the Cisco SD-WAN in 2022. Cisco has knowingly and intentionally induced its customers to infringe the '852 Patent, or in the alternative was willfully blind to the '852

[1] The identified Accused Products also include Cisco's products, services, and systems that are considered sold or related to the infringement in the United States and subject to a reasonable royalty according to the Federal Circuit's decisions in *Carnegie Mellon Univ. v. Marvell Tech. Group. Ltd.*, 807 F.3d 1283 (Fed. Cir. 2015), *Cal. Inst. of Tech. v. Broadcom Ltd.*, 25 F.4th 976 (Fed. Cir. 2022), and *Brumfield v. IBG LLC*, 97 F.4th 854 (Fed. Cir. 2024).

[2] *See, e.g.*, https://learningnetwork.cisco.com/s/article/cisco-catalyst-sd-wan-optimizations-for-starlink; https://www.cisco.com/c/dam/m/en_us/solutions/industries/education/new-education-landscape-of-networking/pdf/SD-WAN_for_Education.pdf.

Patent and the infringement, following the MeshDynamics meeting in 2009.

Cisco further indirectly infringes and has infringed under 35 U.S.C. § 271(c) by supplying the components used in the infringing Cisco SD-WAN, with knowledge of its infringing use (as discuss *supra*) and without substantial non-infringing uses. Further, the Cisco Accused Products were designed specifically to be used in a manner that infringes the '852 Patent. Cisco Accused Products come enabled with FEC features to successfully transmit packets. Cisco advertises the FEC feature such that the SD-WAN is specifically designed to benefit from FEC. As a result of Cisco's selling and/or offering for sale the Cisco Accused Products to other entities, the other entities use these products for their intended purpose and according to their instructions with the result that such entities directly infringed the '852 Patent, literally or under the doctrine of equivalents, for the reason stated *infra*. Cisco's Accused Products are specially made and adapted for this use in an infringing manner, are not staple articles of commerce, and do not have substantial non-infringing uses.

MeshDynamics asserts that Cisco Accused Products literally infringed and continue to infringe the Asserted Claims of the '852 Patent. With respect to any claim limitation that may be found not to be literally infringed, MeshDynamics contends in the alternative that Cisco Accused Products infringed such claim limitations under the doctrine of equivalents and that any claim element not found to be literally met is equivalently met because any difference between the claim limitation and Cisco Accused Products is not a substantial difference. Accordingly, MeshDynamics contends that if any Cisco Accused Products is found not to have infringed any Asserted Claims literally it is nevertheless embodied by Cisco Accused Products under an operative doctrine of equivalents test (*e.g.*, function-way-result or insubstantial difference).

The chart below presents MeshDynamics' preliminary infringement analysis of Cisco Accused Products based solely on public information. MeshDynamics has not received any discovery from Cisco, including any confidential information or source code demonstrating the operation and structure of the Cisco Accused Products. All information contained in this disclosure is the result of publicly available information regarding the Cisco Accused Products. Based on these circumstances, MeshDynamics presents these infringement allegations reflecting its analysis of the facts presently known to it. To the best of MeshDynamics' knowledge, information, and belief, formed after an inquiry that is reasonable under the circumstances, the information contained in this disclosure is correct.

Certain information about Cisco Accused Products is not available without discovery, such as proprietary source code, documents, and deposition testimony, from Cisco. MeshDynamics expects that the Cisco source code for its SD-WAN products will detail the FEC algorithms and packet structure necessary to carry out these steps. Accordingly, MeshDynamics reserved the right to supplement and/or amend this infringement contention claim chart as new information becomes available and as MeshDynamics has the opportunity to review Cisco document productions, including information related to the implementation of Cisco Accused Products that cannot be fully examined based solely on publicly available information. Infringement investigations are

ongoing, and MeshDynamics anticipates that additional facts and relevant documents will be uncovered and disclosed that create cause for supplementation and/or amendment.

<table>
<tr><th>Claim 1</th><th>Cisco Networking Equipment (e.g., Cisco SD-WAN with Forward Error Correction)</th></tr>
<tr><td>1[pre]. A method for transmitting a standard format network packet containing real time information, comprising the steps of:</td><td>
Cisco's SD-WAN (Software-Defined Wide Area Network) is a virtual WAN architecture that allows organizations to securely and efficiently connect users and applications across multiple locations. SD-WAN can perform a method of transmitting standard format network packets containing real time information and is optimized for real-time traffic like voice and video.

Source: https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html.

Cisco's SD-WAN policies configure Forward Error Correction ("FEC"), with "FEC Adaptive" (only send FEC when loss exceeds a threshold), "FEC Always" (always send FEC) and/or "Packet Duplication" (duplicates packets through secondary links to reduce packet loss if one link goes down). Cisco SD-WAN uses FEC to improve the reliability of WAN traffic and transmitting standard format network packets, especially for real-time applications like voice and video.

<table>
<tr><th>Feature Name</th><th>Release Information</th><th>Description</th></tr>
<tr><td>Forward Error Correction</td><td>Cisco IOS XE SD-WAN Release 16.11.x</td><td>Feature introduced. FEC is a mechanism to recover lost packets on a link by sending extra "parity" packets for every group of 4 packets.</td></tr>
</table>
Forward Error Correction (FEC) is a mechanism to recover lost packets on a link by sending extra "parity" packets for every group of 4 packets. As long as the receiver receives a subset of packets in the group (at-least N-1) and the parity packet, up to a single lost packet in the group can be recovered. FEC is supported on Cisco IOS XE Catalyst SD-WAN devices.

Cisco's exact specifications of its FEC algorithms and packet structure are not public. The transmitting Cisco SD-WAN device inserts a parity packet for every four standard format network data packets (a "block" or packet "container") and the receiving WAN can reconstruct a lost packet based on the parity value. As long as the receiver receives a subset of packets in the group (at-least N-1) and the parity packet, up to a single lost packet in the group can be recovered.

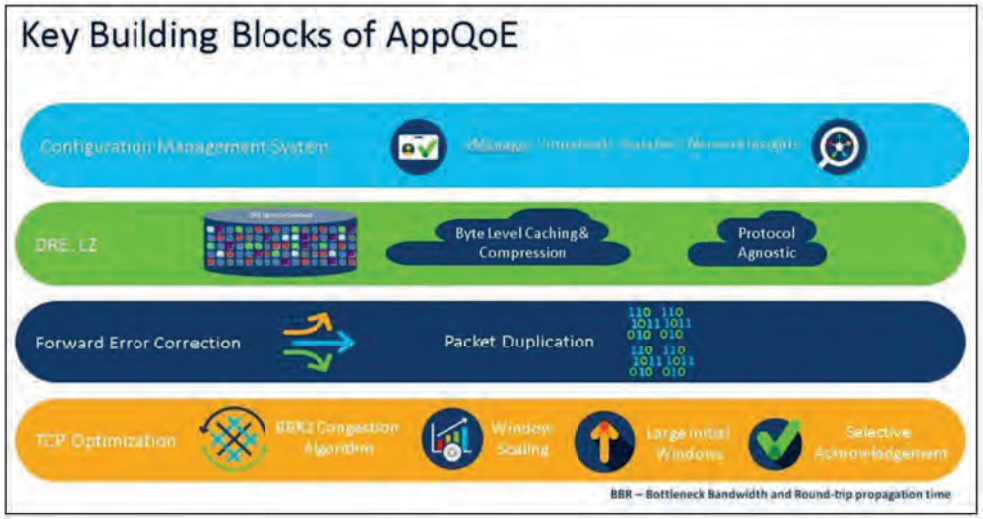
Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/forward-error-correction.html; https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/forward-error-correction.html.

The Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: Cisco
</td></tr>
</table>

vManage to Cisco Catalyst SD-WAN Manager, Cisco vAnalytics to Cisco Catalyst SD-WAN Analytics, Cisco vBond to Cisco Catalyst SD-WAN Validator, Cisco vSmart to Cisco Catalyst SD-WAN Controller, and Cisco Controllers to Cisco Catalyst SD-WAN Control Component. FEC is supported on Cisco's vEdge 1000, 2000, and 5000 routers.

Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/forward-error-correction.html.

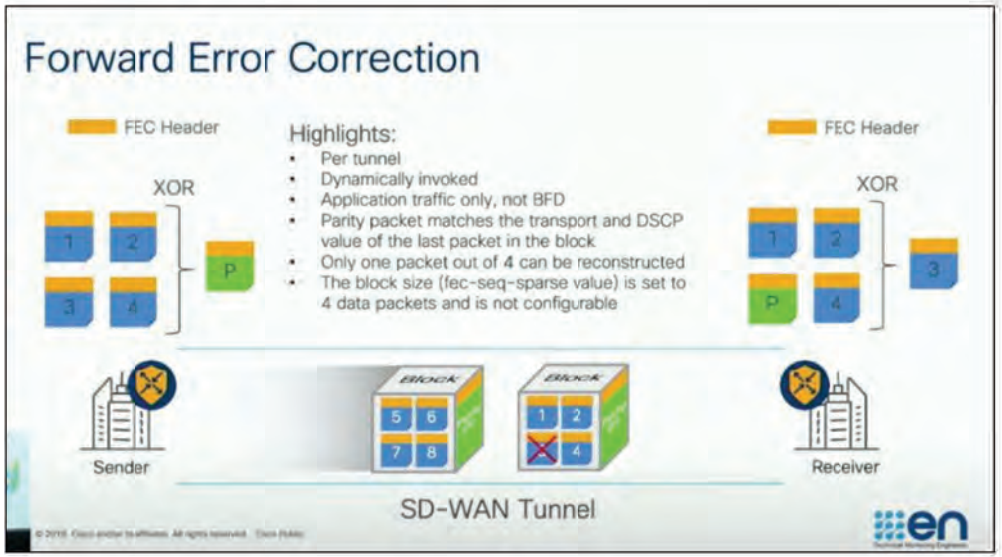
FEC is a key building block of Cisco's AppQoE ("Application Quality of Experience"), which is integrated with the SD-WAN.

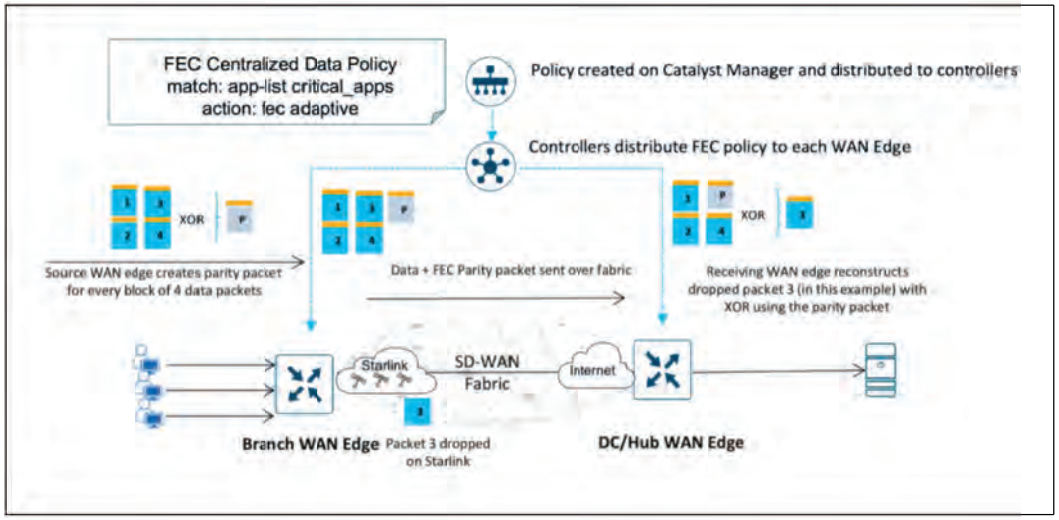


Source: https://community.cisco.com/t5/networking-blogs/cisco-application-quality-of-experience-appqoe-for-wan/ba-p/4532204; https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2025/pdf/BRKSEC-2708.pdf.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of modifying a standard format network packet or single "channel packet" or "parity group packet" in the same way by adding redundant information to the packet and achieves the same result of allowing a receiver to restore any lost data if one packet is missing or corrupted. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because a person skilled in the art would realize that with Cisco's SD-WAN

	policies and FEC, a standard format network packet can be a single channel packet or parity group packet, *e.g.*, each a block of four packets and a parity packet. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
1[a]. modifying said packet by adding redundant information to the packet;	Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, performs the step of modifying said packet by adding redundant information to the packet. The transmitting Cisco SD-WAN inserts a parity packet ("redundant information") for every four standard format network data packets and the receiving WAN can reconstruct a lost packet based on the parity value. As long as the receiver receives a subset of packets in the group (at-least N-1) and the parity packet, up to a single lost packet in the group can be recovered. Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/forward-error-correction.html; https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/forward-error-correction.html. In Cisco's SD-WAN, with four data packets and one parity packet ("modifying said packet by adding redundant information to the packet") in a FEC scheme, the parity packet may be generated by performing a mathematical operation on the data packets. The parity packet is created by applying coding theory ("XOR") to produce a set of checksums or redundant data, which, when combined with any subset of the original data packets, allows the receiver to restore the lost data if one packet is missing or corrupted. 

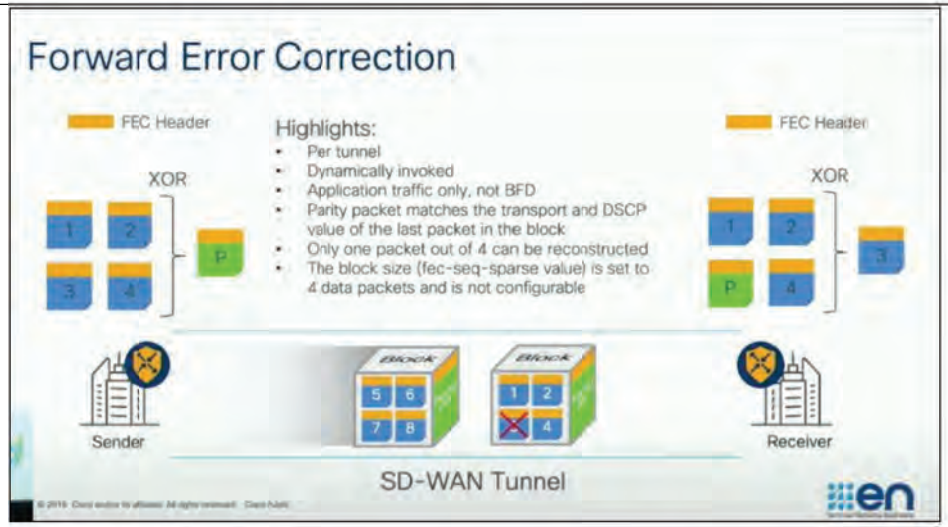
	Source: https://www.youtube.com/watch?v=0LP_XzdNmpU; *see also* https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2025/pdf/BRKSEC-2708.pdf.  Source: https://learningnetwork.cisco.com/s/article/cisco-catalyst-sd-wan-optimizations-for-starlink. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of modifying said packet by adding redundant information to the packet by generating a parity packet and achieves the same result of allowing a receiver to restore any lost data if one packet is missing or corrupted. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because, whether or not the redundant information is added within the packet or included in a packet in the transmission, it is still "modifying" the packet by adding redundant information to the packet that would otherwise not be included and the redundant information is used to recover any lost or corrupted information resulting from packet loss. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
1[b]. modifying at least one packet header to add a	On information and belief, Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, performs the step of modifying at least one packet header to add a position offset reference number (*e.g.*, a sequence number in the packet) that points to the redundant information.

position offset reference number that points to redundant information;	In a Cisco FEC-modified packet transmission, as discussed above, the four data packets are transmitted and followed by an added parity packet (for repair/error correction). Cisco's exact specifications of its FEC algorithms and packet structure are not public. On information and belief, as shown in Cisco's proprietary code, specific FEC sequence numbers or additional information are in the packet header(s) (encoded "FEC Header," shown above) to maintain the order of packets and help the receiver recognize when it has received a full group, block, or container (*i.e.*, data packets and a parity packet). The container, block, or group of four packets needs to include some identification and would require Cisco to modify at least one packet header with a reference or sequence number to point to the parity packet (*e.g.*, modify the headers to include the FEC Header with sequence numbers). It sends one parity packet or error correcting packet for every 4 packets. There are many ways to generate this parity packet. One of which is exclusive OR (XOR) which is used by our stack. The receiving end will examine sequence numbers of the packets to check if they are missing. If it received all the packets, then the parity packet is discarded. If one Source: https://community.cisco.com/t5/networking-blogs/cisco-application-quality-of-experience-appqoe-for-wan/ba-p/4532204. Cisco's FEC encoding format may specify the order and position of both data and parity packets. The parity packet is generated based on the data packets preceding it, and this structure may be fixed according to the FEC scheme being used. On information and belief, the FEC Header or a specific marker is included in the parity packet or in the packet transmission to explicitly indicate the parity packet's place and/or role in the FEC scheme ("that points to the redundant information"). This header in Cisco's SD-WAN FEC policy may be, for example, a flag or a bit pattern that signals to the receiver that a packet is parity rather than data. It may be a sequence number in the packet header. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of modifying at least one packet header to add a position offset reference number that points to redundant information in the same way by encoding the order and position of both the data and parity packets and achieves the same result of allowing the parity packet to correct packet errors by pointing to the redundant information to be recovered. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the indication of the parity packet's place and/or role serves the same purpose of pointing to the information held in the parity packet. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

1[c]. revising all checksums within the packet as modified to agree with the packet contents as modified;	Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, performs the steps of revising all checksums within the packet as modified to agree with the contents of the packet as modified. As discussed above, FEC involves modifying a packet by adding an extra packet containing redundant information for the group of four packets. The parity packet is created using XOR operations. Sequence numbers or additional information are included in the modified FEC Header in the transmission of the data packets and parity packet for FEC, which are used for checking if a packet is missing. For the modified packet with the FEC Header to be valid, it would have a revised checksum to agree with the packet as modified. The block is protected by a single CRC or checksum (*e.g.*, the number of packets or XOR operation) to ensure the integrity of all packets in that group. Typically, any changes to the packet payload or headers trigger a checksum update, ensuring the checksum remains consistent with the modified data. Network stacks and packet processing systems implement checksum recalculation as part of their packet modification routines, making this a fundamental property of how checksums function in practice. FEC in SD-WAN can be leveraged to repair corrupted data. In Cisco SD-WAN, on information and belief, each data packet and parity also includes at least one CRC (Cyclic Redundancy Check) or checksum using XOR operations to ensure the integrity of each data packet being transmitted. It is calculated over the packet's data before transmission. The CRC is used to detect any corruption that might occur during transmission, ensuring that the data received by the receiver matches the original content of the data packet. **Cisco Catalyst SD-WAN Forward Error Correction (FEC) and Packet Duplication** can significantly enhance the performance and reliability of Starlink satellite links by mitigating the effects of packet loss and data corruption. Where FEC can be leveraged to repair corrupted data bits, packet duplication can be used to replicate critical traffic across multiple outgoing (satellite or terrestrial) links between sites to increase its chances of delivery. This feature is beneficial for applications sensitive to packet loss, such as VoIP, video conferencing, and large file transfers. Source: https://learningnetwork.cisco.com/s/article/a-new-era-of-connectivity-cisco-sd-wan-and-starlink-transforming-networks#:~:text=Cisco%20Catalyst%20SD%2DWAN%20Forward,conferencing%2C%20and%20large%20file%20transfers. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of revising all checksums within the packet as modified to agree with the packet contents as modified in the same way by repairing corrupted data bits and achieves the same result of mitigating the effects of packet loss and data corruption. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because it uses redundant information to repair corrupted data. A person skilled in the relevant art

	would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
1[d]. transmitting the packet through a network; 1[e]. modifying the packet, including modifying all checksums to return the packet's format to that of the standard packet format;	Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, performs the steps of transmitting the packet through a network, and modifying the packet, including modifying all checksums to return the packet's format to that of the standard packet format (*e.g.*, receiver removes the redundant information). The packet is transmitted and the receiving end will examine the sequence numbers of the packets to check if they are missing. If the group of packets transmit without error, the packet is modified to return the packet to standard packet format by discarding the parity packet. On information and belief, the FEC headers are removed and this modifies the checksum by discarding a sequence number(s)/packet to return the information back into the format of a standard packet without FEC. On information and belief, any additional checksums or CRCs are modified as necessary to account for the return of the packet's format to the standard packet format. Forward Error Correction addresses the link integrity challenges in the network. This is one of the mechanisms used in a SD-WAN network to mitigate packet loss. It sends one parity packet or error correcting packet for every 4 packets. There are many ways to generate this parity packet. One of which is exclusive OR (XOR) which is used by our stack. The receiving end will examine sequence numbers of the packets to check if they are missing. If it received all the packets, then the parity packet is discarded. If one of the data packets is missing, then it is regenerated by performing the same bitwise exclusive OR operation on the received 3 packets and the parity packet. This removes the need for sender to send the packet again in turn avoiding packet loss. The primary use case for Forward Error Correction is for real time traffic like Voice and Video which is very time sensitive and the whole communication can get impacted with a slight increase in packet loss. Source: https://community.cisco.com/t5/networking-blogs/cisco-application-quality-of-experience-appqoe-for-wan/ba-p/4532204; *see also* https://community.cisco.com/t5/networking-knowledge-base/appqoe-amp-waas-faq/ta-p/4532236. As discussed above, typically, any changes to the packet payload or headers trigger a checksum update, ensuring the checksum remains consistent with the modified data. Network stacks and packet processing systems implement checksum recalculation as part of their packet modification routines, making this a fundamental property of how checksums function in practice. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If these claim elements are not literally infringed, they are infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of transmitting the packet through a network in the same way by sending a parity packet to the

	receiver via the SD-WAN and achieves the same result of transmitting the packet and parity packet. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because both packets and parity packets are transmitted through the network to the same receiver. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial. Cisco's SD-WAN performs the same function of modifying the packet including modifying all checksums to return the packet's format to that of the standard packet format in the same way by regenerating the parity packet and achieves the same result of recovering any lost or corrupted information. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the parity packet performs the same function as the checksum. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
1[f]. if the modified packet, having been transmitted through a network, is determined to have a checksum mismatch as received, modifying the packet by retrieving the redundant information pointed to by said position offset reference number and replacing a portion of the packet with said redundant information; and 1[g]. revising all checksums within the packet as modified to agree with the contents of the modified packet.	Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, if the modified packet having transmitted through the network is determined to have a checksum mismatch as received, performs the step of modifying the packet by retrieving the redundant information pointed to by said position offset reference number and replacing a portion of the packet with said redundant information. The transmitting Cisco SD-WAN inserts a parity packet for every four standard format network data packets, and the receiving WAN can reconstruct a lost packet based on the parity value ("determined to have a checksum mismatch"). As long as the receiver receives a subset of packets in the group (at-least N-1) and the parity packet, up to a single lost packet in the group can be recovered ("modifying the packet by retrieving the redundant information pointed to by said position offset reference number and replacing a portion of the packet with said redundant information"). Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/forward-error-correction.html; https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/forward-error-correction.html.



Source: https://www.youtube.com/watch?v=0LP_XzdNmpU.

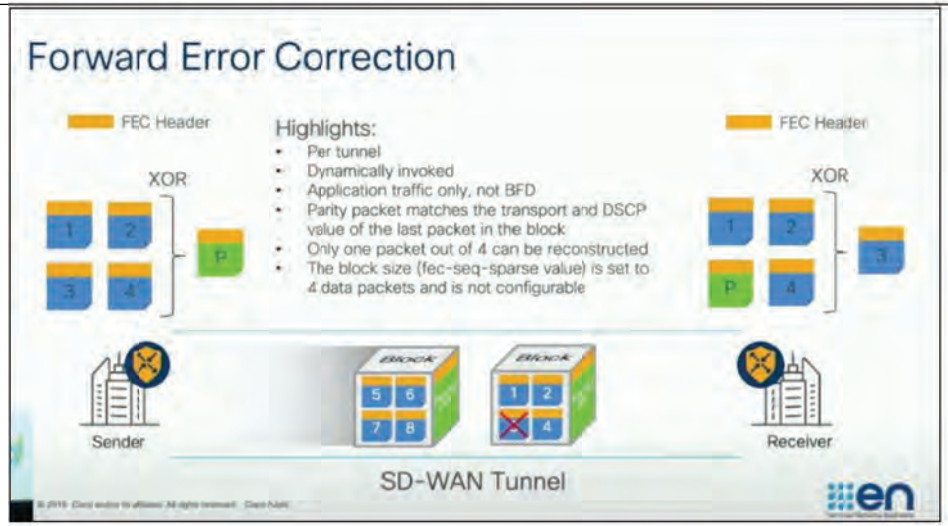
When a data packet is corrected using FEC, the packet's content is modified to recover from the error (such as packet loss or corruption). Since the checksum (*e.g.*, CRC) is calculated based on the number and/or content of the packet, if the content of the packet changes (such as when the packet is replaced or the data is corrected), on information and belief, the checksum must be revised and recalculated to reflect the replaced packet and/or new content.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If these claim elements are not literally infringed, they are infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of modifying the packet by retrieving the redundant information pointed to by said position offset reference number and replacing a portion of the packet with said redundant information in the same way by reconstructing the packet and achieves the same result correcting any lost or corrupted information in the packet. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because a portion of the packet is replaced with the redundant information. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Cisco's SD-WAN performs the same function of revising all checksums within the packet as modified to agree with the contents of the modified packet in the same way by ensuring all packets make it to the receiver and achieves the same result avoiding

	packet loss. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the parity packet is also modified to reflect the packet. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 5	
The method of claim 1 wherein a number indicating a specific position offset reference number is repeated multiple times as a means to later determine the validity of the position offset reference number after transmission.	*See* Claim 1. Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, on information and belief, further comprise wherein a number indicating a specific position offset reference number is repeated multiple times as a means to later determine the validity of the position offset reference number after transmission. The transmitting Cisco SD-WAN inserts a parity packet for every four standard format network data packets, and the receiving WAN can reconstruct a lost packet based on the parity value ("determined to have a checksum mismatch"). As long as the receiver receives a subset of packets in the group (at-least N-1) and the parity packet, up to a single lost packet in the group can be recovered ("modifying the packet by retrieving the redundant information pointed to by said position offset reference number and replacing a portion of the packet with said redundant information"). On information and belief, the specific position offset number is repeated multiple times, *e.g.*, in each of the four standard format packets, to ensure the validity of the number and identification of the parity packet after transmission. Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/forward-error-correction.html; https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/forward-error-correction.html.



Source: https://www.youtube.com/watch?v=0LP_XzdNmpU.

MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of repeating a number indicating a specific position offset reference number multiple times as a means to later determine the validity of the position offset reference number after transmission in the same way by using a number to identify the parity packet multiples times and achieves the same result of determining the validity of the position offset reference number and correct identification of the parity packet after transmission. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the parity packet is also used after transmission to determing the validity of the position offset reference number. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial

Claim 7	
The method of claim 1, wherein revising all checksums within the packet as modified to agree with the contents of	*See* Claim 1. Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, further comprise wherein revising all checksums within the packet as modified to agree with the contents of the modified packet includes creating at least one checksum that matches a real time video content containing errors.

the modified packet includes creating at least one checksum that matches a real time video content containing errors.	SD-WAN and FEC is specially optimized for real-time video content, and FEC would create a checksum (as discussed above) for this content if it was containing errors. **MPLS vs SD-WAN** SD-WAN evolved from MPLS technology, which has powered private connectivity for more than two decades. In many ways, SD-WAN can be seen as a software abstraction of MPLS technology that's applicable to wider scenarios: It brings secure, private connectivity that's agnostic to all kinds of links and providers and is cloud-aware. While MPLS handled failure scenarios with backup links, SD-WAN handles them with real-time traffic steering based on centralized policy. Also, since SD-WAN unifies the entire WAN backbone, it delivers comprehensive analytics across the network globally. This wasn't possible before, because of disparate pieces of infrastructure and policy. Source: https://www.cisco.com/site/us/en/learn/topics/networking/what-is-sd-wan.html. The primary use case for Forward Error Correction is for real time traffic like Voice and Video which is very time sensitive and the whole communication can get impacted with a slight increase in packet loss. Source: https://community.cisco.com/t5/networking-blogs/cisco-application-quality-of-experience-appqoe-for-wan/ba-p/4532204. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of creating at least one checksum that matches a real time video content containing errors in the same way by revising checksums to handle real-time video traffic and achieves the same result of real-time optimized performance. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because both provide error correction and checksums for real-time video and connectivity. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.

Exhibit 6 – U.S. Patent No. 9,049,000 (Cisco SD-WAN with Forward Error Correction)

Cisco Systems, Inc. ("Cisco") has and continues to make, use, sell, offer for sale, and/or import the Cisco Software-Defined Wide Area Network (SD-WAN), including but not limited to Cisco's Catalyst SD-WAN with Forward Error Correction (FEC) and related software and hardware (the "Cisco Accused Product," *see* Exhibit 7), and infringed at least Claims 1, 6 and 7 (the "Asserted Claims") of U.S. Patent No. 9,049,000 (the "'000 Patent").[1]

Cisco has and continues to infringe (literally and/or under the doctrine of equivalents), directly and/or through subsidiaries, agents, representatives, or intermediaries, one or more claims of the '000 Patent by making using, testing, supplying, causing to be supplied, importing, selling, and/or offering for sale in the United States the Cisco Accused Products.

Cisco directly infringes and has infringed under 35 U.S.C. § 271(a) by making, using, selling, offering for sale and importing the Cisco Accused Products. Cisco's SD-WAN directly infringed at least Claims 1, 6 and 7 of the '000 Patent when made, used, sold, offered for sale, and imported into the United States. Cisco further directly infringes and has infringed by testing, setting up, and using the Cisco SD-WAN on Cisco's campuses and locations throughout the United States, and/or assisting customers in setting up and servicing their Cisco SD-WANs. On information and belief, Cisco has partnered with several customers to set up an infringing Cisco SD-WAN in the United States.[2]

Cisco indirectly infringes and has infringed under 35 U.S.C. § 271(b) by providing specific guidance and instructions to its customers and end users on how to infringe the '000 Patent and make and use the infringing Cisco SD-WAN. Specifically, Cisco's SD-WAN deployment guides, Technical Assistance Center, Cisco Tech Talks, technical support, Cisco Community, presentations, and technical documentation on Cisco's website identified in the chart *infra* provide design and deployment guidelines for the deployment of an infringing Cisco SD-WAN. These guides and instructions were published and distributed by Cisco for its customers for the sole purpose to instruct and encourage its customers to purchase the Cisco components to make and use the infringing Cisco SD-WAN (and directly infringe literally and/or under the doctrine of equivalents). Cisco has had knowledge of the '000 Patent since 2009 when Cisco executives met with MeshDynamics to discuss partnering opportunities and the application that would result in the '000 Patent. MeshDynamics further put Cisco on actual notice of its infringement by its making, using, selling, offering for sale and importing the Cisco Accused Products that comprise the Cisco SD-

[1] The identified Accused Products also include Cisco's products, services, and systems that are considered sold or related to the infringement in the United States and subject to a reasonable royalty according to the Federal Circuit's decisions in *Carnegie Mellon Univ. v. Marvell Tech. Group. Ltd.*, 807 F.3d 1283 (Fed. Cir. 2015), *Cal. Inst. of Tech. v. Broadcom Ltd.*, 25 F.4th 976 (Fed. Cir. 2022), and *Brumfield v. IBG LLC*, 97 F.4th 854 (Fed. Cir. 2024).

[2] *See, e.g.*, https://learningnetwork.cisco.com/s/article/cisco-catalyst-sd-wan-optimizations-for-starlink; https://www.cisco.com/c/dam/m/en_us/solutions/industries/education/new-education-landscape-of-networking/pdf/SD-WAN_for_Education.pdf.

WAN in 2022. Cisco has knowingly and intentionally induced its customers to infringe the '000 Patent, or in the alternative was willfully blind to the '000 Patent and the infringement, following the MeshDynamics meeting in 2009.

Cisco further indirectly infringes and has infringed under 35 U.S.C. § 271(c) by supplying the components used in the infringing Cisco SD-WAN, with knowledge of its infringing use (as discuss *supra*) and without substantial non-infringing uses. Further, the Cisco Accused Products were designed specifically to be used in a manner that infringes the '000 Patent. Cisco Accused Products come enabled with FEC features to successfully transmit packets. Cisco advertises the FEC feature such that the SD-WAN is specifically designed to benefit from FEC. As a result of Cisco's selling and/or offering for sale the Cisco Accused Products to other entities, the other entities use these products for their intended purpose and according to their instructions with the result that such entities directly infringed the '000 Patent, literally or under the doctrine of equivalents, for the reason stated *infra*. Cisco's Accused Products are specially made and adapted for this use in an infringing manner, are not staple articles of commerce, and do not have substantial non-infringing uses.

MeshDynamics asserts that Cisco Accused Products literally infringed and continue to infringe the Asserted Claims of the '000 Patent. With respect to any claim limitation that may be found not to be literally infringed, MeshDynamics contends in the alternative that Cisco Accused Products infringed such claim limitations under the doctrine of equivalents and that any claim element not found to be literally met is equivalently met because any difference between the claim limitation and Cisco Accused Products is not a substantial difference. Accordingly, MeshDynamics contends that if any Cisco Accused Products is found not to have infringed any Asserted Claims literally it is nevertheless embodied by Cisco Accused Products under an operative doctrine of equivalents test (*e.g.*, function-way-result or insubstantial difference).

The chart below presents MeshDynamics' preliminary infringement analysis of Cisco Accused Products based solely on public information. MeshDynamics has not received any discovery from Cisco, including any confidential information or source code demonstrating the operation and structure of the Cisco Accused Products. All information contained in this disclosure is the result of publicly available information regarding the Cisco Accused Products. Based on these circumstances, MeshDynamics presents these infringement allegations reflecting its analysis of the facts presently known to it. To the best of MeshDynamics' knowledge, information, and belief, formed after an inquiry that is reasonable under the circumstances, the information contained in this disclosure is correct.

Certain information about Cisco Accused Products is not available without discovery, such as proprietary source code, documents, and deposition testimony, from Cisco. MeshDynamics expects that the Cisco source code for its SD-WAN products will detail the FEC algorithms and packet structure necessary to carry out these steps. Accordingly, MeshDynamics reserved the right to supplement and/or amend this infringement contention claim chart as new information becomes available and as MeshDynamics has the opportunity to review Cisco document productions, including information related to the

implementation of Cisco Accused Products that cannot be fully examined based solely on publicly available information. Infringement investigations are ongoing, and MeshDynamics anticipates that additional facts and relevant documents will be uncovered and disclosed that create cause for supplementation and/or amendment

Claim 1	Cisco Networking Equipment (*e.g.*, Cisco SD-WAN with Forward Error Correction)
1[pre]. A method for transmitting a standard format network packet containing real time information, comprising the steps of:	*See* '852 claim 1, Element (Pre) (Exhibit 5), incorporated by reference herein.
1[a]. modifying said packet by adding redundant information to the packet;	*See* '852 claim 1, Element 1A (Exhibit 5), incorporated by reference herein.
1[b]. modifying at least one packet header to add a position offset reference number that points to redundant information;	*See* '852 claim 1, Element 1B (Exhibit 5), incorporated by reference herein.
1[c]. revising all checksums within the packet as modified to agree with the packet contents as modified;	*See* '852 claim 1, Element 1C (Exhibit 5), incorporated by reference herein.

1[d]. transmitting the packet through a network; wherein transmitting further comprises the steps of checking the modified packet during transmission;	Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, performs the steps of transmitting the packet through a network; wherein transmitting further comprises the steps of checking the modified packet during transmission. The packet is transmitted and the receiving end will examine the sequence numbers of the packets to check if they are missing. If the group of packets transmit without error, the packet is modified to return the packet to standard packet format by discarding the parity packet. On information and belief, the FEC headers are removed and this modifies the checksum by discarding a sequence number(s)/packet to return the information back into the format of a standard packet without FEC. On information and belief, any additional checksums or CRCs are modified as necessary to account for the return of the packet's format to the standard packet format. Forward Error Correction addresses the link integrity challenges in the network. This is one of the mechanisms used in a SD-WAN network to mitigate packet loss. It sends one parity packet or error correcting packet for every 4 packets. There are many ways to generate this parity packet. One of which is exclusive OR (XOR) which is used by our stack. The receiving end will examine sequence numbers of the packets to check if they are missing. If it received all the packets, then the parity packet is discarded. If one of the data packets is missing, then it is regenerated by performing the same bitwise exclusive OR operation on the received 3 packets and the parity packet. This removes the need for sender to send the packet again in turn avoiding packet loss. The primary use case for Forward Error Correction is for real time traffic like Voice and Video which is very time sensitive and the whole communication can get impacted with a slight increase in packet loss. Source: https://community.cisco.com/t5/networking-blogs/cisco-application-quality-of-experience-appqoe-for-wan/ba-p/4532204; *see also* https://community.cisco.com/t5/networking-knowledge-base/appqoe-amp-waas-faq/ta-p/4532236. Typically, any changes to the packet payload or headers trigger a checksum update, ensuring the checksum remains consistent with the modified data. Network stacks and packet processing systems implement checksum recalculation as part of their packet modification routines, making this a fundamental property of how checksums function in practice. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of transmitting the packet through a network, wherein transmitting further comprises the steps of checking the modified packet during transmission in the same way by checking the modified packet, *e.g.*, checking the checksum or header, during transmission and achieves the same result ensuring the modified packet reaches the receiver. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the

	modified packet is checked during transmission to ensure no information is lost or compromised. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
1[e]. if the modified packet is determined to have a checksum mismatch as received, modifying the packet by retrieving the redundant information pointed to by said position offset reference number and replacing a portion of the packet with said redundant information; and	*See* '852 claim 1, Element 1F (Exhibit 5), incorporated by reference herein.
1[f]. calculating new checksums for packet; and 1[g]. revising all checksums within the packet as modified to agree with the contents of the modified packet; and,	On information and belief, Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, performs the steps of calculating new checksums for packet, and revising all checksums within the packet as modified to agree with the contents of the modified packet. Cisco's exact specifications of its FEC algorithms and packet structure are not public. When a data packet is corrected using FEC, the packet's content has been modified to recover from the error (such as packet loss or corruption). Since the checksum (*e.g.*, CRC) is calculated based on the number and/or content of the packet, if the content of the packet changes (such as when the packet is replaced or the data is corrected), on information and belief, the checksum must be revised and recalculated to reflect the replaced packet and/or new content. Typically, any changes to the packet payload or headers trigger a checksum update, ensuring the checksum remains consistent with the modified data. Network stacks and packet processing systems implement checksum recalculation as part of their packet modification routines, making this a fundamental property of how checksums function in practice. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to.

	If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of calculating new checksums for packet and revising all checksums within the packet as modified to agree with the contents of the modified packet in the same way by revising the checksums to agree with the contents of the modified packet after correction and achieves the same result of confirming that the error is corrected and the checksum is consistent with the modified data. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or insubstantial because the checksum remains consistent with the modified data. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
1[h]. upon receipt, modifying the packet to return the packet's format to that of the standard packet format.	Cisco's SD-WAN policies, *e.g.*, Cisco SD-WAN with Forward Error Correction, performs the step of upon receipt, modifying the packet to return the packet's format to that of the standard packet format. The packet is sent and the receiving end will examine the sequence numbers of the packets to check if they are missing. If the group of packets transmit without error, the packet is modified to return the packet to "standard packet format" by discarding the parity packet. On information and belief, the parity packet is further discarded following any necessary regeneration of a lost or corrupt packet to modify the packet to return the packet to the "standard packet format." Forward Error Correction addresses the link integrity challenges in the network. This is one of the mechanisms used in a SD-WAN network to mitigate packet loss. It sends one parity packet or error correcting packet for every 4 packets. There are many ways to generate this parity packet. One of which is exclusive OR (XOR) which is used by our stack. The receiving end will examine sequence numbers of the packets to check if they are missing. If it received all the packets, then the parity packet is discarded. If one of the data packets is missing, then it is regenerated by performing the same bitwise exclusive OR operation on the received 3 packets and the parity packet. This removes the need for sender to send the packet again in turn avoiding packet loss. The primary use case for Forward Error Correction is for real time traffic like Voice and Video which is very time sensitive and the whole communication can get impacted with a slight increase in packet loss. Source: https://community.cisco.com/t5/networking-blogs/cisco-application-quality-of-experience-appqoe-for-wan/ba-p/4532204; *see also* https://community.cisco.com/t5/networking-knowledge-base/appqoe-amp-waas-faq/ta-p/4532236. MeshDynamics asserts that this claim element is a software limitation. Pursuant to Judge Gilstrap's standard discovery order, MeshDynamics will identify what Cisco source code satisfies this limitation 30 days after Cisco's complete production of source code or at such other time as the parties may agree to. If this claim element is not literally infringed, it is infringed under the doctrine of equivalents. Cisco's SD-WAN performs the same function of upon receipt, modifying the packet to return the packet's format to that of the standard packet format in the same way by discarding the parity packet and achieves the same result restoring the packet to contain its original information. Moreover, any differences between the functionality of the Cisco Accused Products and the claimed element are insignificant or

	insubstantial because it returns the packet to its original and intended format. A person skilled in the relevant art would consider any difference between the claimed invention and the Cisco Accused Products to be minor and insubstantial.
Claim 6	
The method of claim 1 wherein a number indicating a specific position offset reference number is repeated multiple times as a means to later determine the validity of the position offset reference number after transmission.	*See* '852 claim 5 (Exhibit 5), incorporated by reference herein.
Claim 7	
The method of claim 1, wherein revising all checksums within the packet as modified to agree with the contents of the modified packet includes creating at least one checksum that matches a real time video content containing errors.	*See* '852 claim 7 (Exhibit 5), incorporated by reference herein.

Exhibit 7 – Accused Instrumentalities ("Cisco Accused Products")

The Cisco Accused Products include Webex and all related hardware (*e.g.*, routers, gateways, endpoints) and software (*e.g.*, IOS XE, UCM, applications) products made, used, imported, offered for sale and/or sold in the United States since June 6, 2019. This includes all products comprising the following Webex features: Webex Site Survivability, Webex Meetings Survivability, and Webex Enhanced Survivability. This also includes Webex Calling, Webex Meetings, Calling in Webex App, Unified Communications Manager, CUBE, Intercluster Lookup Service, and Webex Video Mesh.

The Cisco Accused Products also include Catalyst SD-WAN with Forward Error Correction and all related hardware and software products made, used, imported, offered for sale and/or sold in the United States since June 6, 2019.

This includes, but is not limited to, any and all of the Cisco hardware and software products that are identified in the list below. These products were identified after a reasonable search of publicly-available Cisco information, and on information and belief, comprise a complete or near-complete list of the Cisco Accused Products (and associated licenses to be identified through discovery) since June 6, 2019. Information regarding "end of life" products may not be available on Cisco's publicly-available website. MeshDynamics reserves the right to amend or supplement this list following discovery.

Cisco Webex

Cisco Webex

Cisco Webex Suite

Cisco Webex App

Cisco Webex Edge

Cisco Webex Calling

Cisco Calling for Webex App

Cisco Webex Video Mesh

Cisco Webex Meetings

Cisco VoIP Endpoints

Cisco IP Phones 6800, 7800, 8800 Series desk phones, Cisco IP Conference Phones 7832 and 8832, Cisco IP DECT 6800 Series, Cisco Desk Phone 9800 Series, and analog ATAs, including:

- 6821, 6841, 6851, 6861, 6861 Wi-Fi, 6871
- 7811, 7821, 7841, 7861
- 8811, 8841, 8851, 8861
- 8845 (audio only), 8865 (audio only), 8875(video)
- 9800

- VG400 ATA
- VG410 ATA
- VG420 ATA
- Cisco ATA 191 and 192

Cisco Webex App

Endpoints supported by UCM

All CUBEs and gateways supported by UCM

Cisco Jabber

Cisco Webex Meetings

Cisco Software

Cisco IOS XE 16.8 and later, including, but not limited to:

- 16.9.x (Fuji)
- 16.11.x
- 16.12.x (Gibraltar)
- 17.1.1 (Amsterdam)
- 17.2.1
- 17.3.1
- 17.5.x
- 17.6.x
- 17.7.x
- 17.8.x
- 17.9.x
- 17.10.x
- 17.11.x
- 17.12.x (Dublin)
- 17.13.x
- 17.14.x

Phone OS 3.2 and later versions

CUBE 14.0 IOS XE Amsterdam 17.3.1a (17.3.1)

CUBE 14.1 (IOS XE 17.3.2)

CUBE 14.2 (IOS XE 17.3)

CUBE 14.3 (IOS XE 17.4.1a)

CUBE 14.3 (IOS XE 17.5.1)

CUBE 14.4 (IOS XE 17.6.1a)

CUBE 14.5 (IOS XE 17.8.1a)

CUBE 14.6 (IOS XE 17.9.1a or 17.10.1a or 17.11.1a)

CUBE 14.7 (IOS XE 17.12.1a)

CUBE 14.8 (IOS XE 17.13.1a)

CUBE 14.9 (IOS XE 17.14.1a)

CUBE 14.10 (IOS XE 17.15.1a)

CUBE 14.11 (IOS XE 17.16.1a)

CUBE 15 (IOS XE 17.18.1a)

CUBE 12.5 (IOS XE 16.10.1a)

CUBE 11.5.0 (IOS XE Release 3.17)

CUBE 11.5.1, 11.5.2 (IOS XE Denali 16.3.1)

CUBE (versions with Intercluster Lookup Service)

Enhanced Survivability Node SKUs

A-FLEX-DI-ESV

A-FLEX-DI-NU-ESV

A-FLEX-DI-ESV-E

A-FLEX-DI-NU-ESV-E

Cisco Routers (SGWs) and Local Gateways

Integrated Services Router 4321

Integrated Services Router 4331

Integrated Services Router 4351

Integrated Services Router 4431

Integrated Services Router 4451-X

Integrated Services Router 4461

Catalyst Edge 8200L-1N-4T

Catalyst Edge 8200-1N-4T

Catalyst Edge 8300-1N1S-6T

Catalyst Edge 8300-2N2S-6T

Catalyst Edge 8300-1N1S-4T2X

Catalyst Edge 8300-2N2S-4T2X

Catalyst Edge 8000V software small configuration

Catalyst Edge 8000V software medium configuration

Catalyst Edge 8000V software large configuration

CUBE (including UCK9 license and high availability)

Unified CM

Unified CM 15

Unified CM 14

Unified CM 12.5

United CM 12.0

Unified CM 11.5

Unified CM 10.5

Unified CM 9.5 and later (Intercluster Lookup Service)

Catalyst SD-WAN

Catalyst SD-WAN (including Cloud Delivered)

Cisco SD-WAN (including Cloud Delivered)

Catalyst 8000V

Catalyst 8300

Catalyst 8500

Catalyst 8200

Catalyst 8200 uCPE

ASR 1000 series

ASR1001-HX

ASR1002-HX

ASR1006-X

ISR 4000

ISR 1100-4G

ISR 1100-6G

ISR1100-4GLTE

ISR 1100X-4G

ISR 1100X-6G

ISR 1131

C1111-8PWA

vEdge 100

vEdge 1000

vEdge 2000

vEdge 5000

CSR1000V

IR1100

IR8300

IR8340

ENCS 5406

ENCS 5408

ENCS 5000 series

Firepower

Catalyst Firewalls, including Catalyst Firewall 3100

Catalyst SD-WAN Manager

IOS XE Release 17.6.3 or later

Cisco IOS XE SD-WAN Release 16.11.x

Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Cisco IOS XE Release 16.6.3

Cisco IOS XE Catalyst SD-WAN Release 16.12.1b

Cisco IOS XE Catalyst SD-WAN Devices

(Before rebrand) "v" or Viptela SD-WAN products