

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

K.MIZRA LLC,

Plaintiff,

V.

CIENA CORPORATION,

Defendant.

Civil Action No. _____

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff K.Mizra LLC (“K.Mizra”) files this Complaint for patent infringement against Defendant Ciena Corporation (“Ciena” or “Defendant”) and alleges as follows:

NATURE OF THE ACTION

1. This is a civil action for infringement of U.S. Patent No. 8,782,282 (“the ’282 Patent”); U.S. Patent No. 9,485,176 (“The ’176 Patent”); and U.S. Patent No. 10,735,320 (“the ’320 Patent”) (collectively, the “Patents-in-Suit”). This action arises under the Patent Act of the United States, 35 U.S.C. § 101 *et seq.*

2. Defendant Ciena has been infringing the Patents-in-Suit in violation of 35 U.S.C. § 271 by manufacturing, using, importing, selling, and/or offering for sale in the United States products, methods, processes, services and/or systems that infringe the Patents-in-Suit, which include but are not limited to networking

equipment and/or systems that integrate various components to provide Ciena's customers with "optical and routing systems, services, and automation software"¹ (collectively "Accused Instrumentalities"). In particular, and based on information and belief, Ciena's Blue Planet division provides Operations (or Operational) Support Systems (OSS) to Communication Service Providers (CSPs), including without limitation, the Blue Planet Intelligent Automation Portfolio that "uniquely helps CSPs optimize and automate their operations and streamline the introduction of new services across any network domain or vendor, without creating costly and inefficient operational silos."² According to Ciena's website, Blue Planet provides "the industry's only cloud-native platform that brings together leading inventory, orchestration, and assurance... to enable simplified, end-to-end automation for faster service introduction and monetization."³ Ciena's Accused Instrumentalities including the OSS products and/or services, such as without limitation the Blue Planet Intelligent Automation Portfolio⁴ and its components, infringe each of the Patents-in-Suit.

¹ <https://www.ciena.com/about> (last visited October 14, 2024).

² <https://www.blueplanet.com/about> (last visited October 14, 2024).

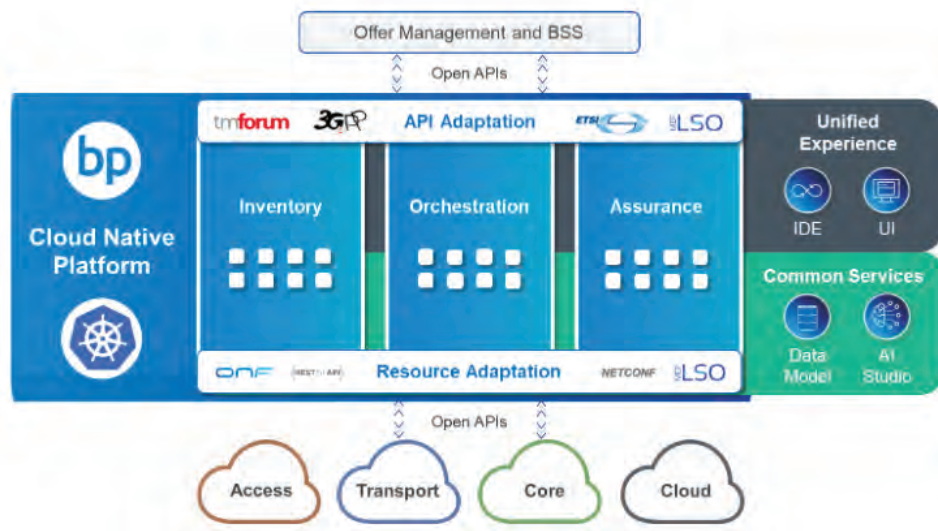
³ <https://www.blueplanet.com/cloud-native-platform> (last visited October 14, 2024).

⁴ On information and belief, Ciena's Blue Planet Intelligent Automation Portfolio includes without limitation the following Ciena products and/or services: Blue Planet Inventory (<https://www.blueplanet.com/products> (last visited October 14, 2024)); Blue Planet Orchestration (which is comprised of "three modular software products," Service Order Orchestration (SOO), Multi-Domain Service Orchestration (MDSO), and Network Functions Virtualization Orchestration

(NFVO)) (<https://www.blueplanet.com/products/orchestration.html> (last visited October 14, 2024)); Multi-Cloud Orchestration (<https://www.blueplanet.com/solutions/5g-automation.html> (last visited October 14, 2024)); Wave Services Automation (<https://www.blueplanet.com/solutions/wave-services-automation.html> (last visited October 14, 2024)); Bandwidth on Demand (<https://www.blueplanet.com/solutions/bandwidth-on-demand.html> (last visited October 14, 2024)); Route Optimization and Analysis (<https://www.blueplanet.com/products/route-optimization.html> (last visited October 14, 2024)); IP/MPLS Automation (https://www.blueplanet.com/_data/assets/pdf_file/0023/9257/Route_Optimization_and_Analysis_DS_4_2024.pdf (last visited October 14, 2024)); 5G Automation Network Slicing (<https://www.blueplanet.com/resources/what-is-network-slicing.html> (last visited October 14, 2024)); Discovery Resource Adapters (https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024)); Unified Assurance and Analytics (<https://www.blueplanet.com/products/uaa.html> (last visited October 14, 2024)). See also <https://www.blueplanet.com/products> (last visited October 14, 2024).

Blue Planet Cloud Native Platform (CNP)

Blue Planet provides a uniquely open and adaptable OSS solution to help you optimize and automate operations and streamline the introduction of new services across any network domain or vendor. Whether introducing a new service or replacing a legacy system, you can take advantage of a proven and productized architecture—enabling a sustainable approach to OSS modernization that avoids extensive customizations and keeps you thriving in a changing market.



3. K.Mizra seeks appropriate damages, prejudgment and post-judgment interest for Ciena's infringement of the Patents-in-Suit.

THE PARTIES

4. Plaintiff K.Mizra is a Delaware limited liability corporation with its principal place of business at 77 Brickell Avenue, #500-96031, Miami, Florida 33131. K.Mizra is the assignee and owner of the Patents-in-Suit.

5. On information and belief, defendant Ciena is a corporation organized and existing under the laws of Delaware that maintains an established place of

business at 1120 Sanctuary Pkwy, Alpharetta, GA 30004.⁵ On further information and belief, Ciena can be served through its registered agent Corporate Service Company at 2 Sun Court, Suite 400, Peachtree Corners, Georgia 30092.

JURISDICTION AND VENUE

6. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

7. This Court has original jurisdiction over the subject matter of this patent litigation action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

8. This Court has personal jurisdiction over defendant Ciena because Ciena maintains an established place of business in this District and conducts substantial business activities in this District. Specifically, Ciena conducted business and committed acts of patent infringement in this District, and the State of Georgia. Ciena committed acts of infringement in this District by, among other things, designing, developing, manufacturing, importing, offering to sell, or selling products that infringed the Patents-in-Suit. Further, Ciena, directly and through subsidiaries or intermediaries (including distributors, re-sellers, and others), has purposely and voluntarily placed one or more of the Accused Instrumentalities into the stream of commerce with the intention and expectation that they will be purchased and used

⁵ <https://www.ciena.com/contact-us/worldwide/alpharetta> (last visited October 14, 2024).

by customers in the Northern District of Georgia. On information and belief, the Accused Instrumentalities have been and continue to be purchased and used by customers in the Northern District of Georgia.

9. Ciena has committed and continues to commit acts of infringement of the Patents-in-Suit in violation of the United States Patent Laws, and has used the Accused Instrumentalities within this District. Ciena's infringement has caused substantial injury to K.Mizra, including within this District.

10. On information and belief, Ciena's Alpharetta, Georgia office is located at 1120 Sanctuary Parkway. On further information and belief, Ciena had, for several years, maintained over 100,000 square feet of office/manufacturing space at its Alpharetta, Georgia location.⁶ On further information and belief, Ciena's Alpharetta, Georgia location was and is still being used as an "engineering facility."⁷ On further information and belief, and in relevant part, employees who have and/or currently work on Ciena's Blue Planet solution at Ciena's Georgia location include individuals holding job titles such as Senior Delivery Architect, Blue Planet⁸; Blue Planet

⁶ See, e.g., <https://www.globest.com/2000/12/15/ciena-goes-on-leasing-spre-adding-147350-sf-of-officemanufacturing-space-at-two-locations/> (last visited October 14, 2024).

⁷ See, e.g., Ciena's December 16, 2022 Annual 10-K, <https://investor.ciena.com/static-files/44985a31-27fc-4b69-bfcb-8a1f748b4922> (last visited October 14, 2024) at 43 ("We also have engineering facilities in ... Alpharetta, Georgia...").

⁸ <https://www.linkedin.com/in/saravananp/> (last visited November 19, 2024).

Software & Test Professional Services Delivery Leader⁹; Senior Manager, Software Test and Automation¹⁰; Senior Director Sales Engineering¹¹; and Senior Delivery Architect.¹²

11. On information and belief, Ciena also advertises that it is currently hiring for engineering positions related to the Accused Instrumentalities in Georgia, including System Design and Architecture Engineer¹³ and Senior Optical DSP Systems Engineer.¹⁴

12. In at least one other action for patent infringement, Ciena has admitted that this District is a proper venue for patent infringement actions against it and that venue exists in such action.¹⁵

⁹ <https://www.linkedin.com/in/matt-becker-4322022/> (last visited November 19, 2024).

¹⁰ <https://www.linkedin.com/in/sharon-n-87461062/> (last visited November 19, 2024).

¹¹ <https://www.linkedin.com/in/manueldamas/> (last visited November 19, 2024).

¹² <https://www.linkedin.com/in/mallikarjun-kore-9b679a12/> (last visited November 19, 2024).

¹³ <https://careers.ciena.com/us/en/job/R025076/Systems-Design-and-Architecture-Engineer-Hybrid-Alpharetta-GA> (last accessed October 14, 2024).

¹⁴ <https://careers.ciena.com/us/en/job/R021839/Senior-Optical-DSP-Systems-Engineer> (last accessed October 14, 2024).

¹⁵ See Ciena's First Amended Answer and Counterclaims, *Graywire, LLC v. Ciena Corp., et al.*, case no. 1:08-CV-2993 (BBM) (N.D. Ga., Apr. 17, 2009), ¶¶ 9-10 (“...Ciena admits that venue exists under 28 U.S.C. §§ 1391 and 1400...Ciena admits that it is subject to the jurisdiction of this Court...”).

13. By registering to conduct business in Georgia and by maintaining facilities in at least the city of Alpharetta, Ciena has at least one regular and established place of business within the Northern District of Georgia.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1400(b) on the grounds that Ciena committed acts of infringement in and has a regular and established place of business in this District. Ciena's Blue Planet division has an established place of operation in Ciena's Georgia offices, and Ciena has committed acts of infringement in this District by, among other things, designing, developing, manufacturing, importing, offering to sell, or selling products that infringed the Patents-in-Suit.

THE '282 PATENT-IN-SUIT

15. The '282 Patent is titled "Network Management System" and was issued by the United States Patent Office to inventors Eileen Zhou, Roger Liu, Vijoy Choyi, Moshe Itah, and John Z. Yu.

16. The '282 Patent was fully examined by the USPTO and duly issued on July 15, 2014. The earliest application related to the '282 Patent was filed on December 19, 2003. A true and correct copy of the '282 Patent is attached as Exhibit A.

17. K.Mizra is the owner of all right, title and interest in and to the '282 Patent with the full and exclusive right to bring suit to enforce the '282 Patent.

18. The '282 Patent is valid and enforceable under the United States Patent Laws.

19. Each of the named inventors of the '282 Patent assigned the patent to Hammerhead Systems, Inc., who thereafter assigned them to Brixham Solutions Ltd. Brixham Solutions Ltd. assigned the Patents-in-Suit to Global Innovation Aggregators LLC, who in turn assigned them to K.Mizra. K.Mizra owns the right, title and interest in each of the Patents-in-Suit, including the right to sue for past infringement.

20. The '282 Patent teaches novel systems and methods for improving scalability and efficiency in handling large volumes of events occurring in the network and network management tasks. The '282 Patent's claimed systems and methods combine specific hardware and software components in unconventional ways. In contrast, conventional network management systems (NMS) systems faced several challenges as the size of data communications networks grew in size. As networks expanded, NMS's required increased processing power to manage network performance, identify and fix problems or malfunctions in the network, and plan for further network growth without becoming overwhelmed by the number of events occurring in the network that are generated by network nodes and elements.

21. Through its novel technological innovation, the '282 Patent provides systems and methods for a scalable and robust NMS architecture that can efficiently

manage increasing network demands by implementing server clusters, load balancing, and distributed gateway and adapter systems. This allows for incremental addition of network management resources without interrupting network operations, thereby optimizing performance and scalability.

THE '176 PATENT-IN-SUIT

22. The '176 Patent is titled "Global IP-Based Service Oriented Network Architecture" and was issued by the United States Patent Office to inventors Ping Pan and Richard Gitlin.

23. The '176 Patent was fully examined by the United States Patent and Trademark Office ("USPTO") and duly issued on November 1, 2016. The earliest application related to the '176 Patent was filed on August 4, 2006. A true and correct copy of the '176 Patent is attached as Exhibit B.

24. K.Mizra is the owner of all right, title and interest in and to the '176 Patent with the full and exclusive right to bring suit to enforce the '176 Patent.

25. The '176 Patent is valid and enforceable under the United States Patent Laws.

26. Each of the named inventors of the '176 Patent assigned the patent to Hammerhead Systems, Inc., who thereafter assigned them to Brixham Solutions Ltd. Brixham Solutions Ltd. assigned the Patents-in-Suit to Global Innovation Aggregators LLC, who in turn assigned them to K.Mizra. K.Mizra owns the right,

title and interest in each of the Patents-in-Suit, including the right to sue for past infringement.

27. The '176 Patent teaches novel systems and methods for improved network traffic routing policies and facilitating internet services across disparate network technologies and service providers. The '176 Patent's claimed systems and methods combine specific hardware and software components in unconventional ways. In contrast, conventional systems faced several challenges due to diversity between access/metro networks and core/backbone networks, which complicated the management of the disparate network interfaces and the provision of consistent network services. For example, conventional network Layer-2 and Layer-3 Quality of Service (QoS) mechanisms were not adequate to satisfy varying internet service requirements such as for multimedia applications, which can have different tolerances for data packet delivery issues, e.g., latency, packet loss, etc. In other words, conventional systems could not adequately meet specific performance requirements or QoS guarantees for video and voice traffic traversing across specific service provider networks.

28. Through its novel technological innovation, the '176 Patent provides systems and methods with a service-oriented network architecture, which facilitates the transport of QoS-guaranteed voice and video traffic across disparate provider networks. The '176 Patent leverages pseudowires to enable the delivery of new

services over network deployments that may be operated by different service providers and carriers with diverse network technologies, e.g., both legacy and new. The '176 Patent aggregates network traffic into pseudowires and routes the traffic accordingly based on routing policies specific to the type of applications associated with the traffic to ensure service level agreements (SLA) and QoS guaranteed by the service providers.

THE '320 PATENT-IN-SUIT

29. The '320 Patent is titled "Application Wire" and was issued by the United States Patent Office to inventors Ping Pan and Richard Gitlin.

30. The '320 Patent was fully examined by the USPTO and duly issued on August 4, 2020. The earliest application related to the '320 Patent was filed on October 7, 2005. A true and correct copy of the '320 Patent is attached as Exhibit C.

31. K.Mizra is the owner of all right, title and interest in and to the '320 Patent with the full and exclusive right to bring suit to enforce the '320 Patent.

32. The '320 Patent is valid and enforceable under the United States Patent Laws.

33. Each of the named inventors of the '320 Patent assigned the patent to Hammerhead Systems, Inc., who thereafter assigned them to Brixham Solutions Ltd. Brixham Solutions Ltd. assigned the Patents-in-Suit to Global Innovation Aggregators LLC, who in turn assigned them to K.Mizra. K.Mizra owns the right,

title and interest in each of the Patents-in-Suit, including the right to sue for past infringement.

34. The '320 Patent teaches novel systems and methods for improved management of network traffic such as traffic for multimedia applications over a service provider or carrier network, particularly in the context of Multi Protocol Label Switching (MPLS) networks. The '320 Patent's claimed systems and methods combine specific hardware and software components in unconventional ways. In contrast, conventional MPLS network systems primarily handled data traffic at the network Layer-3 level and below, which limited their ability to provide QoS guarantees at the user application level. Traditional methods like IntServ/RSVP and DiffServ had limitations in scalability and required over-provisioning of network bandwidth to ensure QoS, which was not always feasible. Additionally, these methods required changes to intermediate nodes and equipment, which was not desirable.

35. Through its novel technological innovation, the '320 Patent provides systems and methods for more efficient management and transfer of application traffic across the network, enhancing QoS and flexibility in handling application-specific service requirements and guarantees. The '320 Patent maps application specific traffic or application flows to pseudowires with an awareness of application protocol requirements, thereby providing a scalable solution for managing

application-specific QoS without requiring changes to the existing equipment at intermediate network nodes.

K.MIZRA'S PRE-LITIGATION COMMUNICATIONS WITH CIENA

36. On or about February 13, 2024, K. Mizra sent letters to Ciena's Senior Intellectual Property Counsel and VP of Intellectual Property (the "Notice Letters") as a "notice to Ciena that Ciena's products have and are continuing to infringe various claims of K. Mizra's patents."¹⁶ In relevant part, the Notice Letters informed Ciena that K.Mizra's patent portfolio "cover[ed] various aspects of pseudowire technology such as those made and used in Ciena products."¹⁷

37. In further relevant part, the Notice Letters informed Ciena of its infringement of at least the '282, '176, and '320 Patents via attached infringement claim charts that detailed K.Mizra's allegations of infringement on an element-by-element basis for certain claims.¹⁸ The claim charts for the '282, '176, and '320 Patents included citations to supporting documents, including content found at the following URLs:

- https://software.ciena.com/releasenotes/MCP-DOCS_5.2-227/build/site/mcp-docs/api-guide/APICollections.html;

¹⁶ True and correct copies of February 13, 2024 letters from Charles Hausman of K.Mizra to Raymond Gabriel and Robert Kucler of Ciena are attached hereto as Exhibit D.

¹⁷ Exhibit D.

¹⁸ Exhibit D.

- https://software.ciena.com/releasesnotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/TAPI.html;
- https://software.ciena.com/releasesnotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/Topology.html;
- https://software.ciena.com/releasesnotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/Overview.html;
- https://software.ciena.com/releasesnotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/PacketServiceMgmt.html;
- https://software.ciena.com/releasesnotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/PacketServiceMgmt.html#provision-eline-pwhand;
- https://software.ciena.com/releasesnotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/PacketInfrastructureMgmt.html;
- https://software.ciena.com/releasesnotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/PacketInfrastructureMgmt.html#packet-infrastructure-management;
- [https://software.ciena.com/releasesnotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/L3VPNservice.html#viewing-l3-vpn-service:~:text=Create%20%22L3%20VPN%20service%22](https://software.ciena.com/releasesnotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/L3VPNservice.html#viewing-l3-vpn-service:~:text=Create%20%22L3%20VPN%20service%22;);
- <https://www.ciena.com/insights/articles/What-is-FlexEthernet-and-Why-is-it-so-Important.html>; and
- <https://www.ciena.com/insights/articles/How-utility-network-managers-can-gain-critical-visibility-to-meet-user-demands.html>.

38. On information and belief, each of the URLs listed in Paragraph 37 above were at all times under the possession, custody, and/or control of Ciena.

39. After K.Mizra informed Ciena of its infringement of the Patents-in-Suit via the Notice Letters' claim charts and citations to Ciena documentation, K.Mizra learned that the URLs listed in at least Paragraph 37 were no longer available for access by the time of filing of this Complaint. On further information and belief, at least some of the links listed in Paragraph 37 were made unavailable mere weeks following K.Mizra's Notice Letters. On further information and belief, each of the above-listed links now redirects either to a "403" error page or a general Ciena content page, indicating that the individual URL could not be found and displayed.

40. Additionally, K.Mizra's claim charts attached to the February 13, 2024 Notice Letters included certain diagrams and graphics obtained from Ciena's websites as part of the element-by-element infringement analysis. In several instances, those graphics have since been changed on Ciena's website following delivery of the Notice Letters.

41. As an example, certain graphics at the following URLs that K.Mizra had cited in its infringement charts attached to the Notice Letters had been changed and/or omitted from the cited webpage by the filing of this Complaint:

- <https://www.blueplanet.com/solutions/5g-automation.html>; and
- https://www.blueplanet.com/data/assets/pdf_file/0021/81264/5G_Automation_Network_Slicing_SB1.pdf.

42. K.Mizra did not receive any communication and/or correspondence from Ciena in response to its February 13, 2024 Notice Letters.

COUNT I: INFRINGEMENT OF THE '282 PATENT

43. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

44. On information and belief, Ciena has directly infringed, literally and/or by the doctrine of equivalents, individually and/or jointly, one or more claims of the '282 Patent, including at least claim 1, in violation of 35 U.S.C. § 271, et seq., by using in this District and in the United States certain products and/or services, including but not limited to those, relating to the Accused Instrumentalities.

45. Based on publicly available information, Ciena's Accused Instrumentalities meet all elements of at least claim 1 of the '282 Patent.

46. Claim 1 of the '282 Patent provides:

[Preamble] 1. A method, comprising:

[1A] receiving, at a first application server instance selected from a plurality of application server instances based on a load balancing process, first adapter processed information from a first adapter, wherein the first adapter processed information comprises event information received by the first adapter from a network element and processed by the first adapter based on a first communication protocol;

[1B] processing, by the first application server instance, the first adapter processed information based on an event management service to produce application processed information;

[1C] sending, by the first application server instance, the application processed information to a gateway device, wherein the gateway device is one of a plurality of gateway devices respectively associated with the plurality of application server instances and is configured to transfer the application processed information to a second adapter of a plurality of second adapters configured to process the application processed information and transfer the second adapter processed information to an operation support system device; and

[1D] in response to determining that the first application server instance has become disabled, facilitating establishing an association between the first adapter and a second application server instance of the plurality of application server instances and between the gateway device and the second application server instance.

47. Regarding the preamble of claim 1, to the extent the preamble is determined to be limiting, the Accused Instrumentalities perform the claimed method as set forth herein. For example, Ciena documents detail the services (outlined below in red) provided by Ciena to its customer¹⁹:

19

<https://manuals.plus/m/e0a8a7f7c005eb2cfdb698612b839a7dd4355f8b778f751030300cc66c0ce957.pdf> (last visited October 14, 2024) (emphasis added).

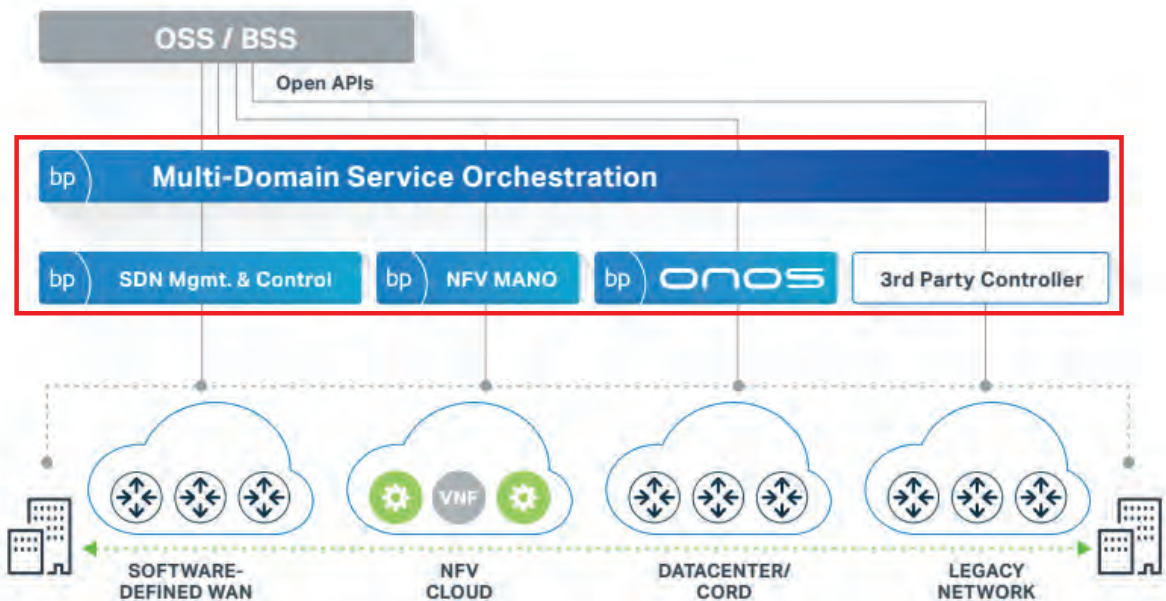


Figure 2. Blue Planet serves four primary use cases to meet our customers' business and operational requirements

48. As a further example, Ciena states that “Blue Planet facilitates a vendor-agnostic and modular approach to automating the network service lifecycle in multi-domain environments. Beyond eliminating technology silos, this gives network operators more freedom to use the best-of-breed (physical and virtual) network components of their choice, and allows them to focus on delivering services instead of managing appliances.”²⁰

49. As a further example, Ciena states that “Blue Planet supports both Ciena and non-Ciena domains (e.g., access, metro, core, cloud) through the use of

²⁰

<https://manuals.plus/m/e0a8a7f7c005eb2cfdb698612b839a7dd4355f8b778f751030300cc66c0ce957.pdf> (last visited October 14, 2024).

resource adapters to interface with a single multi-domain service orchestration layer.”²¹

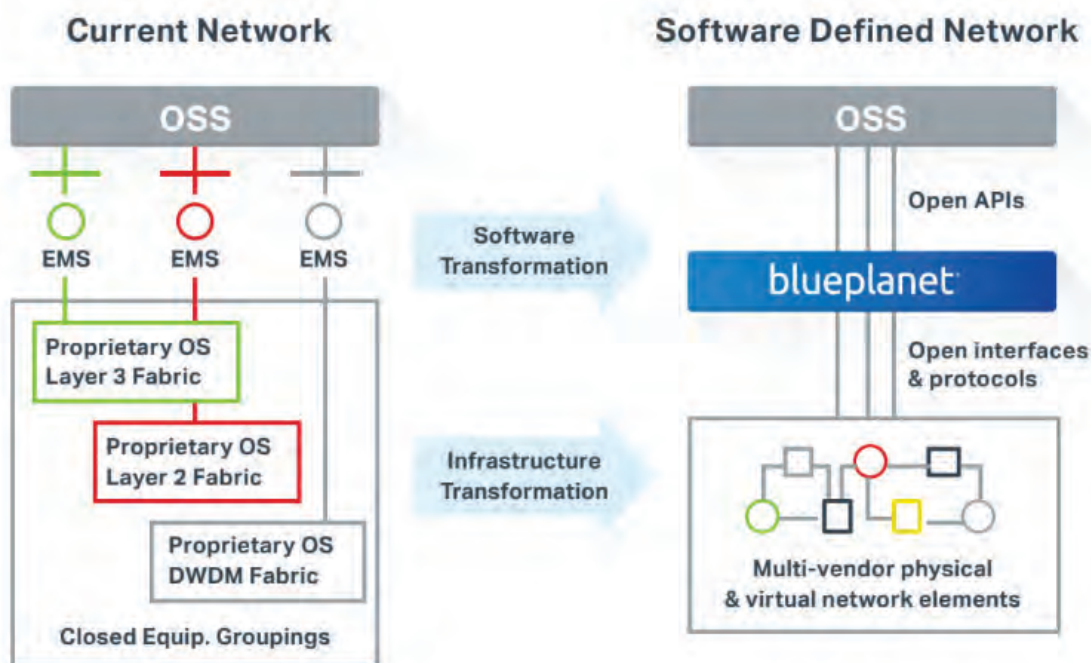
50. Thus, to the extent the preamble of claim 1 is limiting, Ciena performs the preamble of claim 1 at least by using the Blue Planet Intelligent Automation Portfolio.

51. Limitation [1A] requires “receiving, at a first application server instance selected from a plurality of application server instances based on a load balancing process, first adapter processed information from a first adapter, wherein the first adapter processed information comprises event information received by the first adapter from a network element and processed by the first adapter based on a first communication protocol.” On information and belief, Ciena, through the Accused Instrumentalities, performs this step of the claimed method by operating, maintaining, and enabling others to operate, utilize, or otherwise benefit from Ciena’s Blue Planet Intelligent Automation Portfolio. For example, on information and belief, Ciena provides “SDN Management and Control” that employs various FCAPS²² management functions that control and manage various elements in a

²¹ <https://www.blueplanet.com/blog/Ciena-Blue-Planet-unveils-the-dawn-of-service-orchestration-prx.html> (last visited October 14, 2024) (emphasis added).

²² On information and belief, “FCAPS” refers to Fault, Configuration, Accounting, Performance, Security. *See, e.g.*, <https://manuals.plus/m/e0a8a7f7c005eb2cfdb698612b839a7dd4355f8b778f751030300cc66c0ce957.pdf> (last visited October 14, 2024).

network.²³ Thus, on information and belief, Ciena utilizes a plurality of application server instances that receive various data from network elements. In the figure below, taken from Ciena documentation, Blue Planet utilizes “[o]pen interfaces & protocols” to communicate with “[m]ulti-vendor physical & virtual network elements.”²⁴



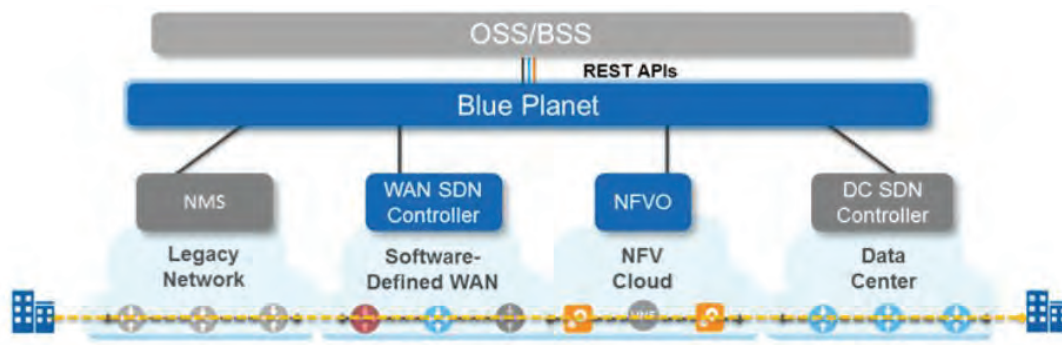
²³

<https://manuals.plus/m/e0a8a7f7c005eb2cfdb698612b839a7dd4355f8b778f751030300cc66c0ce957.pdf> (last visited October 14, 2024).

²⁴

<https://manuals.plus/m/e0a8a7f7c005eb2cfdb698612b839a7dd4355f8b778f751030300cc66c0ce957.pdf> (last visited October 14, 2024).

52. On information and belief, Ciena also advertises that “Blue Planet supports both Ciena and non-Ciena domains (e.g., access, metro, core, cloud) ***through the use of resource adapters*** to interface with a single multi-domain service orchestration layer. ... Additionally, open APIs expose critical data to northbound platforms in our software stack.”²⁵ In other words, Blue Planet allows network elements to connect to and communicate with an external OSS/BSS.



53. Additionally, other Ciena documentation discloses that “[t]he Resource adapter controller manages RAs and coordinates provisioning of network elements across multiple RA instances,” which demonstrates the load-balancing process Ciena operates as required by claim element [1A].²⁶

54. Ciena describes its Discovery Resource Adapters as “discover[ing], collect[ing], and abstract[ing] all types of inventory data from physical, virtual, and

²⁵ <https://www.blueplanet.com/blog/Ciena-Blue-Planet-unveils-the-dawn-of-service-orchestration-prx.html> (last visited October 14, 2024) (emphasis added).

²⁶ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-227/build/site/mcp-docs/api-guide/APICollections.html (last visited July 18, 2024). On information and belief, the document appears to be no longer available on Ciena’s website.

logical network resources... RAs are developed for a vendor's specific family of products. For communicating southbound with network functions, RAs can use any open standard protocol... or other native interfaces supported by the device.”²⁷ Additionally, Ciena states that “Discovery RAs serve as a technology- and vendor-agnostic abstraction framework for collecting data from any virtual or cloud-based network function, or physical network element—including from Ciena, Cisco, Nokia, Fortinet, Infinera, Juniper, and many other vendors.”²⁸ “RAs can interface directly with any data source including inventory management systems, Element or Network Management Systems (EMS/NMS), and domain controllers, as well as directly with underlying network functions.”²⁹ Notably, Ciena advertises that its Discovery Resource Adapters “[c]apture[] all types of inventory data from network resources... either direct from the device family or an EMS.” The figure below also

²⁷

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024).

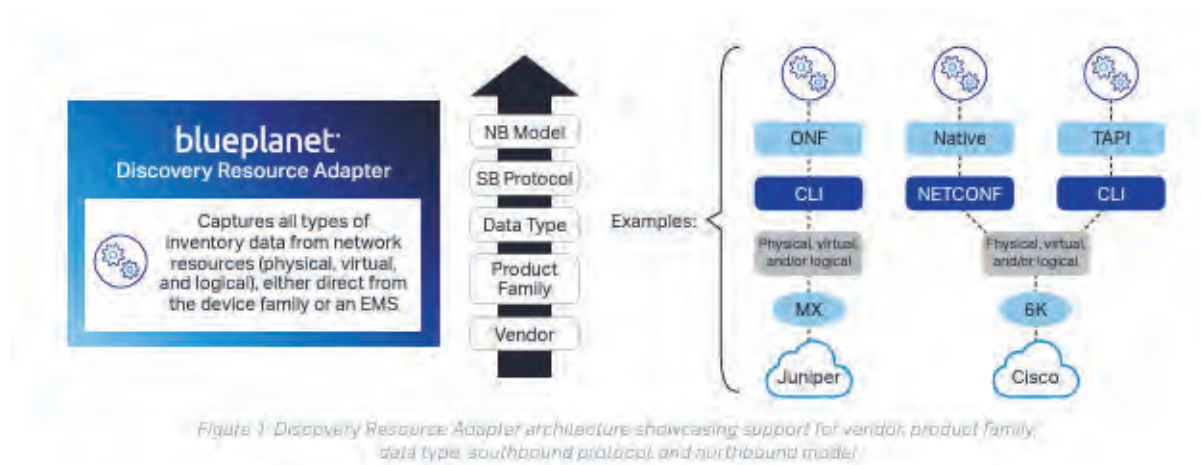
²⁸

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024).

²⁹

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024).

shows examples of communication protocols employed by Ciena Discovery Resource Adapters.³⁰



55. As a further example, and as depicted in the figure below, Ciena discloses that information such as telemetry, event, and/or fault data is collected by its Resource Adapters to feed into Blue Planet’s Unified Assurance and Analytics (UAA).³¹ Ciena’s UAA Resource Adapters provide “comprehensive device support that includes discovery of all physical, virtual, and service inventory, as well as support for key protocols including SNMP, TL-1, APIs, Netconf, and streaming telemetry, among others.”³² Further, a Ciena UAA Resource Adapter “will discover

³⁰

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024).

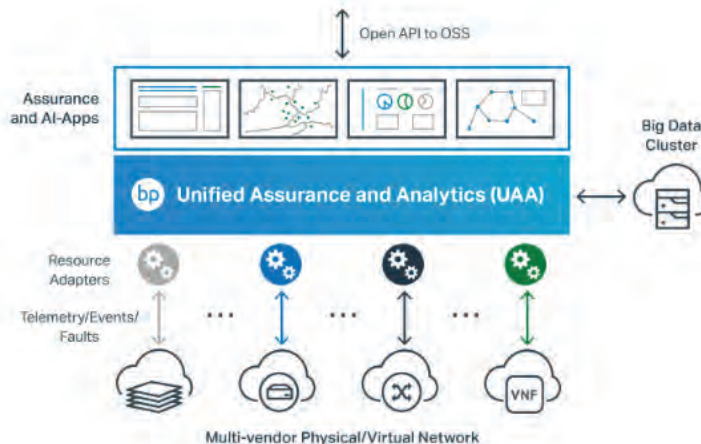
³¹ <https://www.blueplanet.com/products/uaa.html> (last visited October 14, 2024).

³²

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024).

each device's inventory, begin processing traps or alarms, and start polling for metrics supported for that device.”³³

Blue Planet Unified Assurance and Analytics



56. Furthermore, Ciena advertises that “[o]pen southbound interfaces and Resource Adapters (RAs) enable Blue Planet to communicate with control and/or manage a wide array of multi-vendor network functions (physical, virtual, or whole domain) using a variety of protocols and interfaces including CLI, OpenFlow, TL1, NETCONF/YANG, and others.”³⁴

³³

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024).

³⁴

<https://manuals.plus/m/e0a8a7f7c005eb2cfdb698612b839a7dd4355f8b778f751030300cc66c0ce957.pdf> (last visited October 14, 2024).

57. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1A] of the '282 Patent.

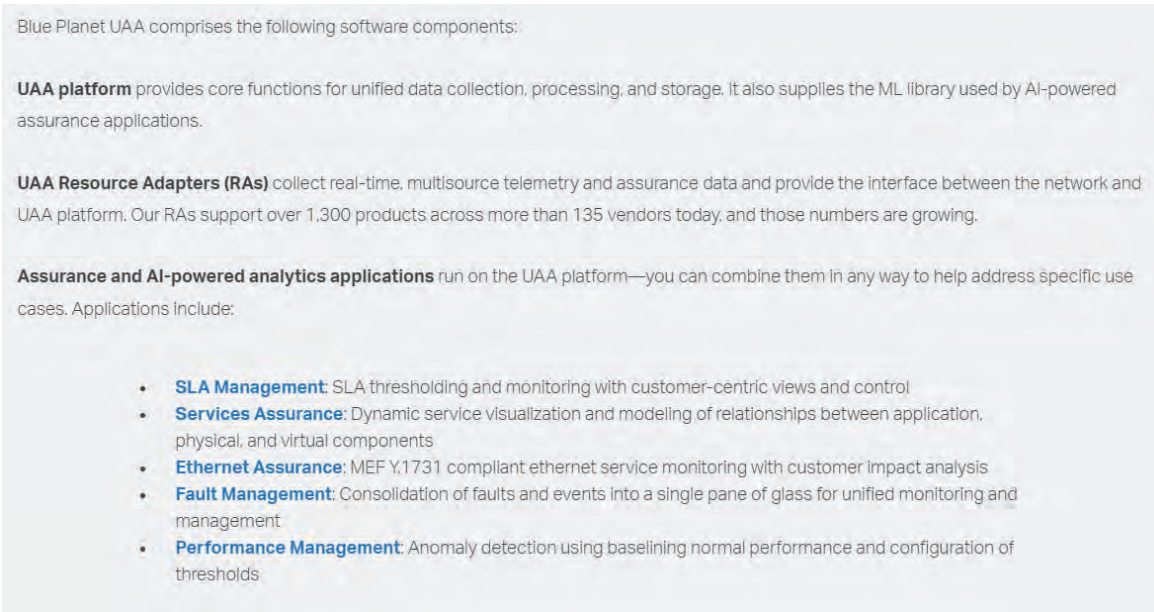
58. Limitation [1B] requires: “processing, by the first application server instance, the first adapter processed information based on an event management service to produce application processed information.” Ciena, through the Accused Instrumentalities, performs this step of the claimed method by operating, maintaining, and enabling others to operate, utilize, or otherwise benefit from Ciena’s Blue Planet Intelligent Automation Portfolio. For example, as shown above in at least Figure 5, Ciena’s Blue Planet Discovery Resource Adapter “[c]aptures all types of inventory data from network resources (physical, virtual, and logical), either direct from the device family or an EMS”³⁵ which demonstrates that first adapter information is processed based on an event management service.

59. As a further example, Ciena advertises that its “[a]ssurance and AI-powered analytics applications run on the UAA platform—you can combine them in any way to help address specific use cases” and goes on to list as included applications “Fault Management”—advertised as “[c]onsolidation of faults and events into a single pane of glass for unified monitoring and management”—and

35

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024).

“Performance Management”—advertised as comprising “[a]nomaly detection using baselining normal performance and configuration of thresholds.”³⁶ As a non-limiting example, Ciena’s Resources Adapters collect telemetry, event, and/or fault data (i.e., first adapter processed information) from network elements. According to Ciena’s documentation, that first adapter processed information is then further processed by, for example, the Fault Management and/or the Performance Management applications, to produce application processed information.³⁷



³⁶ <https://www.blueplanet.com/products/uaa.html> (last visited October 14, 2024).

³⁷ <https://www.blueplanet.com/products/uaa.html> (last visited October 14, 2024).

See also

<https://manuals.plus/m/e0a8a7f7c005eb2cfdb698612b839a7dd4355f8b778f751030300cc66c0ce957.pdf> (last visited October 14, 2024) (stating that one of the four “primary use cases” served by Blue Planet is “SDN Management and Control: Fault, Configuration, Accounting, Performance, Security (FCAPS) management and control of multi-vendor and multi-layer physical network elements”).

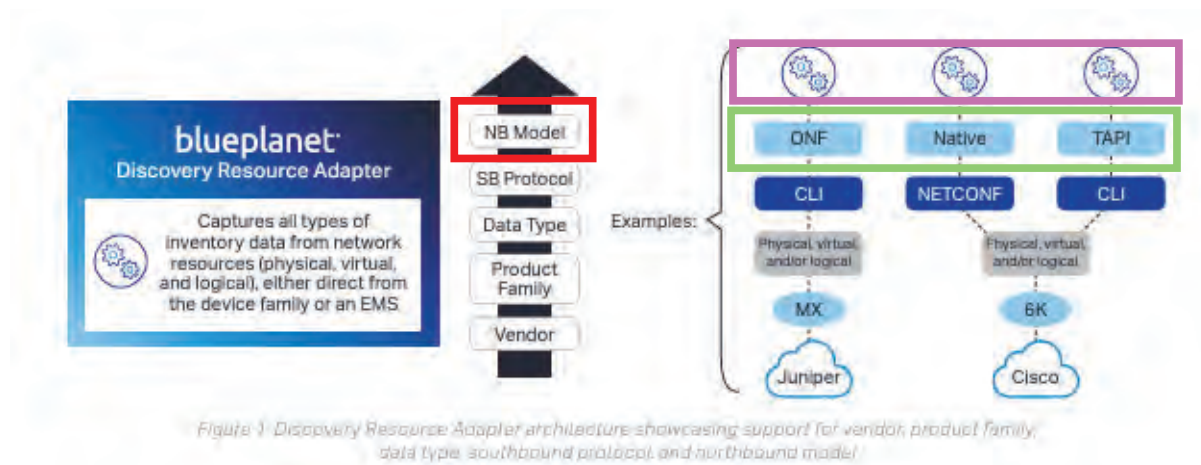
60. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1B] of the '282 Patent.

61. Limitation [1C] requires: “sending, by the first application server instance, the application processed information to a gateway device, wherein the gateway device is one of a plurality of gateway devices respectively associated with the plurality of application server instances and is configured to transfer the application processed information to a second adapter of a plurality of second adapters configured to process the application processed information based on a second communication protocol to produce second adapter processed information and transfer the second adapter processed information to an operation support system device.” Ciena, through the Accused Instrumentalities, performs this step of the claimed method by operating, maintaining, and enabling others to operate, utilize, or otherwise benefit from Ciena’s Blue Planet Intelligent Automation Portfolio. For example, as shown in at least the figure below, the highlighted “NB Model” or northbound mode sends data from the Blue Planet system to other OSS systems.³⁸ The figure below also discloses various gateway devices (outlined in

³⁸

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024) (emphasis added).

green), including without limitation ONF, TAPI, etc., that transfer northbound data to the Ciena Blue Planet Resource Adapters (e.g., the second adapter, outlined in purple). Further, the figure below discloses different protocols such as NETCONF and CLI.



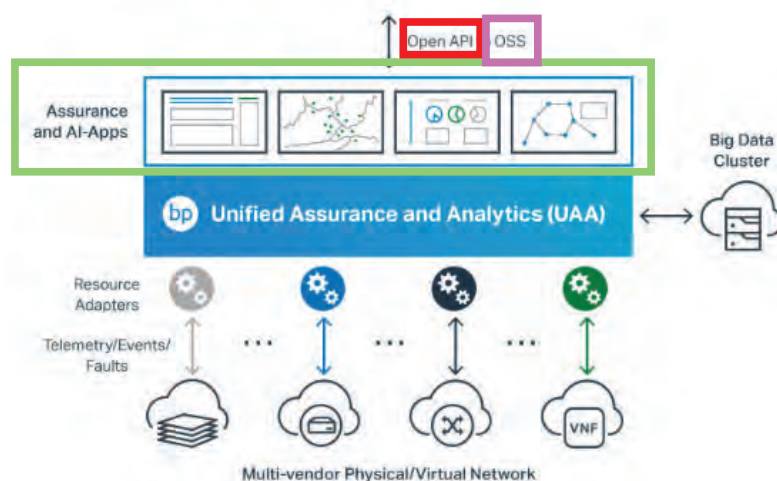
62. According to Ciena documentation, “TAPI is a standard for coordinating machine-to-machine communication particularly for the purposes of synchronizing network state information between two systems. The TAPI Bulk Sync APIs designed to efficiently and reliably synchronize bulk state data from a source system (in this case, MCP) to a destination system.”³⁹ Thus, Ciena, via its Blue Planet system, employs a gateway device out of a plurality of gateway devices that

³⁹ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/TAPI.html (last visited July 18, 2024). On information and belief, this document appears to be no longer available on Ciena’s website. See also https://web.archive.org/web/20220811144917/https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/TransportServiceMgmt.html (last visited October 14, 2024).

is configured to transfer network data. The disclosed “bulk state data from a source system” satisfies the claim limitation “transfer the second adapter processed information.” Further, Ciena’s “destination system” satisfies the claimed “operation support system device.”

63. As a further example, Ciena’s Blue Planet UAA documentation depicts various elements of claim limitation [1C]. As shown in the figure below, Ciena discloses transferring “Assurance and AI-apps” (outlined below in green) (i.e., the required “application processed information”) via “Open APIs” (outlined below in red) to “OSS” (outlined below in purple) (i.e., “operation support system device”).⁴⁰

Blue Planet Unified Assurance and Analytics



⁴⁰ <https://www.blueplanet.com/products/uaa.html> (last visited October 14, 2024) (emphasis added).

64. Ciena documentation further demonstrates the claimed “second adapter of a plurality of second adapters configured to process” data and transferring said data to an “operation support system device.” For example, Ciena software release notes state that “[t]he Resource Adapter (RA) Framework allows MCP to mediate to external models.”⁴¹

65. As a further example, Ciena documentation discloses that “RAs can use any open standard protocol such as Network Configuration Protocol (NETCONF), Representational State Transfer (REST), or other native interfaces supported by the device such as Command Line Interface (CLI). RAs provide flexible northbound adaptation to a standard data model. This flexible architecture ensures a standard

⁴¹ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/Topology.html (last visited July 18, 2024). On information and belief, the document appears to be no longer available on Ciena’s website. *See also* https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024) (“RAs can interface directly with any data source including existing inventory management systems, Element or Network Management Systems (EMS/NMS)...”); <https://manuals.plus/m/e0a8a7f7c005eb2cfdb698612b839a7dd4355f8b778f751030300cc66c0ce957.pdf> (last visited October 14, 2024), at Figure 1; https://www.analysysmason.com/globalassets/x_migrated-media/media/analysys_mason_ciena_blue_planet_profile_march2019_rma073.pdf (last visited October 14, 2024), Figure 6 (“The [Blue Planet (BP)] platform also communicates through northbound open APIs to third party OSS/BSS.”).

mediation framework exists between the southbound network function and the northbound tailored solutions.”⁴²

66. As a further example, Ciena documentation discloses that “RAs can interface directly with any data source including existing inventory management systems, [and] Element or Network Management Systems (EMS/NMS) [...]”⁴³

67. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1C] of the ’282 Patent.

68. Limitation [1D] requires: “in response to determining that the first application server instance has become disabled, facilitating establishing an association between the first adapter and a second application server instance of the plurality of application server instances and between the gateway device and the second application server instance.” Ciena, through the Accused Instrumentalities, performs this step of the claimed method by operating, maintaining, and enabling others to operate, utilize, or otherwise benefit from Ciena’s Blue Planet Intelligent Automation Portfolio. For example, Ciena documentation states that “Northbound

⁴²

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024).

⁴³

https://www.blueplanet.com/_data/assets/pdf_file/0023/137516/Discovery_Resource_Adapters_for_Blue_Planet_Inventory_DS.pdf (last visited October 14, 2024).

REST clients scale is achieved using a high-availability proxy (HAProxy) software load balancer... HAProxy uses a floating virtual IP (VIP) address to provide redundancy. All REST clients point to the MCP 'Site IP' virtual IP address. This approach achieves both scale and redundancy when interfacing with Northbound clients.”⁴⁴

69. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1D] of the '282 Patent.

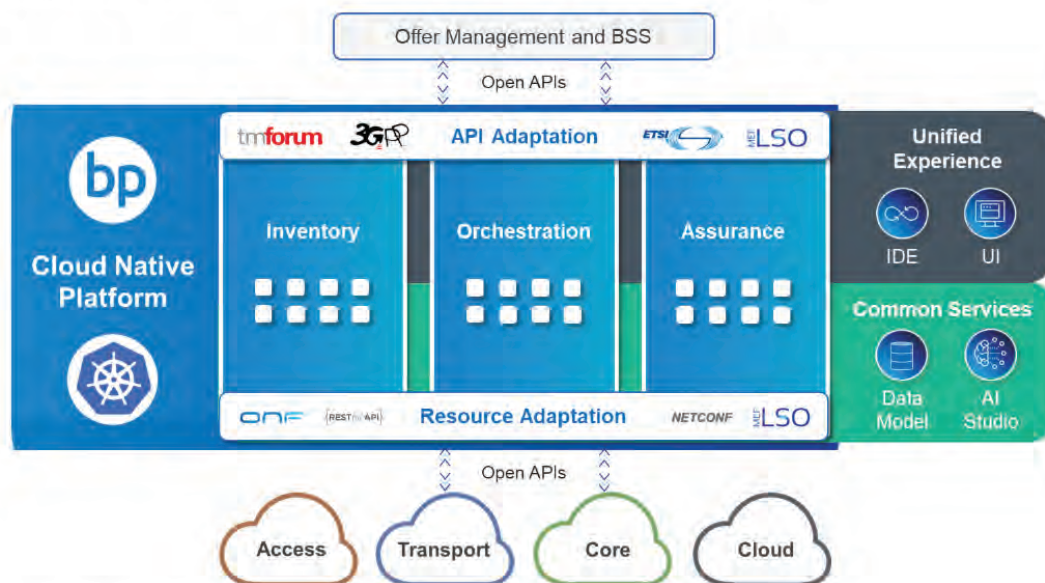
70. Thus, Ciena's operation and maintenance of the Accused Instrumentalities satisfies each and every limitation of claim 1 of the '282 Patent.

71. On information and belief, Ciena has directly used the Accused Instrumentalities in Ciena data centers and has directly used the Accused Instrumentalities when setting up, running, troubleshooting, and/or operating the Accused Instrumentalities on behalf of itself or its customers. As evidenced by the non-limiting examples below, support for these statements is located throughout Ciena's websites.

⁴⁴ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/Overview.html (last visited February 26, 2024). On information and belief, this document appears to be no longer available on Ciena's website.

72. On information and belief, the Accused Instrumentalities are used in data centers. For example, as shown below, Ciena advertises that its Blue Planet solution may be deployed “on premises, in any private or public cloud.”⁴⁵

Built on a ultra-modern Kubernetes-based architecture, the Blue Planet Cloud Native Platform (CNP) can be deployed on premises, in any private or public cloud—including AWS, Google, Microsoft and even in any multi-cloud mix of public and private clouds—with complete feature consistency. In addition to deployment flexibility, Blue Planet CNP also provides cloud-native support services that streamline the transition and ensure interoperability.

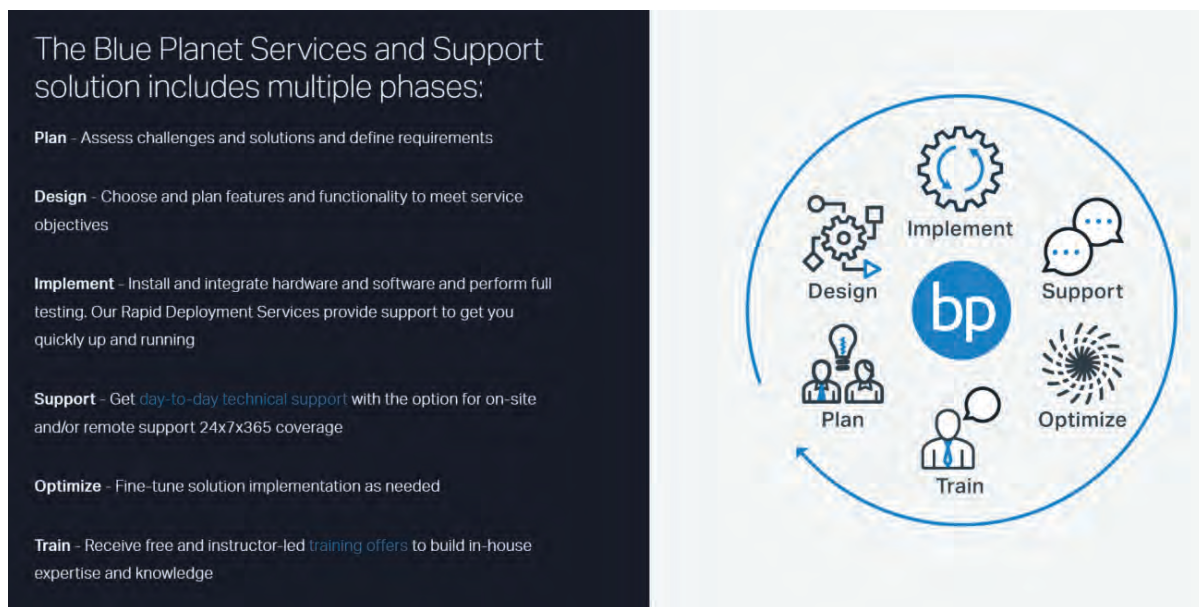


Blue Planet's Cloud Native Platform and applications

73. As a further example, as shown below, Ciena provides its customers with technical support for planning, deployment, and maintenance of its Blue Planet solution.⁴⁶

⁴⁵ <https://www.blueplanet.com/resources/what-is-cloud-native-oss> (last visited October 14, 2024).

⁴⁶ <https://www.blueplanet.com/support> (last visited October 14, 2024). See also <https://www.blueplanet.com/support/contacts> (last visited October 14, 2024)



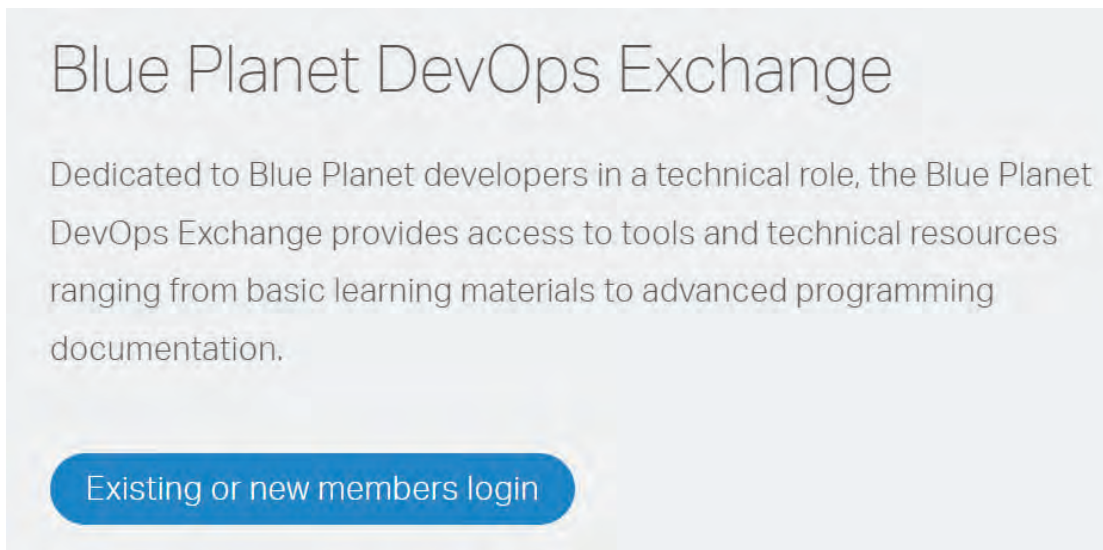
74. On information and belief, and based on publicly available information, Ciena provides customers and/or potential customers of its Blue Planet solution with multiple sources of technical support. For example, Ciena provides “[a]ccess to software library including latest updates and new, innovative product features” as well as “Blue Planet expertise to assist with product use, configuration, and troubleshooting issues.”⁴⁷ On further information and belief, Ciena provides a customer forum where technical information about its products and/or services may be discussed by its personnel and customers.⁴⁸ On further information and belief,

(“Customers can also take advantage of the Blue Planet Community, which is dedicated to helping you enrich your Blue Planet experience no matter where you are in your journey in network transformation.”).

⁴⁷ <https://www.blueplanet.com/support/contacts> (last visited October 14, 2024) (providing domestic and international contact information for technical support).

⁴⁸ <https://my.ciena.com/CienaPortal/s/blue-planet> (last visited October 14, 2024).

Ciena also provides a learning portal for its customers and potential customers to learn about the Accused Instrumentalities and their deployments and implementations.⁴⁹ On further information and belief, Ciena provides access to instructional and informational videos about its Accused Instrumentalities.⁵⁰ On further information and belief, Ciena also provides a “DevOps Exchange” “[d]edicated to Blue Planet developers in a technical role” that “provides access to tools and technical resources ranging from basic learning materials to advanced programming documentation.”⁵¹



⁴⁹ <https://www.blueplanet.com/learning> (last visited October 14, 2024).

⁵⁰ <https://www.blueplanet.com/learning/blue-planet-overview> (last visited October 14, 2024).

⁵¹ <https://www.blueplanet.com/learning/blue-planet-overview> (last visited October 14, 2024). On information and belief, login information to the DevOps exchange may be entered at https://developer.blueplanet.com/signin/?return_url=https://developer.blueplanet.com/index.html (last visited October 14, 2024).

75. On information and belief, Ciena has and continues to advertise its partnerships with its customers internationally and in the United States.⁵² For example, Ciena has touted its partnership with Consolidated Communications⁵³, and its integration of the Blue Planet solution to “provide Consolidated Communications with next generation network automation and control by leveraging ... the multi-vendor Blue Market Multi-Domain Service Orchestration (MDSO) and Blue Planet Route Optimization and Analysis (ROA) software.”⁵⁴ As another example, Ciena has and continues to advertise its business relationship with DISH Network Corporation: “Blue Planet is a key component within [DISH’s] 5G platform, allowing [DISH] to dynamically manage all of [its] network inventory and service order in real-time.”⁵⁵

76. Ciena was not licensed or otherwise authorized by K.Mizra to make, use, import, sell, or offer to sell any products and/or services covered by the ’282 Patent, and Ciena’s conduct is, in every instance, without K.Mizra’s consent.

⁵² See, e.g., <https://www.blueplanet.com/about/press-releases> (last visited October 14, 2024) (listing various news articles regarding Ciena’s partnerships with customers).

⁵³ On information and belief, Consolidated Communications is a third-party broadband provider and Ciena customer “serving customers across a 20-plus state service area.” See <https://www.consolidated.com/about-us> (last visited October 14, 2024).

⁵⁴ <https://www.blueplanet.com/about/press-releases/consolidated-communications-builds-5g-ready-network-with-cienas-adaptive-ip-solution.html> (last visited October 14, 2024).

⁵⁵ <https://www.blueplanet.com/about/press-releases/dish-selects-blue-planet-automation-software-to-accelerate-5g-services.html> (last visited October 14, 2024).

77. Ciena undertook the infringing actions despite an objectively high likelihood that such activities infringe the '282 Patent, which has been duly issued by the USPTO and presumed valid.

78. Since at least the date of first learning of the '282 Patent, which is no later than the date of the Notice Letters as detailed herein, Ciena has continued its infringing activities. As such, Ciena has willfully infringed the '282 Patent.

79. Since at least the date of first learning of the '282 Patent, which is no later than the date of the Notice Letters as detailed herein, Ciena has also indirectly infringed and continues to indirectly infringe the '282 Patent in violation of 35 U.S.C. § 271(b). Ciena has actively induced, for example, network service providers such as Consolidated Communications and/or DISH to directly infringe the '282 Patent by performing the method of claim 1 as detailed above throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Instrumentalities in various websites, including providing and disseminating product descriptions, operating manuals, technical documentation, instructional and/or informational videos, and other instructions on how to implement the Accused Instrumentalities. Examples of such advertising, promotion, and/or instruction include without limitation the documents cited in the paragraphs above. Ciena did so knowing and intending that its customers and end users commit these infringing acts, despite its knowledge of the '282 Patent,

thereby specifically intending for and inducing its customers to infringe the '282 Patent through the customers' normal and customary use of the Accused Instrumentalities.

80. As a result of Ciena's infringement of the '282 Patent, K.Mizra has suffered substantial injury and is entitled to recover all damages caused by Ciena's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Cisco's wrongful conduct, but in no event less than a reasonable royalty as provided for in 35 U.S.C. § 284.

COUNT II: INFRINGEMENT OF THE '176 PATENT

81. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

82. On information and belief, Ciena has directly infringed, literally and/or by the doctrine of equivalents, individually and/or jointly, one or more claims of the '176 Patent, including at least claim 1, in violation of 35 U.S.C. § 271, et seq., by using in this District and in the United States certain products and/or services, including but not limited to those, relating to the Accused Instrumentalities.

83. Based on publicly available information, Ciena's Accused Instrumentalities meet all elements of at least claim 1 of the '176 Patent.

84. Claim 1 of the '176 Patent provides:

[Preamble] A method, comprising:

- [1A]** encapsulating, by a first node device of a first network associated with a first service provider identity, a data packet with a pseudowire label determined based on an application flow specified by an application header of the data packet; and
- [1B]** selecting, based on the application flow, a routing policy from a set of application-specific routing policies defined for the first network, wherein the routing policy specifies that the data packet is to traverse at least a second network, comprising a second node device and associated with a second service provider identity, in transit to a third network comprising a third node device and associated with a third service provider identity.

85. Regarding the preamble of claim 1, to the extent the preamble is determined to be limiting, the Accused Instrumentalities perform the claimed method as set forth herein. For example, Ciena documents⁵⁶ provide:

⁵⁶ <https://www.blueplanet.com/products/orchestration.html> (last visited October 14, 2024).

Blue Planet Orchestration

Accelerate service velocity, improve service agility, and reduce service fulfillment OPEX

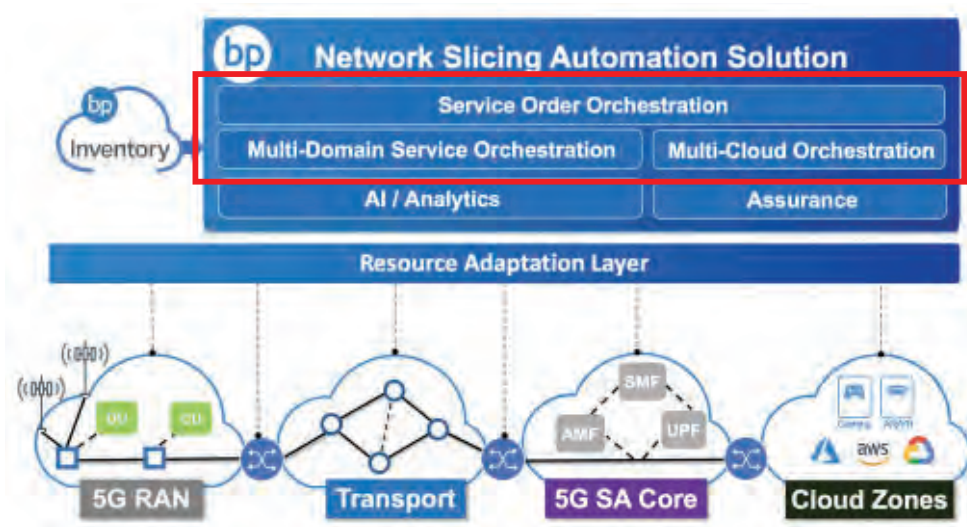
Blue Planet Orchestration (BPO) is a suite of open, modular, and vendor-agnostic product applications that help network operators improve customer experience, reduce OPEX, and achieve their business goals by automating service fulfillment end-to-end across complex multi-vendor and multi-domain networks.

The BPO suite is built on the Blue Planet Cloud Native Platform (CNP), a modern operations support system (OSS) that converges design, delivery, and assurance software applications to eliminate inefficient operational silos and help networks streamline the introduction and delivery of innovative services across network domains and vendors. Both the CNP and BPO suite can be flexibly deployed in private and public clouds or consumed in an elastic software-as-a-service (SaaS) model, letting you automate your order-to-service processes in complete alignment with your technical and business needs.

86. As a further example, Ciena states that “BPO consists of three modular software products—Service Order Orchestration (SOO), Multi-Domain Service Orchestration (MDSO), and Multi-Cloud Orchestration (MCO) that can be deployed individually or combined to fully automate the order-to-service process.”⁵⁷

⁵⁷ <https://www.blueplanet.com/products/orchestration.html> (last visited October 14, 2024).

87. As a further example, Ciena has depicted its Network Slicing Automation Solution as set forth below.⁵⁸ As shown below, Ciena discloses implementing operations across multiple domains and may work across various technology layers (see, e.g., red highlighted section).:



88. As a further example, Ciena states that its “Blue Planet products and services facilitate end-to-end visibility and management across physical and virtual components.”⁵⁹

89. As a further example, Ciena states: “Vendor and technology agnostic, [MDSO] discovers network resources and uses model-driven abstraction and templating to provide automated, repeatable, and policy-based service orchestration

⁵⁸ <https://www.blueplanet.com/solutions/5g-automation.html> (last visited October 10, 2023)(emphasis added). On information and belief, the current version of this webpage has been edited to exclude the above graphic.

⁵⁹ <https://www.ciena.com/insights/why/Why-NFV.html> (last visited October 14, 2024).

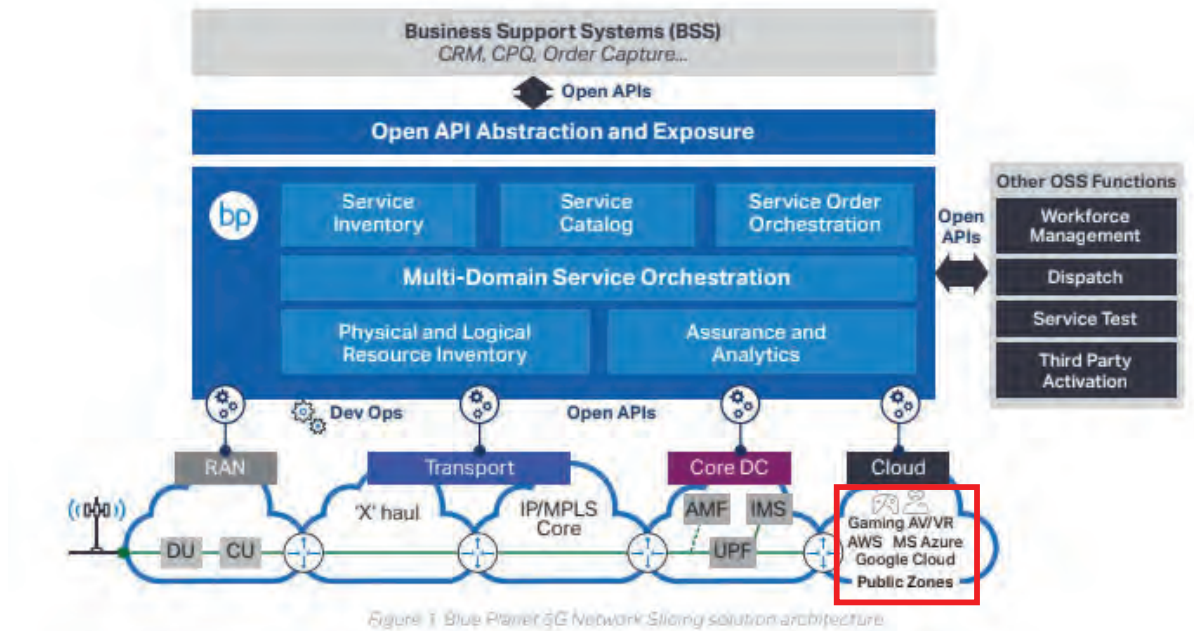
and activation end to end across network layers and domains.”⁶⁰ Further, Ciena describes its BPO suite as “fully programmable,” facilitating “service innovation” and avoiding “costs and risks associated with customizing legacy Operational Support Systems (OSS)” to let its customers “automate [their] order-to-service processes in complete alignment with [their] technical and business needs.”⁶¹

90. As a further example, Ciena has depicted its Blue Planet 5G Network Slicing Architecture as set forth below, which depicts service orchestration for different types of application flows or services such as “Gaming AR/VR,” “AWS,” “Google Cloud,” etc. (see red highlighting).⁶²

⁶⁰ <https://www.blueplanet.com/products/orchestration.html> (last visited October 14, 2024).

⁶¹ <https://www.blueplanet.com/products/orchestration.html> (last visited October 14, 2024).

⁶² https://www.blueplanet.com/_data/assets/pdf_file/0021/81264/5G_Automation_Network_Slicing_SB1.pdf (last visited August 22, 2024) (emphasis added). On information and belief, the current version of this webpage has been edited to exclude the above graphic.



91. As a further example, Ciena “partition[s] network resources and guarantee[s] SLAs by leveraging FlexE in the access portion of the networks and segment routing in the core—both standardized processes. These allow [Ciena] to have bandwidth guarantees and a Class of Service (CoS) structure.”⁶³ On information and belief, Blue Planet users may remotely adjust the parameters and quality of service of their network offerings, which allows users to have a single management/control interface that reduces the complexity of service operations.⁶⁴

⁶³ <https://www.ciena.com/insights/articles/2022/addressing-mid-market-opportunities-by-utilizing-network-convergence> (last visited October 14, 2024).

⁶⁴ See also <https://www.ciena.com/insights/articles/What-is-FlexEthernet-and-Why-is-it-so-Important.html> (last visited August 22, 2024) (“The net benefit [of FlexE] is the ability to remotely adjust service bandwidth as needed, more efficiently utilize each networking layer, and improve end-to-end manageability of the network.”). On information and belief, the webpage appears to be no longer available on Ciena’s website.

92. Thus, to the extent the preamble of claim 1 is limiting, Ciena performs the preamble of claim 1 at least by using the Blue Planet Intelligent Automation Portfolio.

93. Limitation [1A] requires “encapsulating, by a first node device of a first network associated with a first service provider identity, a data packet with a pseudowire label determined based on an application flow specified by an application header of the data packet.” On information and belief, Ciena, through the Accused Instrumentalities, performs this step of the claimed method by operating, maintaining, and enabling others to operate, utilize, or otherwise benefit from Ciena’s Blue Planet Intelligent Automation Portfolio. For example, on information and belief and as shown in the figure below, Ciena makes use of pseudowires in its Blue Planet solution, which encapsulates data packets associated with a service or application flow.⁶⁵

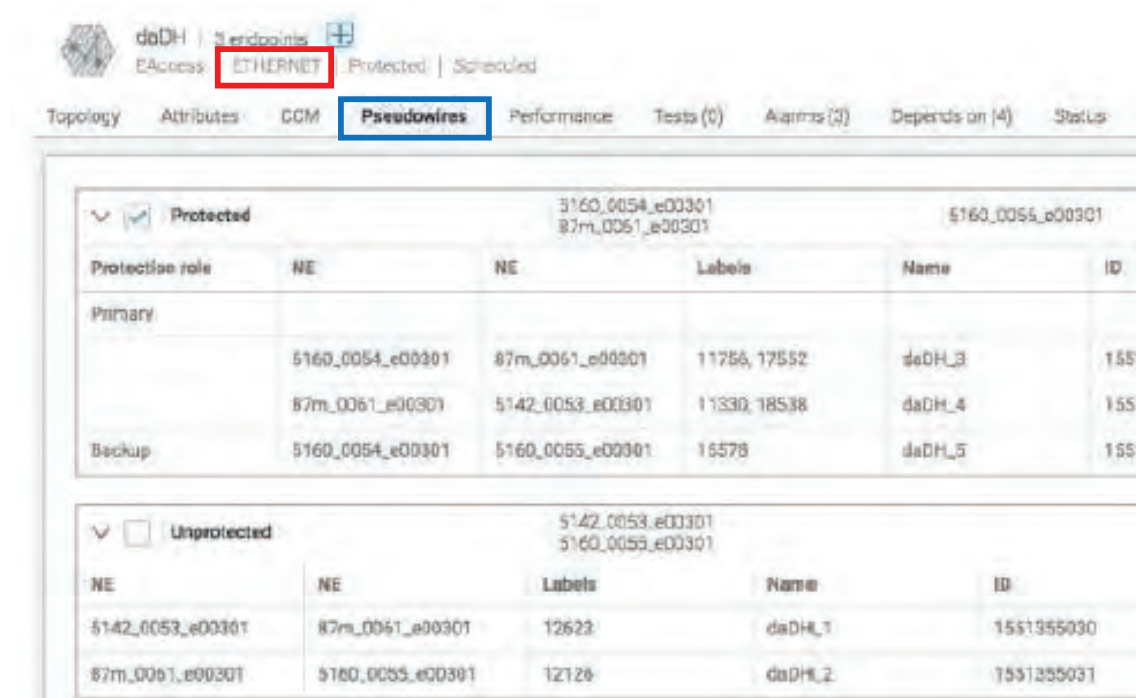
3. Click on the **Pseudowires** tab.

The Pseudowires tab displays the set of pseudowires| both protected and unprotected, that are associated with the service. There is a checkbox to the left of each pseudowire in the list.

94. As a further example, and as shown in the figure below, Ciena documentation discloses that Blue Planet may use “Ethernet” thus indicating a “first

⁶⁵ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/PacketInfrastructureMgmt.html (last visited October 20, 2023). On information and belief, this document appears to be no longer available on Ciena’s website.

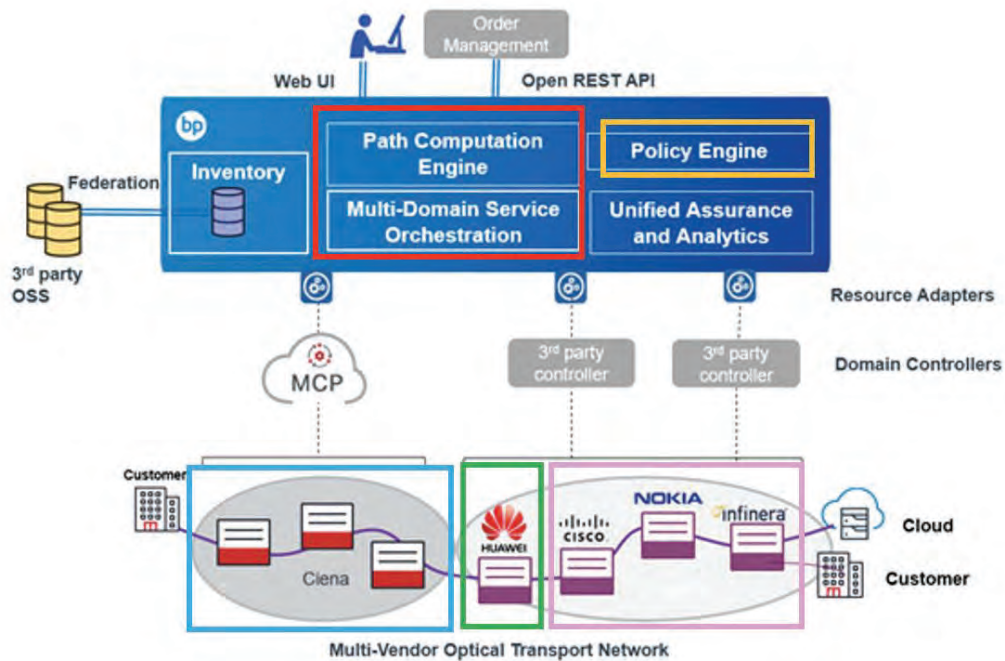
network associated with a first service provider identity (outlined in red below).⁶⁶ The Ciena documentation depicted below also discloses the use of pseudowires (outlined in blue below).



95. The illustration below also shows a first network associated with a service provider, which is outlined in blue.⁶⁷

⁶⁶ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/PacketInfrastructureMgmt.html (last visited October 20, 2023). On information and belief, this document appears to be no longer available on Ciena's website.

⁶⁷ <https://www.blueplanet.com/solutions/wave-services-automation.html> (last visited October 14, 2024) (emphasis added).



96. As a further example, and as shown in the figure below, Ciena documentation discloses that Blue Planet Blue Planet makes use of “pseudowires supporting a service that uses MPLS transport.”⁶⁸

If you want to view

information about the pseudowires supporting a service that uses MPLS transport.

Then

Click Pseudowires.

Pseudowires and LSPs details display, including the following information:

NOTE

The list of pseudowires is not in any particular order.

⁶⁸ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/PacketInfrastructureMgmt.html (last visited October 20, 2023). On information and belief, this document appears to be no longer available on Ciena’s website.

97. As a further example, Ciena documentation discloses using multi-segment pseudowires on different endpoints related to a particular Ethernet service. As shown below, and on information and belief, a “first node device” required by claim 1 of the ’176 Patent is the “root node” discussed in Ciena documentation.⁶⁹

Retrieve an E-Tree single-root service

This API call applies to service discovery and inventory of an E-Tree single-root service over Static MPLS transport only with:

- Multi-segment pseudowire (MS-PW) (6.x (as leaf), 8700 (as leaf or root), 6500 Packet Fabric (as leaf or root))
- Single-segment pseudowire (SS-PW) (6.x (as leaf), 8700 (as leaf or root), 6500 Packet Fabric (as leaf or root))

98. On information and belief, and as shown in the figure below, Ciena documentation discloses “endpoints” that are configured as “root” nodes for particular pseudowires, which encapsulates data. The excerpts below also demonstrate the definition of various endpoints, which correspond to the claim’s required first, second, and third node devices, each with their own “id.” According to Ciena, “[t]he endpoint ‘role’ has a single ‘root.’ The ‘role’ of each of the other endpoints is ‘leaf.’”⁷⁰

⁶⁹ https://software.ciena.com/releases/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/PacketServiceMgmt.html#provision-eline-pwhand (last accessed October 23, 2023). On information and belief, this document appears to be no longer available on Ciena’s website.

⁷⁰ https://software.ciena.com/releases/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/PacketServiceMgmt.html (last accessed October 23, 2023). On information and belief, this document appears to be no longer available on Ciena’s website.

```

    "endPoints": {
      "data": [
        {
          "type": "endPoints",
          "id": "1484498907288457250:1"
        },
        {
          "type": "endPoints",
          "id": "1484498907288457250:2"
        },
        {
          "type": "endPoints",
          "id": "1484498907288457250:3"
        }
      ]
    },

    "included": [
      {
        "id": "1484498907288457250:1",
        "type": "endPoints",
        "attributes": {
          "role": "root",
          "directionality": "bidirectional"
        }
      },

```

99. As a further example, Ciena documentation discloses the use and configuration of multi-segment pseudowires on different endpoints, as shown below.

71

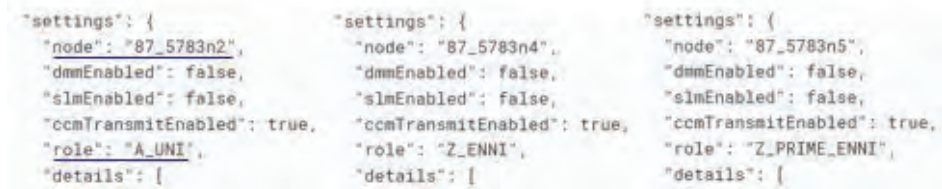
Provision a three-point E-Line service with pseudowire protection

You can use the MCP REST API to provision an E-Line service with Pseudowire protection (for both single-segment and multi-segment Pseudowires), and select one or more specific LSP tunnels to carry the A-Z, A-Z', and Z-Z' routes.

This capability is also supported in cases where the LSP path includes linear Q-in-Q spurs.

Note: The example below shows the configuration of a three-point protected E-Line service; but with minor variations the same API call can be used to provision a conventional two-point E-Line service instead.

⁷¹ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/PacketServiceMgmt.html (last accessed October 23, 2023). On information and belief, this document appears to be no longer available on Ciena's website.



```

"settings": {
  "node": "87_5783n2",
  "dmmEnabled": false,
  "slmEnabled": false,
  "ccmTransmitEnabled": true,
  "role": "A_UNI",
  "details": [
    "settings": {
      "node": "87_5783n4",
      "dmmEnabled": false,
      "slmEnabled": false,
      "ccmTransmitEnabled": true,
      "role": "Z_ENNI",
      "details": [
        "settings": {
          "node": "87_5783n5",
          "dmmEnabled": false,
          "slmEnabled": false,
          "ccmTransmitEnabled": true,
          "role": "Z_PRIME_ENNI",
          "details": [

```

100. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1A] of the '176 Patent.

101. Limitation [1B] requires “selecting, based on the application flow, a routing policy from a set of application-specific routing policies defined for the first network, wherein the routing policy specifies that the data packet is to traverse at least a second network, comprising a second node device and associated with a second service provider identity, in transit to a third network comprising a third node device and associated with a third service provider identity.” On information and belief, Ciena, through the Accused Instrumentalities, performs this step of the claimed method by operating, maintaining, and enabling others to operate, utilize, or otherwise benefit from Ciena’s Blue Planet Intelligent Automation Portfolio. For example, Ciena documentation describes its Multi-Domain Service Orchestration.⁷²

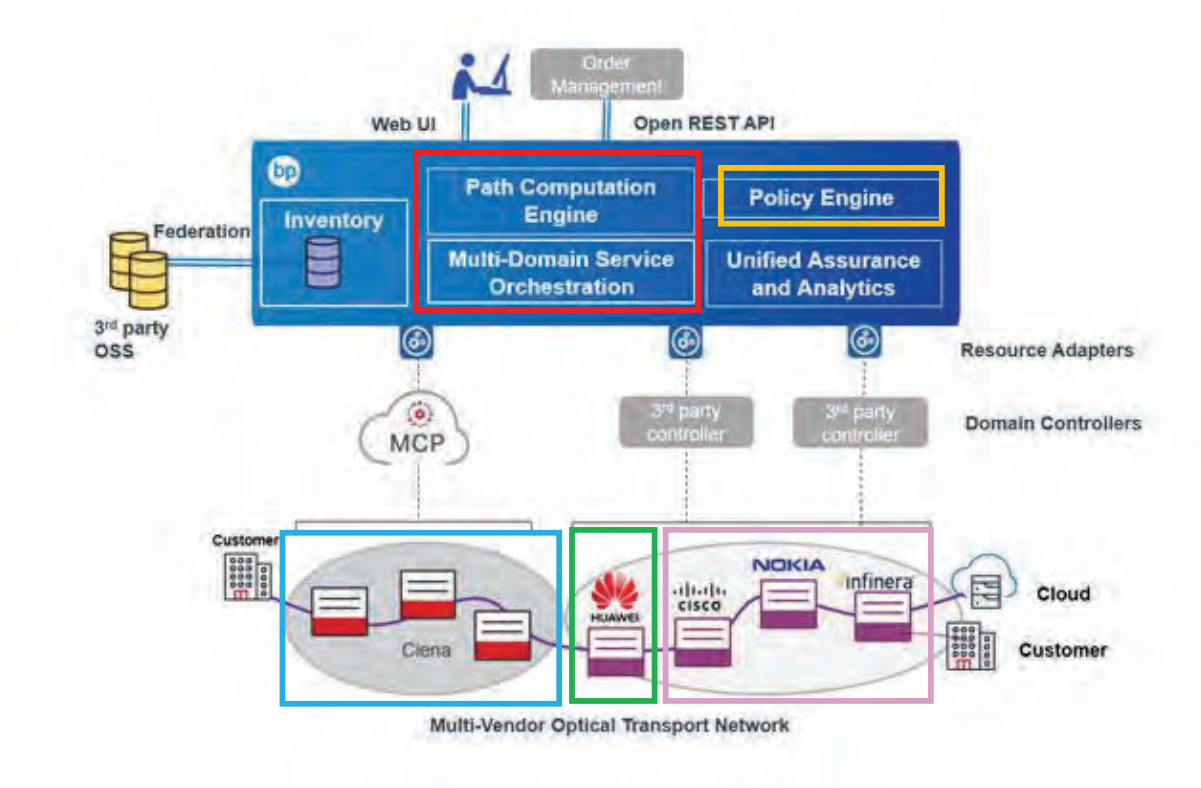
⁷² <https://www.blueplanet.com/products/orchestration.html> (last visited October 14, 2024).

Vendor and technology agnostic, MDSO discovers network resources and uses model-driven abstraction and templating to provide automated, repeatable, and policy-based service orchestration and activation end to end across network layers and domains. MDSO also improves troubleshooting efforts by unifying service and network visualization and correlating service-related issues with network events, and provides DevOps-style onboarding that simplifies the incorporation of new resources and technologies, streamlines new feature introduction, and accelerates new service creation.

102. As a further example, Ciena has depicted its Blue Planet solution as shown in the following figure.⁷³ The “Path Computation Engine” and “Multi-Domain Service Orchestration” (highlighted in red), for example, satisfy the claimed limitation of “selecting... a routing policy,” and the “Policy Engine” (highlighted in orange), for example, satisfies the the claimed limitation, “set of application-specific routing policies.” Further, the claim’s required “first network associated with a first service provider identity” is identified below by the blue box. The claim’s required “second network... associated with a second service provider identity” is identified

⁷³ <https://www.blueplanet.com/solutions/wave-services-automation.html> (last visited October 14, 2024) (emphasis added).

below by the green box. And the claim’s required “third network... associated with a third service provider identity” is identified by the purple box.



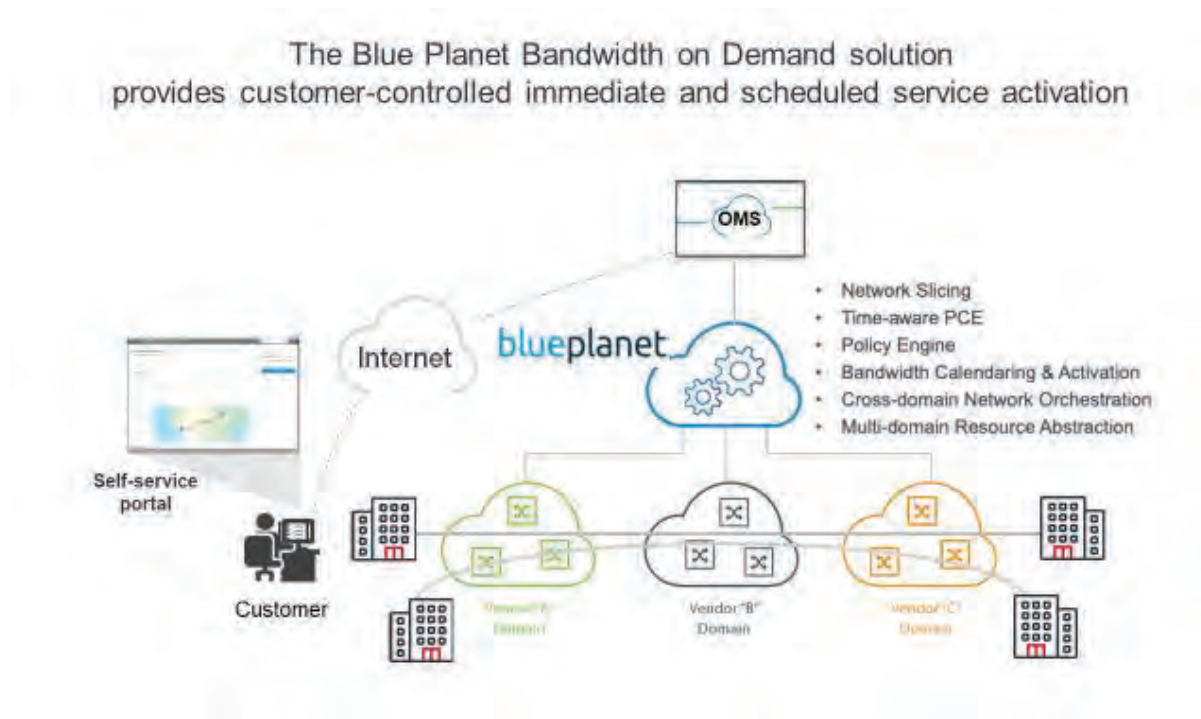
103. As a further example, Ciena’s Blue Planet solution offers “Bandwidth on Demand” and enables “clients [to] create, modify, terminate and schedule services,” such that network resources are reserved for particular application flows.⁷⁴

104. As a further example, Ciena includes the following illustration in describing its “Bandwidth On Demand” feature.⁷⁵ As shown below, Ciena discloses

⁷⁴ <https://www.blueplanet.com/solutions/bandwidth-on-demand.html> (last visited October 14, 2024).

⁷⁵ <https://www.blueplanet.com/solutions/bandwidth-on-demand.html> (last visited October 14, 2024).

the presence of a policy engine with a set of application-specific routing policies. On information and belief, Blue Planet enables the reservation of network resources for different clients according to their service and/or application needs. On further information and belief, Ciena discloses that the data may traverse multiple domains from a first network with a first service provider identity (denoted below as “Vendor ‘A’ Domain”), through a second network with a second service provider identity (denoted below as “Vendor ‘B’ Domain”), to a third service provider with a third service provider identity (denoted below as “Vendor ‘C’ Domain”).



105. As a further example, Ciena’s documentation discloses that during the provisioning of an Ethernet service, a user can assign a Class of Service (CoS)⁷⁶, which mapping can be rearranged for “adjacent service provider[s].”⁷⁷ Thus, the Blue Planet solution operates in a multiple service provider and multiple domain environment, in which data packets for particular services are routed accordingly.

106. As a further example, and as shown in the figure below, Ciena documentation discloses that provisioning an Ethernet service in its Blue Planet solution may include parameters such as “ingressCosSetting,” such that packets at the ingress of an endpoint or node are analyzed to comply with service orchestration parameters.⁷⁸

⁷⁶ A Class of Service (CoS) is defined by Ciena to mean “[a] queuing discipline in which an algorithm compares fields of packets or CoS tags to classify packets and assign them to queues of differing priority.” *See, e.g.*, <https://www.ciena.com/insights/telecom-glossary#LetterC> (last visited October 14, 2024).

⁷⁷ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/PacketServiceMgmt.html#provision-eline-cos-options (last accessed October 23, 2023). On information and belief, this document appears to be no longer available on Ciena’s website.

⁷⁸ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/PacketServiceMgmt.html#provision-eline-cos-options (last accessed October 23, 2023). On information and belief, this document appears to be no longer available on Ciena’s website.

POST {MCP_SERVER}/bpocore/market/api/v1/resources

Note that in the following API calls:

- L2_SVC_FACADE_PRODUCT_ID is a product ID to create Layer-2 Service in Facade.
- SVC_RSC_ID is the Facade resource ID of the Layer-2 service.

Note in particular the following CoS parameters for the service endpoints the sample call provided below:

"ingressCosSetting": { "ingressCosPolicy": "L2PcpCos"

"ingressCosSetting": { "ingressCosPolicy": "custom", "ingressCosMapName": "CustomCosMap"

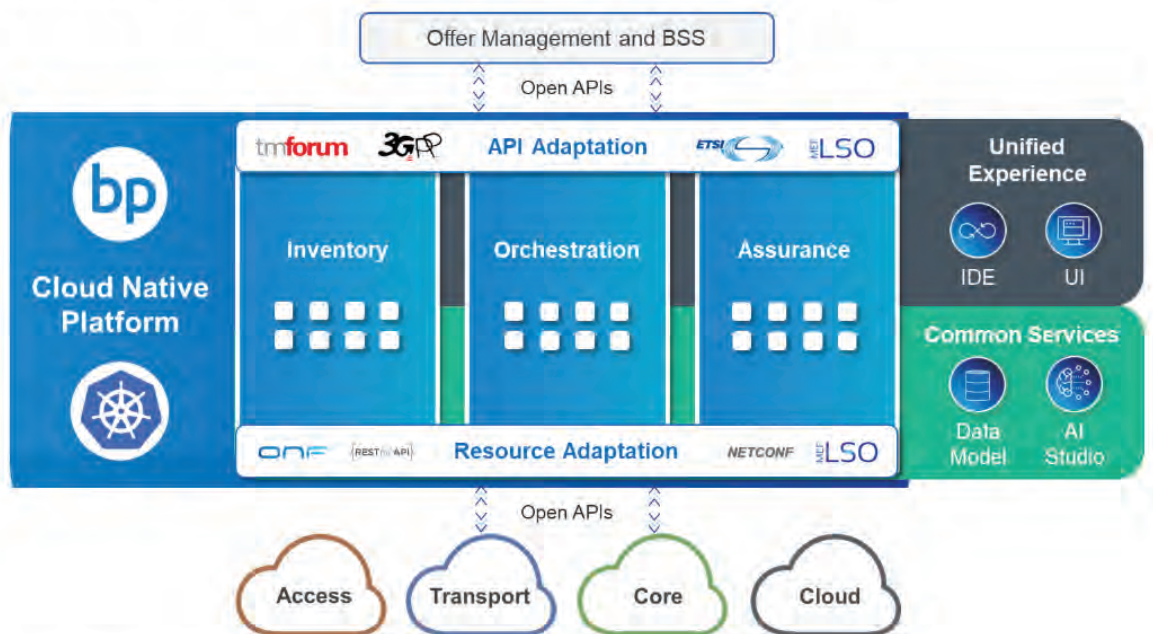
107. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1B] of the '176 Patent.

108. Thus, Ciena's operation and maintenance of the Accused Instrumentalities satisfies each and every limitation of claim 1 of the '176 Patent.

109. On information and belief, Ciena has directly used the Accused Instrumentalities in Ciena data centers and has directly used the Accused Instrumentalities when setting up, running, troubleshooting, and/or operating the Accused Instrumentalities on behalf of itself or its customers. As evidenced by the non-limiting examples below, support for these statements is located throughout Ciena's websites.

110. On information and belief, the Accused Instrumentalities are used in data centers. For example, as shown below, Ciena advertises that its Blue Planet solution may be deployed “on premises, in any private or public cloud.”⁷⁹

Built on a ultra-modern Kubernetes-based architecture, the Blue Planet Cloud Native Platform (CNP) can be deployed on premises, in any private or public cloud—including AWS, Google, Microsoft and even in any multi-cloud mix of public and private clouds—with complete feature consistency. In addition to deployment flexibility, Blue Planet CNP also provides cloud-native support services that streamline the transition and ensure interoperability.



Blue Planet's Cloud Native Platform and applications

111. As a further example, as shown below, Ciena provides its customers with technical support for planning, deployment, and maintenance of its Blue Planet solution.

⁷⁹ <https://www.blueplanet.com/resources/what-is-cloud-native-oss> (last visited October 14, 2024).

112. On information and belief, and based on publicly available information, Ciena provides customers and/or potential customers of its Blue Planet solution with multiple sources of technical support. For example, Ciena provides “[a]ccess to software library including latest updates and new, innovative product features” as well as “Blue Planet expertise to assist with product use, configuration, and troubleshooting issues.”⁸⁰ On further information and belief, Ciena provides a customer forum where technical information about its products and/or services may be discussed by its personnel and customers.⁸¹ On further information and belief, Ciena also provides a learning portal for its customers and potential customers to learn about the Accused Instrumentalities and their deployments and implementations.⁸² On further information and belief, Ciena provides access to instructional and informational videos about its Accused Instrumentalities.⁸³ On further information and belief, Ciena also provides a “DevOps Exchange” “[d]edicated to Blue Planet developers in a technical role” that “provides access to

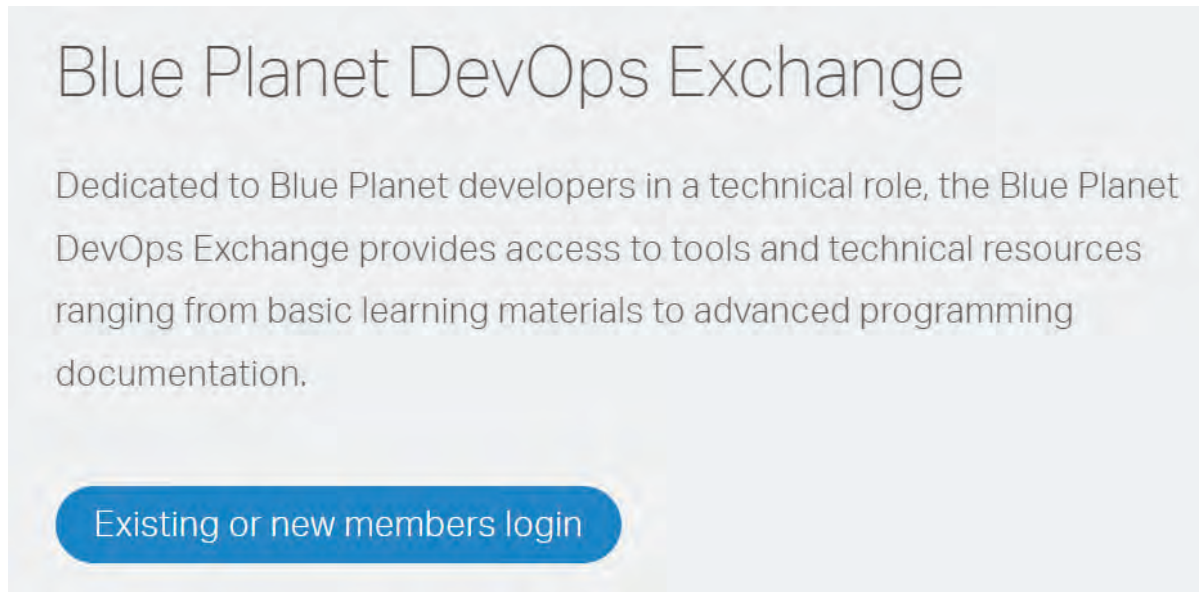
⁸⁰ <https://www.blueplanet.com/support/contacts> (last visited October 14, 2024) (providing domestic and international contact information for technical support).

⁸¹ <https://my.ciena.com/CienaPortal/s/blue-planet> (last visited October 14, 2024).

⁸² <https://www.blueplanet.com/learning> (last visited October 14, 2024).

⁸³ <https://www.blueplanet.com/learning/blue-planet-overview> (last visited October 14, 2024).

tools and technical resources ranging from basic learning materials to advanced programming documentation.”⁸⁴



113. On information and belief, Ciena has and continues to advertise its partnerships with its customers internationally and in the United States.⁸⁵ For example, Ciena has touted its partnership with Consolidated Communications⁸⁶, and

⁸⁴ <https://www.blueplanet.com/learning/blue-planet-overview> (last visited October 14, 2024). On information and belief, login information to the DevOps exchange may be entered at https://developer.blueplanet.com/signin/?return_url=https://developer.blueplanet.com/index.html (last visited October 14, 2024).

⁸⁵ See, e.g., <https://www.blueplanet.com/about/press-releases> (last visited October 14, 2024) (listing various news articles regarding Ciena’s partnerships with customers).

⁸⁶ On information and belief, Consolidated Communications is a third-party broadband provider and Ciena customer “serving customers across a 20-plus state service area.” See <https://www.consolidated.com/about-us> (last visited October 14, 2024).

its integration of the Blue Planet solution to “provide Consolidated Communications with next generation network automation and control by leveraging ... the multi-vendor Blue Market Multi-Domain Service Orchestration (MDSO) and Blue Planet Route Optimization and Analysis (ROA) software.”⁸⁷ As another example, Ciena has and continues to advertise its business relationship with DISH Network Corporation: “Blue Planet is a key component within [DISH’s] 5G platform, allowing [DISH] to dynamically manage all of [its] network inventory and service order in real-time.”⁸⁸

114. Ciena was not licensed or otherwise authorized by K.Mizra to make, use, import, sell, or offer to sell any products and/or services covered by the ’176 Patent, and Ciena’s conduct is, in every instance, without K.Mizra’s consent.

115. Ciena undertook the infringing actions despite an objectively high likelihood that such activities infringe the ’176 Patent, which has been duly issued by the USPTO and presumed valid.

116. Since at least the date of first learning of the ’176 Patent, which is no later than the date of the Notice Letters as detailed herein, Ciena has continued its infringing activities. As such, Ciena has willfully infringed the ’176 Patent.

⁸⁷ <https://www.blueplanet.com/about/press-releases/consolidated-communications-builds-5g-ready-network-with-cienas-adaptive-ip-solution.html> (last visited October 14, 2024).

⁸⁸ <https://www.blueplanet.com/about/press-releases/dish-selects-blue-planet-automation-software-to-accelerate-5g-services.html> (last visited October 14, 2024).

117. Since at least the date of first learning of the '176 Patent, which is no later than the date of the Notice Letters as detailed herein, Ciena has also indirectly infringed and continues to indirectly infringe the '176 Patent in violation of 35 U.S.C. § 271(b). Ciena has actively induced, for example, network service providers such as Consolidated Communications and/or DISH to directly infringe the '176 Patent by performing the method of claim 1 as detailed above throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Instrumentalities in various websites, including providing and disseminating product descriptions, operating manuals, technical documentation, instructional and/or informational videos, and other instructions on how to implement the Accused Instrumentalities. Examples of such advertising, promotion, and/or instruction include without limitation the documents cited in the paragraphs above. Ciena did so knowing and intending that its customers and end users commit these infringing acts, despite its knowledge of the '176 Patent, thereby specifically intending for and inducing its customers to infringe the '176 Patent through the customers' normal and customary use of the Accused Instrumentalities.

118. As a result of Ciena's infringement of the '176 Patent, K.Mizra has suffered substantial injury and is entitled to recover all damages caused by Ciena's infringement to the fullest extent permitted by the Patent Act, together with

prejudgment interest and costs for Cisco's wrongful conduct, but in no event less than a reasonable royalty as provided for in 35 U.S.C. § 284.

COUNT III: INFRINGEMENT OF THE '320 PATENT

119. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

120. On information and belief, Ciena has directly infringed, literally and/or by the doctrine of equivalents, individually and/or jointly, one or more claims of the '320 Patent, including at least claim 1, in violation of 35 U.S.C. § 271, et seq., by using in this District and in the United States certain products and/or services, including but not limited to those, relating to the Accused Instrumentalities.

121. Based on publicly available information, Ciena's Accused Instrumentalities meet all elements of at least claim 1 of the '320 Patent.

122. Claim 1 of the '320 Patent provides:

[Preamble] A method comprising:

[1A] at a node associated with a multiprotocol label switching system (MPLS) network, performing:

[1B] identifying information associated with an application flow based on one or more unencapsulated packet headers of the application flow or based on an ingress data stream that includes the application flow;

[1C] in response to identifying the information, and based on stored data that maps application flows with pseudowires, determining a plurality of pseudowires corresponding to paths through the MPLS network, wherein the stored data indicates, for a sending device application, a

distributed mapping of the application flow via at least one of the plurality of pseudowires; and

[1D] communicating data related to the sending device application via at least one of the plurality of pseudowires.

123. Regarding the preamble of claim 1, to the extent the preamble is determined to be limiting, the Accused Instrumentalities perform the claimed method as set forth herein. For example, as shown in the figure below, Ciena documents describe Blue Planet’s “Route Optimization and Analysis (ROA)” feature, which involves “IP/MPLS networks” and states that ROA has “path computation and provisioning capabilities.”⁸⁹

⁸⁹ <https://www.blueplanet.com/products/route-optimization.html> (last visited October 14, 2024).

Route Optimization and Analysis (ROA)

Path-aware observability and automation for IP/MPLS networks

Assure and automate your IP/MPLS network and services

Modern IP/MPLS networks are built on a vendor-agnostic, ecosystem approach with thousands of routing paths—each carrying a myriad number of critical services and 5G network slices.

These dynamic networks need next-gen analytics and observability for informed decision-making and to enable faster activation, assurance, and automation of IP/MPLS services and slices. But traditional monitoring tools fall short of delivering meaningful insights that correlate network performance and routing behavior with service delivery.

Blue Planet® Route Optimization and Analysis (ROA) fills this visibility and management gap in your IP/MPLS networks. It delivers observability into IP/MPLS network and overlay services, including 5G network slices from any tower to the data center. And with ROA's path computation and provisioning capabilities, you are on the path to service automation.

124. As a further example, Ciena describes ROA as being “used by the world’s leading network operators, enterprises, and government entities to assure the delivery of critical Layer 3 services across the cloud.”⁹⁰ Further, as shown in the figure below, ROA “recommends new TE tunnels to split traffic and automatically provisions them, helping alleviate congestion.”

90

https://www.blueplanet.com/data/assets/pdf_file/0023/9257/Route_Optimization_and_Analysis_DS_4_2024.pdf (last visited October 14, 2024).

ROA leverages routing and traffic data to enable automation of service provisioning and assurance. Its IP/MPLS Automation module's built-in PCE can compute the best route from a source to destination and uses ROA's PCEP support to automatically provision a new RSVP-TE or segment mouting TE tunnel. The module also provides recommendations based on traffic matrices to identify congested links or links with the longest paths (most hops) to optimize. It then recommends new TE tunnels to split traffic and automatically provisions them, helping alleviate congestion.

125. As a further example, Ciena states that its “IP/MPLS Automation also enables policy-driven automated optimization for existing TE tunnels to alleviate congestion. Based on traffic matrices, it can identify heavily congested links or links with most hops and use optimization algorithms to split among multiple paths, thereby optimizing the network and alleviating congestion.”⁹¹

126. Thus, to the extent the preamble of claim 1 is limiting, Ciena performs the preamble of claim 1 at least by using the Blue Planet Intelligent Automation Portfolio.

127. Limitation [1A] requires “at a node associated with a multiprotocol label switching system (MPLS) network, performing...” On information and belief, Ciena, through the Accused Instrumentalities, satisfies this limitation of the claim by operating, maintaining, and enabling others to operate, utilize, or otherwise benefit

⁹¹ <https://www.blueplanet.com/products/route-optimization.html> (last visited October 14, 2024).

from Ciena's Blue Planet Intelligent Automation Portfolio. For example, the Ciena graphic below demonstrate nodes in the Blue Planet-administered MPLS network.⁹²

The screenshot shows the 'Pseudowires' tab in the Ciena Blue Planet Intelligent Automation Portfolio. The interface displays a network topology with various nodes and connections. The 'Protected' section is expanded, showing a table of pseudowires. The table has columns for Protection role, NE, NE, Labels, Name, ID, and Signaling type. The 'Unprotected' section is also visible below the 'Protected' section.

Protection role	NE	NE	Labels	Name	ID	Signaling type
Primary	5160_0054_e00301	87m_0061_e00301	11756, 17552	daDH_3	1551355032	static
	87m_0061_e00301	5142_0053_e00301	11330, 18538	daDH_4	1551355033	static
Backup	5160_0054_e00301	5160_0055_e00301	15578	daDH_5	1551355030	static

NE	NE	Labels	Name	ID	Signaling type
5142_0053_e00301	87m_0061_e00301	12623	daDH_1	1551355030	static
87m_0061_e00301	5160_0055_e00301	12126	daDH_2	1551355031	static

128. On information and belief, and as shown in the figure above, Ciena discloses nodes (labeled “NE” and assigned names) that use a plurality of pseudowires. Moreover, the above figure discloses the existence of various Label Switched Paths through the MPLS network.

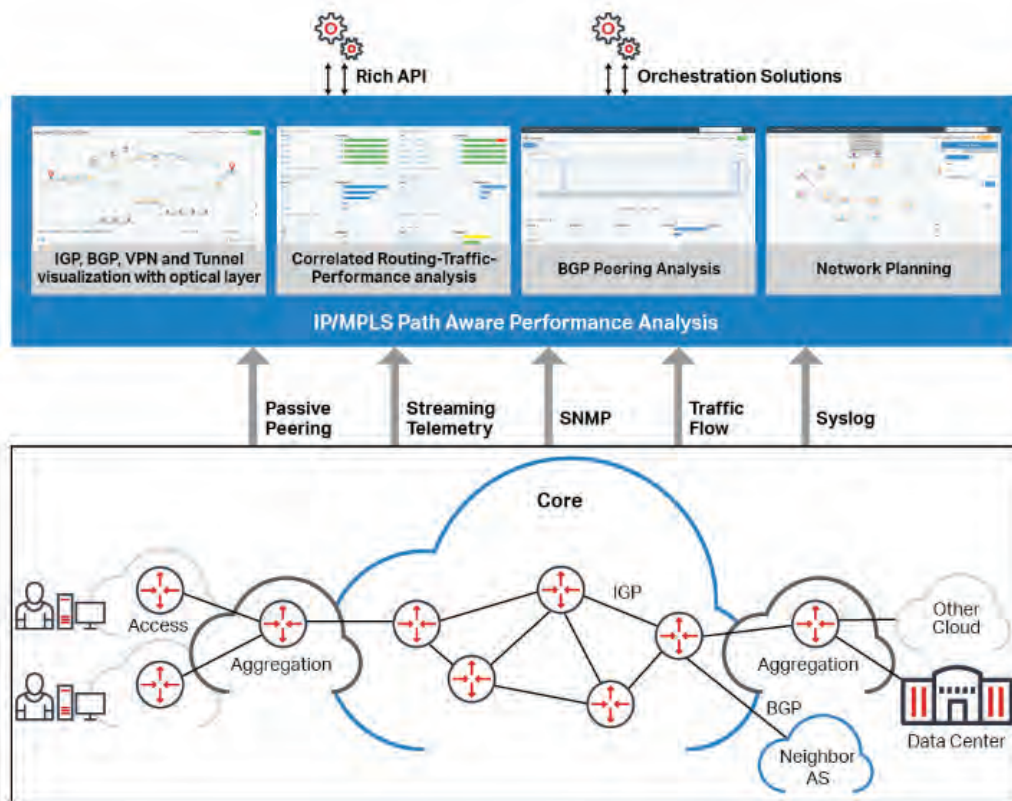
⁹² https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/PacketInfrastructureMgmt.html (last visited October 23, 2023). On information and belief, this document appears to be no longer available on Ciena's website.

129. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1A] of the '320 Patent.

130. Limitation [1B] requires “identifying information associated with an application flow based on one or more unencapsulated packet headers of the application flow or based on an ingress data stream that includes the application flow.” On information and belief, Ciena, through the Accused Instrumentalities, performs this step of the claimed method by operating, maintaining, and enabling others to operate, utilize, or otherwise benefit from Ciena’s Blue Planet Intelligent Automation Portfolio.⁹³

⁹³ <https://www.blueplanet.com/products/route-optimization.html> (last visited October 14, 2024).

How Blue Planet ROA helps



131. As shown in the figure above, Blue Planet operates in an IP/MPLS environment. Further, the figure above demonstrates that application traffic flow is analyzed by the Blue Planet solution, indicating that it identifies information associated with an application flow.

132. As another example, Ciena advertises that “Blue Planet is orchestrating and controlling mission critical services and applications,”⁹⁴ which further

⁹⁴ <https://www.ciena.com/insights/why/Why-NFV.html> (last visited October 14, 2024).

demonstrates that Blue Planet identifies information associated with an application flow. Other examples demonstrating that Blue Planet identifies information associated with application flows appear in various other instances on Ciena's website. For example, Ciena advertises Blue Planet's ability to maintain "the availability and performance of critical SCADA applications"⁹⁵ and that Blue Planet "delivers a real-time view of the IP/MPLS topology with correlated traffic flow and performance metrics to help network operators visualize how routing behavior affects service delivery and optimizes the delivery of critical services."⁹⁶

133. As a further example, and as shown in the figure below, Ciena discloses that Blue Planet performs network slicing for specific user equipment application flows such as gaming and mobile.⁹⁷

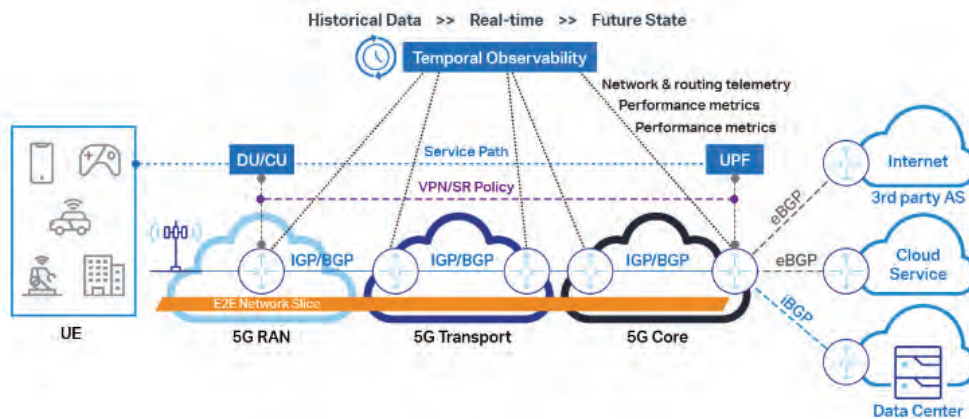
⁹⁵ <https://www.ciena.com/insights/articles/How-utility-network-managers-can-gain-critical-visibility-to-meet-user-demands.html> (last visited August 22, 2024). On information and belief, this document appears to be no longer available on Ciena's website.

⁹⁶ <https://www.blueplanet.com/accelerate-digital-transformation> (last visited October 14, 2024).

⁹⁷ <https://www.blueplanet.com/accelerate-digital-transformation> (last visited October 14, 2024).

5G network slicing assurance

The viability of future 5G services hinges on the ability to activate, monitor, and assure thousands of network slices in real-time. What's more, assuring network slice SLAs is a necessary step toward monetizing 5G slices, and this requires a new kind of network monitoring—one that understands the traffic, service, and path from the device to the application in the cloud across multiple protocols and technology domains.



134. As a further example, Ciena documentation discloses that Blue Planet may provision service (e.g., Layer 2 services and L3VPN) for specific customers and associate customer names with specific tunnels, thus identifying information associated with an application flow based on an ingress data stream that includes the application flow.⁹⁸

⁹⁸ See, e.g., https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/L3VPNservice.html#viewing-l3-vpn-service~:text=Create%20%22L3%20VPN%20service%22 (last visited October 23, 2023); https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/PacketInfrastructureMgmt.html#packet-infrastructure-management (last visited October 23, 2023). On information and belief, neither of these documents appears to be available on Ciena's website any longer.

135. As a further example, Ciena documentation discloses that Blue Planet is used to configure peer routers for specific customers or applications. In at least one example, Ciena states that “there are two exit routers labeled as LAX-P-101 and ORD-P-122 has direct peering with Google, whereas LAX-P-101 takes a longer route, traversing through multiple transit AS’s, with AS 3356 as the last hop before reaching the Google prefix. BGP prefers shorter AS path routes, so it dictates that the direct peering routers should be used.”⁹⁹ Thus, Blue Planet identifies traffic based on ingress data streams at particular peered routers.

136. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1B] of the ’320 Patent.

137. Limitation [1C] requires “in response to identifying the information, and based on stored data that maps application flows with pseudowires, determining a plurality of pseudowires corresponding to paths through the MPLS network, wherein the stored data indicates, for a sending device application, a distributed mapping of the application flow via at least one of the plurality of pseudowires.” On information and belief, Ciena, through the Accused Instrumentalities, performs this step of the claimed method by operating, maintaining, and enabling others to

⁹⁹ https://www.blueplanet.com/_data/assets/pdf_file/0026/94670/understanding-bgp-peering-relationships-with-advanced-route-and-traffic-analysis.pdf (last visited October 14, 2024).

operate, utilize, or otherwise benefit from Ciena's Blue Planet Intelligent Automation Portfolio. For example, as shown in the figure below, Ciena discloses the use of a plurality of pseudowires in its implementation of Blue Planet.¹⁰⁰

Protected					
Protection role	NE	NE	Labels	Name	ID
Primary	5160_0054_e00301	87m_0061_e00301	11756, 17552	daDH_3	1551355032
	87m_0061_e00301	5142_0053_e00301	11330, 18538	daDH_4	1551355033
Backup	5160_0054_e00301	5160_0055_e00301	15578	daDH_5	1551355030

Unprotected					
NE	NE	Labels	Name	ID	Signaling
5142_0053_e00301	87m_0061_e00301	12623	daDH_1	1551355030	static
87m_0061_e00301	5160_0055_e00301	12126	daDH_2	1551355031	static

138. On information and belief, and as shown in the figure above (highlighted in red), the Blue Planet solution makes use of multiple pseudowires. The claim limitation “plurality of pseudowires corresponding to paths through the MPLS network” is satisfied as shown above (highlighted in purple). Further, Ciena discloses the nodes that make use of the plurality of pseudowires (highlighted in

¹⁰⁰ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/PacketInfrastructureMgmt.html (last visited October 23, 2023) (emphasis added). On information and belief, this document appears to be no longer available on Ciena's website.

green), and that pseudowires are associated with or “mapped to” specific services or certain customer data flows.¹⁰¹

139. As a further example, and as shown in the figure below, Ciena discloses that Blue Planet provisions services with different and multiple pseudowires.¹⁰² On information and belief, Ciena enables the selection of one or more LSP tunnels to carry traffic, which demonstrates a distributed mapping for every service that is provisioned.

Provision a three-point E-Line service with pseudowire protection

You can use the MCP REST API to provision an E-Line service with Pseudowire protection (for both single-segment and multi-segment Pseudowires), and select one or more specific LSP tunnels to carry the A-Z, A-Z', and Z-Z' routes.

This capability is also supported in cases where the LSP path includes linear Q-in-Q spurs.

Note: The example below shows the configuration of a three-point protected E-Line service; but with minor variations the same API call can be used to provision a conventional two-point E-Line service instead.

140. As a further example, and as shown in the figure below, Ciena discloses that Blue Planet uses stored data (e.g., update-able Table Maps) for pseudowire services and flows.¹⁰³

¹⁰¹ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/user-guide/PacketInfrastructureMgmt.html (last visited October 23, 2023) (“The Pseudowires tab displays the set of pseudowires, both protected and unprotected, that are associated with the service.”). On information and belief, this document appears to be no longer available on Ciena’s website.

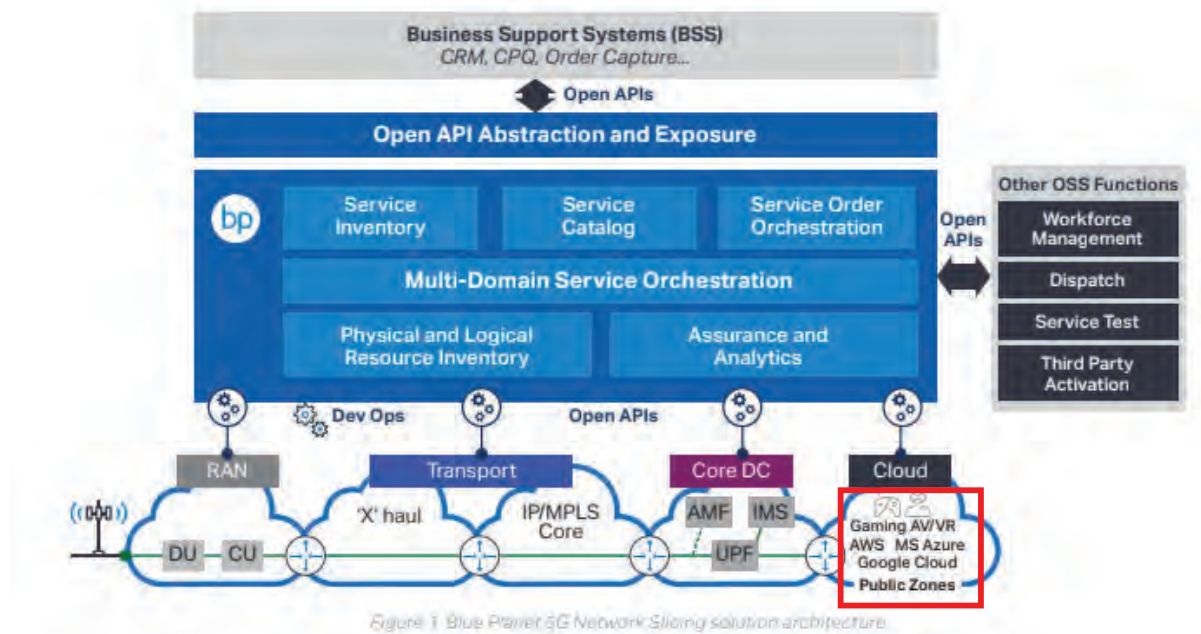
¹⁰² https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/PacketServiceMgmt.html (last visited October 30, 2023). On information and belief, this document appears to be no longer available on Ciena’s website.

¹⁰³ https://software.ciena.com/releasenotes/MCP-DOCS_5.2-217/build/site/mcp-docs/api-guide/PacketServiceMgmt.html (last visited October 30, 2023). On

Table Map Update

During PW-Handoff service create, if AN endpoint node is SAOS 6x then, on it's neighbouring AGN node, additional table map update CLI will be executed, to add PWHE peer IP in the prefix-list, when peer IP is not already there in prefix-list.

141. As a further example, and as shown in the figure below, Ciena discloses that Blue Planet may provision services for specific applications (e.g., gaming, VR, Google Cloud), which demonstrates that the services are provisioned for specific applications and/or for specific customers.¹⁰⁴



information and belief, this document appears to be no longer available on Ciena's website.

104

https://www.blueplanet.com/_data/assets/pdf_file/0021/81264/5G_Automation_Network_Slicing_SB1.pdf (last visited August 22, 2024) (emphasis added). On information and belief, the current version of this webpage has been edited to exclude the above graphic.

142. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1C] of the '320 Patent.

143. Limitation [1D] requires “communicating data related to the sending device application via at least one of the plurality of pseudowires.” On information and belief, Ciena, through the Accused Instrumentalities, performs this step of the claimed method by operating, maintaining, and enabling others to operate, utilize, or otherwise benefit from Ciena’s Blue Planet Intelligent Automation Portfolio. For example, and as shown in the figure below, Ciena documentation discloses that Blue Planet splits traffic into multiple transport paths (the TE tunnels), which demonstrates a distributed mapping of the service or application flow with multiple pseudowires through which data is communicated.¹⁰⁵

¹⁰⁵

https://www.blueplanet.com/_data/assets/pdf_file/0023/9257/Route_Optimization_and_Analysis_DS_4_2024.pdf (last visited October 14, 2024). Ciena advertises that Blue Planet “comput[es] and provision[s] transport paths to deploy new services.”

ROA leverages routing and traffic data to enable automation of service provisioning and assurance. Its IP/MPLS Automation module's built-in PCE can compute the best route from a source to destination and uses ROA's PCEP support to automatically provision a new RSVP-TE or segment mouting TE tunnel. The module also provides recommendations based on traffic matrices to identify congested links or links with the longest paths (most hops) to optimize. It then recommends new TE tunnels to split traffic and automatically provisions them, helping alleviate congestion.

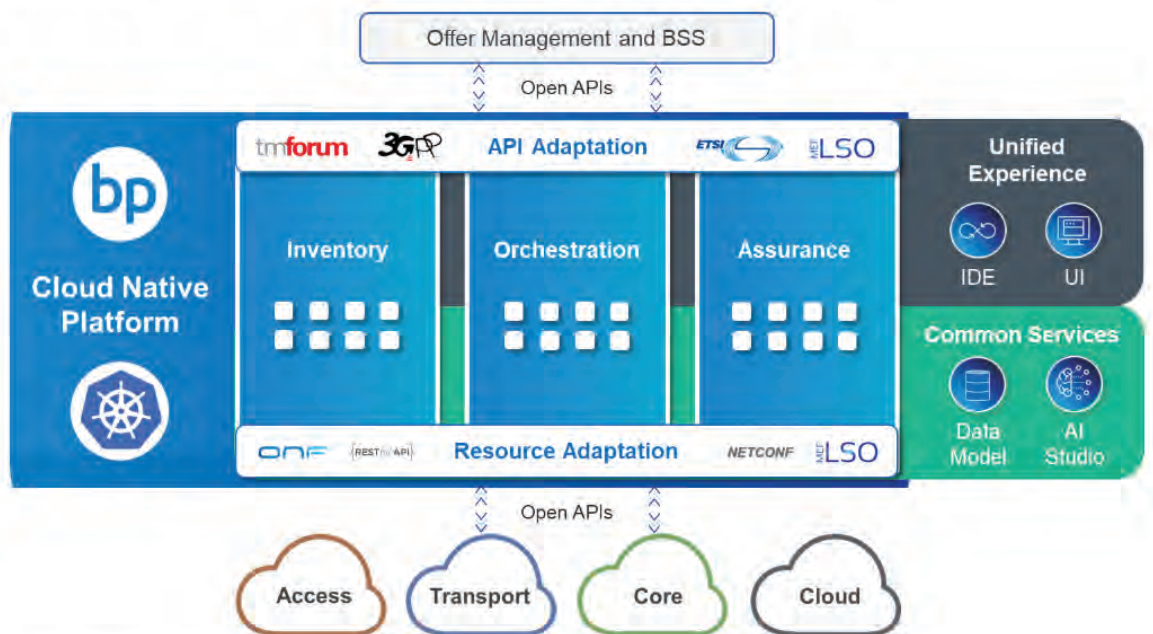
144. Accordingly, based on information and belief, and based upon publicly available information, Ciena, through its operation and/or maintenance of Blue Planet satisfies limitation [1D] of the '320 Patent.

145. Thus, Ciena's operation and maintenance of the Accused Instrumentalities satisfies each and every limitation of claim 1 of the '320 Patent.

146. On information and belief, Ciena has directly used the Accused Instrumentalities in Ciena data centers and has directly used the Accused Instrumentalities when setting up, running, troubleshooting, and/or operating the Accused Instrumentalities on behalf of itself or its customers. As evidenced by the non-limiting examples below, support for these statements is located throughout Ciena's websites.

147. On information and belief, the Accused Instrumentalities are used in data centers. For example, as shown below, Ciena advertises that its Blue Planet solution may be deployed “on premises, in any private or public cloud.”¹⁰⁶

Built on a ultra-modern Kubernetes-based architecture, the Blue Planet Cloud Native Platform (CNP) can be deployed on premises, in any private or public cloud—including AWS, Google, Microsoft and even in any multi-cloud mix of public and private clouds—with complete feature consistency. In addition to deployment flexibility, Blue Planet CNP also provides cloud-native support services that streamline the transition and ensure interoperability.



Blue Planet's Cloud Native Platform and applications

148. As a further example, as shown below, Ciena provides its customers with technical support for planning, deployment, and maintenance of its Blue Planet solution.

¹⁰⁶ <https://www.blueplanet.com/resources/what-is-cloud-native-oss> (last visited October 14, 2024).

149. On information and belief, and based on publicly available information, Ciena provides customers and/or potential customers of its Blue Planet solution with multiple sources of technical support. For example, Ciena provides “[a]ccess to software library including latest updates and new, innovative product features” as well as “Blue Planet expertise to assist with product use, configuration, and troubleshooting issues.”¹⁰⁷ On further information and belief, Ciena provides a customer forum where technical information about its products and/or services may be discussed by its personnel and customers.¹⁰⁸ On further information and belief, Ciena also provides a learning portal for its customers and potential customers to learn about the Accused Instrumentalities and their deployments and implementations.¹⁰⁹ On further information and belief, Ciena provides access to instructional and informational videos about its Accused Instrumentalities.¹¹⁰ On further information and belief, Ciena also provides a “DevOps Exchange” “[d]edicated to Blue Planet developers in a technical role” that “provides access to

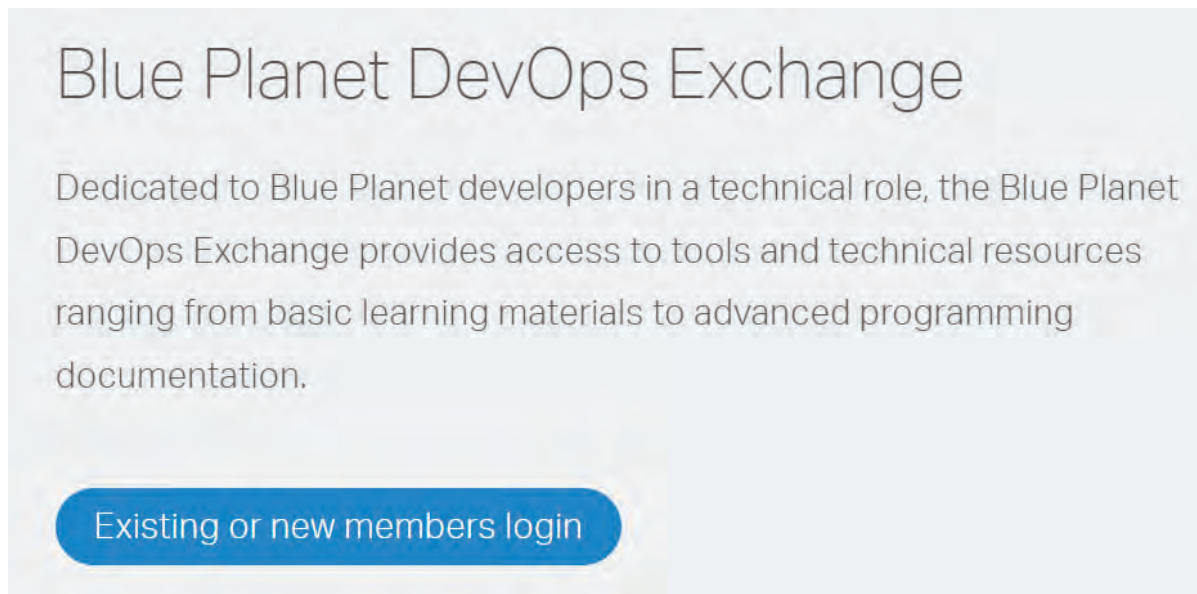
¹⁰⁷ <https://www.blueplanet.com/support/contacts> (last visited October 14, 2024) (providing domestic and international contact information for technical support).

¹⁰⁸ <https://my.ciena.com/CienaPortal/s/blue-planet> (last visited October 14, 2024).

¹⁰⁹ <https://www.blueplanet.com/learning> (last visited October 14, 2024).

¹¹⁰ <https://www.blueplanet.com/learning/blue-planet-overview> (last visited October 14, 2024).

tools and technical resources ranging from basic learning materials to advanced programming documentation.”¹¹¹



150. On information and belief, Ciena has and continues to advertise its partnerships with its customers internationally and in the United States.¹¹² For example, Ciena has touted its partnership with Consolidated Communications¹¹³,

¹¹¹ <https://www.blueplanet.com/learning/blue-planet-overview> (last visited October 14, 2024). On information and belief, login information to the DevOps exchange may be entered at https://developer.blueplanet.com/signin/?return_url=https://developer.blueplanet.com/index.html (last visited October 14, 2024).

¹¹² See, e.g., <https://www.blueplanet.com/about/press-releases> (last visited October 14, 2024) (listing various news articles regarding Ciena’s partnerships with customers).

¹¹³ On information and belief, Consolidated Communications is a third-party broadband provider and Ciena customer “serving customers across a 20-plus state

and its integration of the Blue Planet solution to “provide Consolidated Communications with next generation network automation and control by leveraging ... the multi-vendor Blue Market Multi-Domain Service Orchestration (MDSO) and Blue Planet Route Optimization and Analysis (ROA) software.”¹¹⁴ As another example, Ciena has and continues to advertise its business relationship with DISH Network Corporation: “Blue Planet is a key component within [DISH’s] 5G platform, allowing [DISH] to dynamically manage all of [its] network inventory and service order in real-time.”¹¹⁵

151. Ciena was not licensed or otherwise authorized by K.Mizra to make, use, import, sell, or offer to sell any products and/or services covered by the ’320 Patent, and Ciena’s conduct is, in every instance, without K.Mizra’s consent.

152. Ciena undertook the infringing actions despite an objectively high likelihood that such activities infringe the ’320 Patent, which has been duly issued by the USPTO and presumed valid.

service area.” See <https://www.consolidated.com/about-us> (last visited October 14, 2024).

¹¹⁴ <https://www.blueplanet.com/about/press-releases/consolidated-communications-builds-5g-ready-network-with-cienas-adaptive-ip-solution.html> (last visited October 14, 2024).

¹¹⁵ <https://www.blueplanet.com/about/press-releases/dish-selects-blue-planet-automation-software-to-accelerate-5g-services.html> (last visited October 14, 2024).

153. Since at least the date of first learning of the '320 Patent, which is no later than the date of the Notice Letters as detailed herein, Ciena has continued its infringing activities. As such, Ciena has willfully infringed the '320 Patent.

154. Since at least the date of first learning of the '320 Patent, which is no later than the date of the Notice Letters as detailed herein, Ciena has also indirectly infringed and continues to indirectly infringe the '320 Patent in violation of 35 U.S.C. § 271(b). Ciena has actively induced, for example, network service providers such as Consolidated Communications and/or DISH to directly infringe the '320 Patent by performing the method of claim 1 as detailed above throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Instrumentalities in various websites, including providing and disseminating product descriptions, operating manuals, technical documentation, instructional and/or informational videos, and other instructions on how to implement the Accused Instrumentalities. Examples of such advertising, promotion, and/or instruction include without limitation the documents cited in the paragraphs above. Ciena did so knowing and intending that its customers and end users commit these infringing acts, despite its knowledge of the '320 Patent, thereby specifically intending for and inducing its customers to infringe the '320 Patent through the customers' normal and customary use of the Accused Instrumentalities.

155. As a result of Ciena's infringement of the '320 Patent, K.Mizra has suffered substantial injury and is entitled to recover all damages caused by Ciena's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Cisco's wrongful conduct, but in no event less than a reasonable royalty as provided for in 35 U.S.C. § 284.

COMPLIANCE WITH 35 U.S.C. § 287

156. K.Mizra has never manufactured or sold a product.

157. On information and belief, at no point in time before Ciena was put on actual notice via K.Mizra's February 2024 Notice Letters did K.Mizra have any licensee to any of the Patents-in-Suit that manufactured or sold a product that practices any of the Patents-in-Suit.

158. On information and belief, at no point in time did Global Innovation Aggregators LLC ever manufacture or sell a product, or have any licensee to any of the Patents-in-Suit that manufactured or sold a product that practices any of the Patents-in-Suit.

159. On information and belief, at no point in time did Brixham Solutions Ltd. ever manufacture or sell a product, or have any licensee to any of the Patents-in-Suit that manufactured or sold a product that practices any of the Patents-in-Suit.

160. Hammerhead Systems, Inc. ceased to do business in approximately 2009, and approximately five years before the first of the Patents-in-Suit issued from the USPTO.

DEMAND FOR JURY TRIAL

K.Mizra LLC respectfully requests a trial by jury of all triable issues.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff K.Mizra LLC respectfully requests that the Court enter judgment in its favor against Defendant Ciena Corporation, granting the following relief:

- A. That the Court enter judgment for K.Mizra on all causes of action asserted in this Complaint;
- B. That the Court enter judgment in favor of K.Mizra and against Ciena for monetary damages to compensate it for Ciena's infringement of the Patents-in-Suit pursuant to 35 U.S.C. § 284, including costs and pre and post-judgment interest as allowed by law;
- C. That the Court enter judgment in favor of K.Mizra and against Ciena for accounting and/or supplemental damages for all damages occurring after any discovery cutoff and through the Court's entry of final judgment;

- D. That the Court adjudge Ciena's infringement of the Patents-in-Suit to be willful dated from February 13, 2024 when Ciena was put on actual notice of infringement of the Patents-in-Suit;
- E. That the Court enter judgment that this case is exceptional under 35 U.S.C. § 285 and enter an award to K.Mizra of its costs and attorneys' fees; and
- F. That the Court award K.Mizra all further relief as the Court deems just and proper.

Dated: November 25, 2024

Respectfully submitted,

/s/ Scott P. Amy

Scott P. Amy, GA Bar No. 141416

PERILLA KNOX &

HILDEBRANDT LLP

5871 Glenridge Drive, Suite 350

Atlanta, GA 30328

Tel: (770) 927-7802

Fax: (877) 389-6779

s.amy@pkhip.com

Timothy Dewberry, GA Bar No. 114643

FOLIO LAW GROUP PLLC

13492 Research Blvd.,

Suite 120, No. 177

Austin, TX 78750

Tel: (737) 234-0201

timothy.dewberry@foliolaw.com

Counsel for Plaintiff K.Mizra LLC

EXHIBIT A



US008782282B1

(12) **United States Patent**
Zhou et al.

(10) **Patent No.:** **US 8,782,282 B1**

(45) **Date of Patent:** **Jul. 15, 2014**

(54) **NETWORK MANAGEMENT SYSTEM**

(56) **References Cited**

(75) Inventors: **Eileen Zhou**, San Jose, CA (US); **Roger Liu**, San Jose, CA (US); **Vijoy Choyi**, Santa Clara, CA (US); **Moshe Itah**, Palo Alto, CA (US); **John Z. Yu**, Santa Clara, CA (US)

(73) Assignee: **Brixham Solutions Ltd.**, Tortola (VG)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 2172 days.

(21) Appl. No.: **10/742,573**

(22) Filed: **Dec. 19, 2003**

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/246; 709/203; 719/320**

(58) **Field of Classification Search**
USPC **709/203, 246; 719/320**
See application file for complete search history.

U.S. PATENT DOCUMENTS

5,812,768 A *	9/1998	Page et al.	709/228
7,111,077 B1 *	9/2006	Starkovich et al.	709/246
7,325,062 B2 *	1/2008	Hamilton et al.	709/226
2003/0093403 A1 *	5/2003	Upton	707/1
2003/0177240 A1 *	9/2003	Gulko et al.	709/226
2004/0040030 A1 *	2/2004	Fenton et al.	719/320
2004/0107277 A1 *	6/2004	Levesque et al.	709/223
2004/0249644 A1 *	12/2004	Schiefer et al.	705/1
2005/0108387 A1 *	5/2005	Li et al.	709/224

* cited by examiner

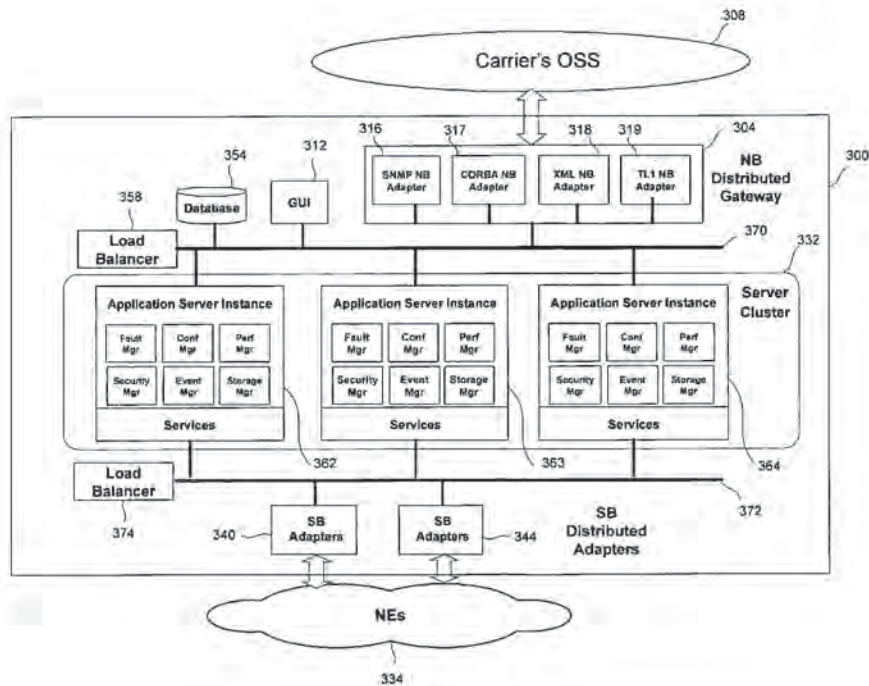
Primary Examiner — Glenford Madamba

(74) *Attorney, Agent, or Firm* — Amin, Turcoy & Watson, LLP

(57) **ABSTRACT**

A technique for communicating in a network management system is disclosed. The technique includes transferring information from an application server to a gateway that processes the information, transferring the gateway processed information from the gateway to a plurality of adapters associated with the gateway that process the gateway processed information, and transferring the adapter processed information from one of the adapters to a client.

22 Claims, 6 Drawing Sheets



NB distributed gateway, SB distributed adapters, server cluster, & load balancers

U.S. Patent

Jul. 15, 2014

Sheet 1 of 6

US 8,782,282 B1

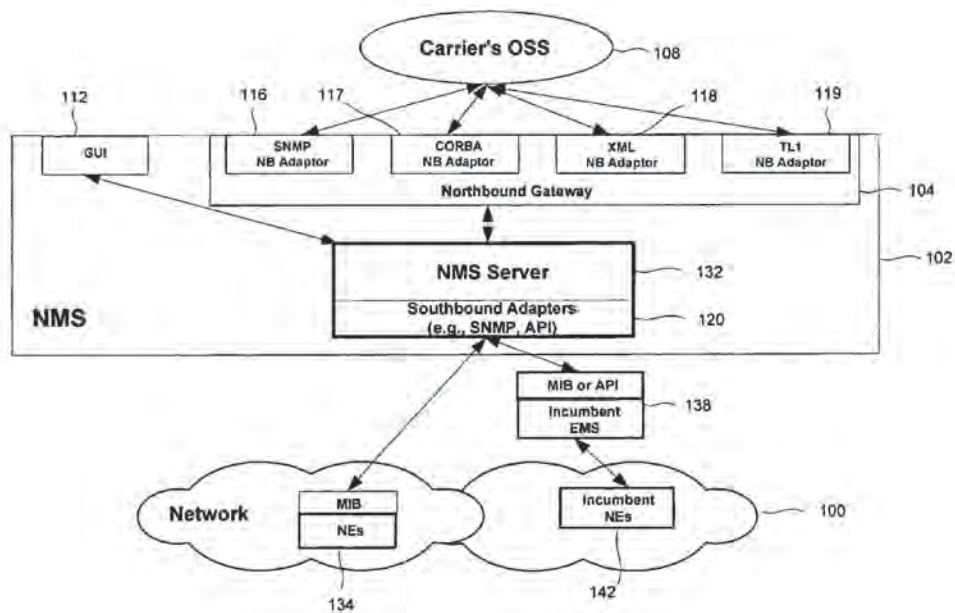


FIG. 1: An overall network management view

U.S. Patent

Jul. 15, 2014

Sheet 2 of 6

US 8,782,282 B1

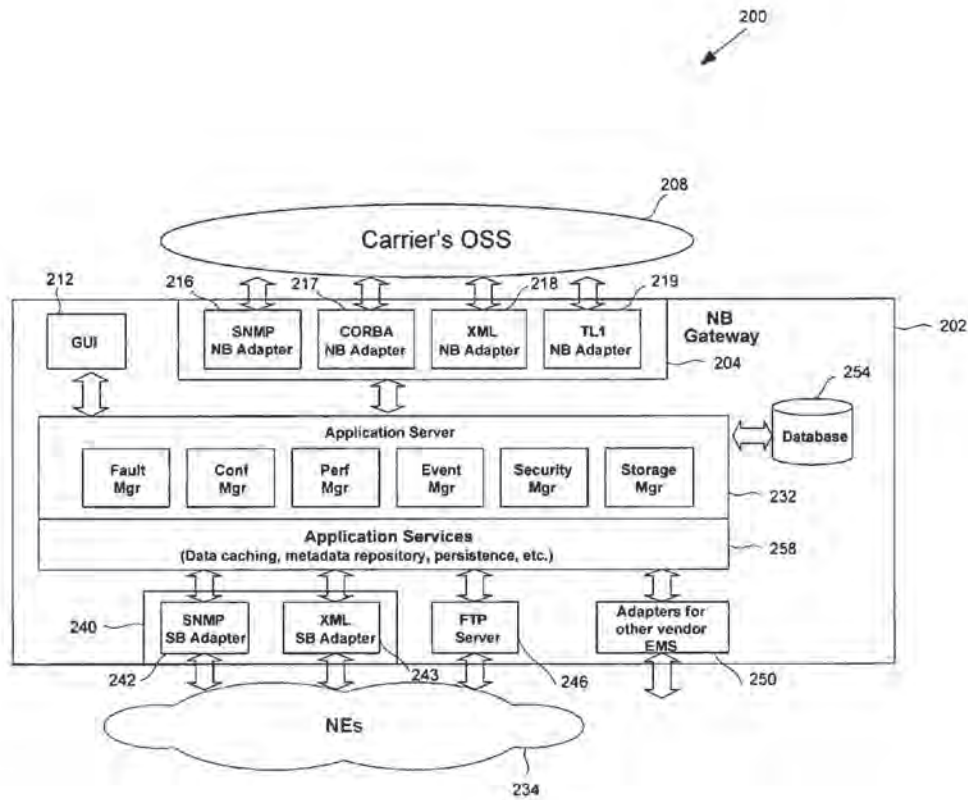


FIG. 2: NMS functional block diagram

U.S. Patent

Jul. 15, 2014

Sheet 3 of 6

US 8,782,282 B1

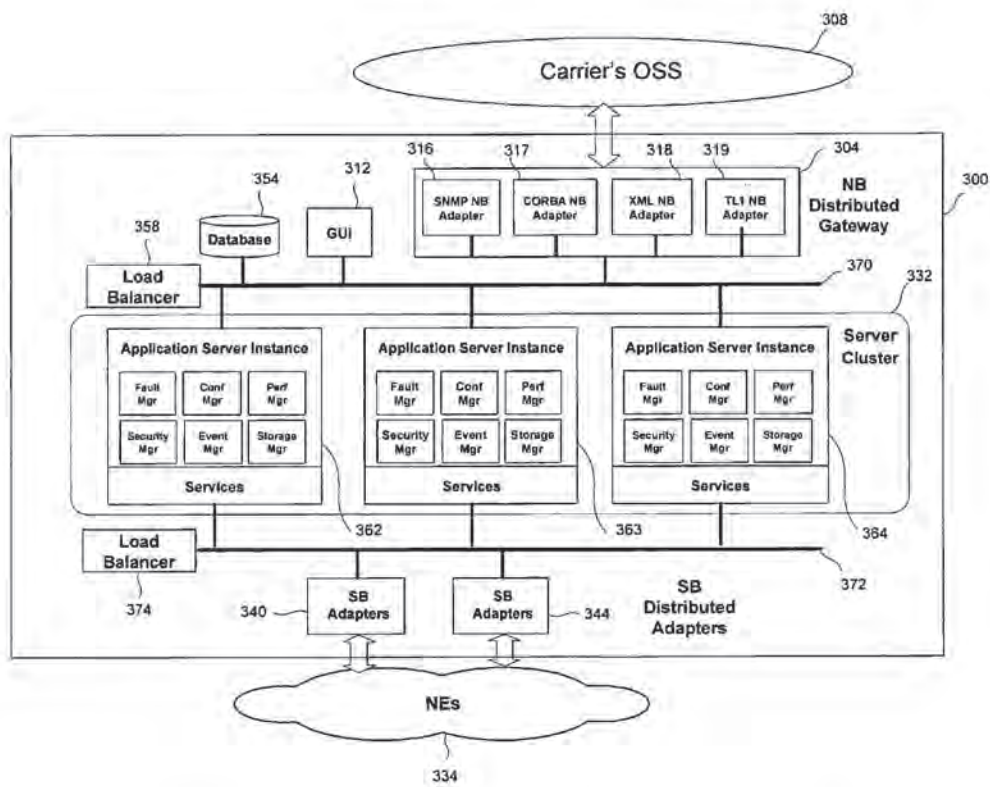


FIG. 3A: NB distributed gateway, SB distributed adapters, server cluster, & load balancers

U.S. Patent

Jul. 15, 2014

Sheet 4 of 6

US 8,782,282 B1

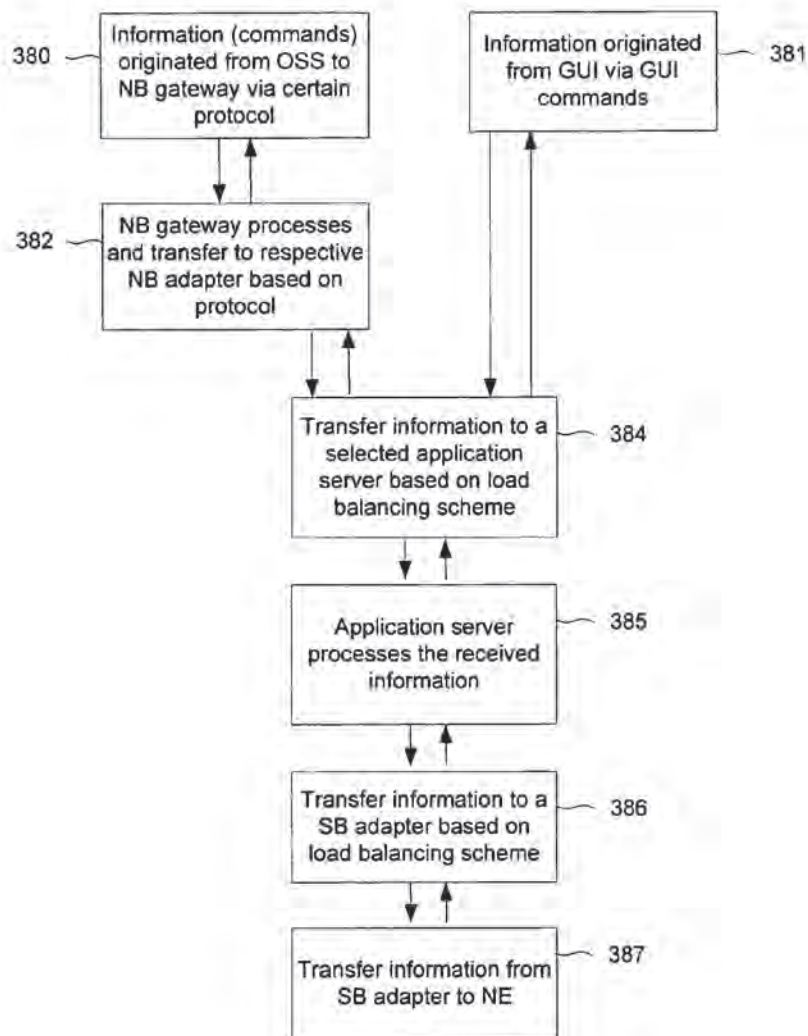


FIG. 3B: Downlink information flow (OSS or GUI as originator)

U.S. Patent

Jul. 15, 2014

Sheet 5 of 6

US 8,782,282 B1

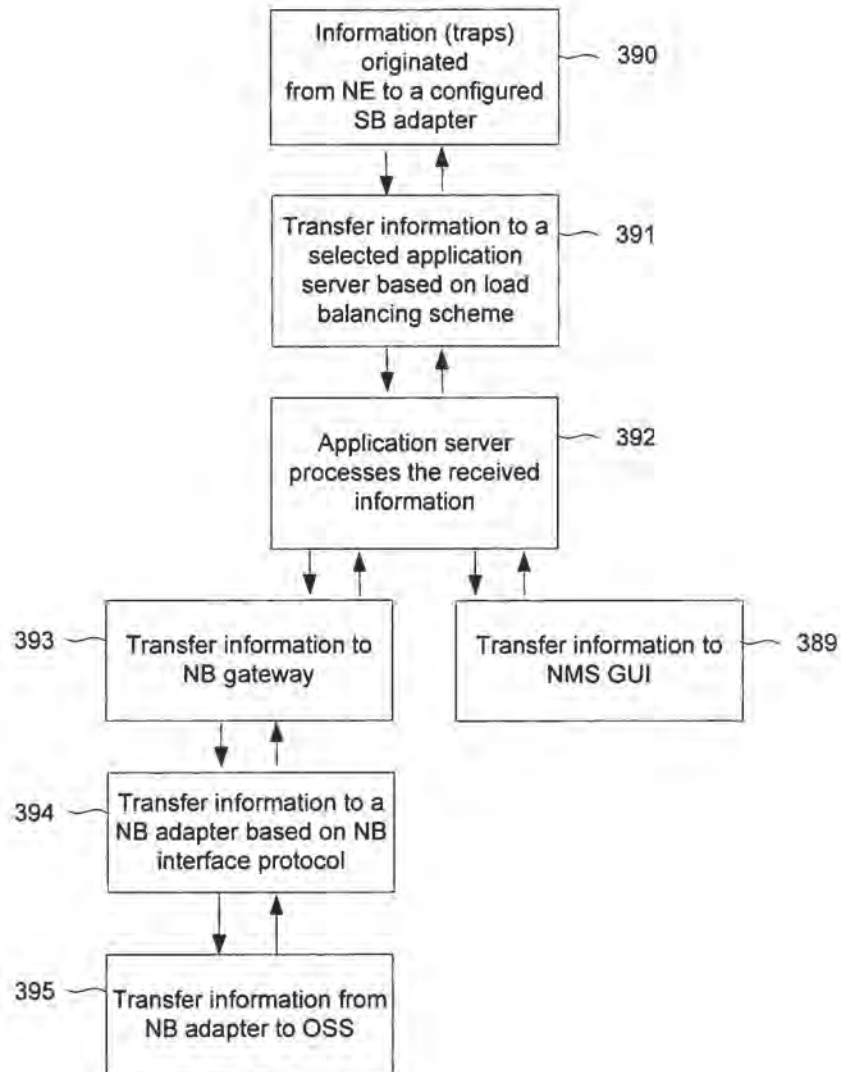


FIG. 3C: Uplink information flow (NE as originator)

U.S. Patent

Jul. 15, 2014

Sheet 6 of 6

US 8,782,282 B1

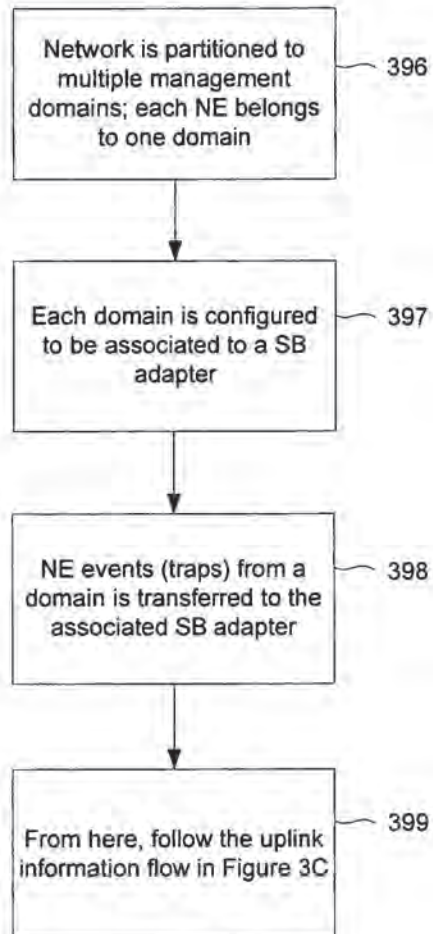


FIG. 3D: Uplink information flow with network partitioning

US 8,782,282 B1

1

NETWORK MANAGEMENT SYSTEM

FIELD OF THE INVENTION

The present invention relates generally to communications networks. More specifically, a network management system is disclosed.

BACKGROUND OF THE INVENTION

Network management systems (NMS) facilitate the exchange of management information between Network Elements (NEs) and network administrators' Operations Support Systems (OSS). Network administrators can use an NMS to install and configure NEs, provision services, manage network performance, find and solve network problems, and plan for network growth. Network management systems today face many challenges as networks grow in size. Network management systems need to be scalable. For example, thousands of events can be generated when a fault is discovered at a network element. In a large network, a network management system can easily be overwhelmed. It would be desirable to develop a network management system that is robust, scalable, and capable of efficiently handling a growing network.

BRIEF DESCRIPTION OF THE DRAWINGS

Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

FIG. 1 is an overall view of a carrier's OSS 108, an NMS 102, and a network 100 including NEs 134 and 142.

FIG. 2 is a functional block diagram illustrating a network management system 202 in a network 200.

FIG. 3A is a diagram illustrating NMS 300 using application server cluster and load balancing between NB gateway (adapters) and NMS server instances, and between SB adapters and NMS server instances.

FIG. 3B is a flowchart illustrating a downlink information flow in which OSS 308 or NMS GUI 312 is the originator of the information while NE 334 or application server (362, or 363, or 364) is the recipient of the information.

FIG. 3C is a flowchart illustrating an information flow in which NE 334 is the originator of the information while OSS 308 or NMS GUI 312 is the recipient of the information.

FIG. 3D is a flowchart illustrating a technique for transferring information (e.g., traps) from an NE in a partitioned network to server cluster 332.

DETAILED DESCRIPTION

The invention can be implemented in numerous ways, including as a process, an apparatus, a system, a composition of matter, a computer readable medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or electronic communication links. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention.

A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the

2

invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

A scalable network management system (NMS) is disclosed. In some embodiments, the NMS includes a so-called northbound (NB) gateway, which includes various NB adapters, to facilitate transferring and translating information between the NMS server, or servers in a server cluster and an OSS from the network administrator, or carrier. The NB gateway design may be distributed so that multiple NB gateways, each of which includes a certain number of NB adapters, can be logically or physically distributed over different workstations. Information transferred from the gateway to the server cluster can be distributed among servers within the server cluster based on a load balancing scheme, to best utilize the NMS server's processing power. In the direction from NE to NMS (uplink), the managed network can be partitioned by configuring for each Network Element (NE) a so-called southbound (SB) adapter to handle information (or events) originating from that NE. SB adapters may be distributed so that SB adapters can be logically or physically distributed over different workstations. A load balancing scheme may be used to associate a SB adapter to a particular server or servers for processing power efficiency. In the direction from NMS to NE, the load balancing scheme may be used to distribute information from the NMS to a selected SB adapter to reach the destined NE.

FIG. 1 is an overall view of a carrier's OSS 108, an NMS 102, and a network 100 including NEs 134 and 142. An NMS refers to a system responsible for managing a network, and facilitates the communication between a carrier's OSS and NEs in the network. In the embodiment illustrated, incumbent element management system (EMS) 138, and incumbent NEs 142 refer to the existing management system and NEs, while NEs 134 refer to the newly introduced NEs for existing network growth. NMS 102 may be used to manage the existing NEs (via existing EMS 138) and newly introduced NEs. A carrier may operate an OSS over the NMS to manage the entire network to provide services through the growing network. An NE, as used herein, includes any device or node on the network, such as a network switch. GUI 112 and NB gateway 104 are connected to NMS server 132 as clients. NB gateway 104 can be physically and logically separated from the NMS server. The NMS server may include a service cluster which includes multiple service instances. NB gateway 104 includes multiple NB adapters to process information to facilitate communications between NMS and OSS using different types of protocols. More specifically, NB gateway may include Simple Network Management Protocol (SNMP) NB adapter 116, Common Object Request Broker Architecture (CORBA) NB adapter 117, Extensible Markup Language (XML) NB adapter 118, and Transaction Language 1 (TL1) NB adapter 119.

NB devices, such as northbound adapters, include client side devices or network elements or devices that process information between an OSS and an NMS server. SB devices, such as SB adapter and API 120, process information to facilitate communication between the NMS server and NEs, or between the NMS server and incumbent EMS 138. North-

US 8,782,282 B1

3

bound information includes information that travels in the direction from a network element to an OSS. Southbound information includes information that travels in the direction from an OSS to a network element.

NMS server 132 is connected to an MIB (Management Information Base) running on NEs 134 via SB SNMP/MIB adapter 120. NMS server 132 is also connected to a MIB associated with incumbent EMS 138 via SB SNMP/MIB adapter 120. NMS server 132 is also connected to an application program interface (API) associated with incumbent EMS 138 via API adapter 120. Incumbent EMS 138 is connected to incumbent NEs 142.

NMS 102 is shown to manage both NEs 134 and incumbent NEs 142. NMS 102 can manage incumbent NEs 142 by communicating with incumbent EMS 138. In general, NMS 102 can assume management of any incumbent network by connecting to an EMS associated with the incumbent network.

NMS server 132 communicates with adapters 116-119 via NB gateway 104. Adapters 116-119 are software modules on NB gateway 104. Accordingly, processing of common functions between adapters 116-119 can be shared. For example, an event sent from an NE to more than one NB adapter can be sent as one event to the NB gateway. Gateway 104 then processes the event and distributes the information appropriately to each NB adapter.

NMS 102 communicates in various protocols in different embodiments. For example:

The SNMP protocol is used on its downlink (southbound) to communicate with switches or NEs. Command line interface (CLI) access to NEs through Telnet is also provided through the NMS in a cut-through mode;

The SNMP protocol or a proprietary API is used on its downlink (southbound) to communicate with existing EMS managing incumbent NEs in installed networks; XML, CORBA, TLI, and SNMP protocols are used on its uplink (northbound) to communicate with external carriers' OSS's and NMS's.

In some embodiments, most of the time OSS 108 accesses NMS 102 for information and operation support. At other times, OSS 108 directly accesses NEs 134 or NEs 142 using the SNMP protocol. In some embodiments, hundreds or thousands of NEs are managed by an NMS. At the same time, an NE can be managed by multiple NMS's.

FIG. 2 is a functional block diagram illustrating a network management system 202 in a network 200. Network 200 includes OSS 208, NMS 202 and NEs 234. NMS 202 includes NB gateway 204, GUI 212, application server 232, NMS database 254, SB adapters 240, file transfer protocol (FTP) server 246, and adapter 250 to communicate with external (incumbent) EMS's. NB gateway 204 includes SNMP adapter 216, CORBA adapter 217, XML adapter 218, and TLI adapter 219.

OSS 208 is connected to adapters 216-219. GUI 212, NB gateway 204, and database 254 are connected to application server 232. NB gateway 204, application server 232, GUI 212, database 254, SB adapters 240, FTP server 246, and adapter 250 can be configured as physically or logically separate elements. For example, SB adapters 240, FTP server 246, or adapter 250 may be included on the same physical machine as server 232. Application server 232 is connected to NEs 234 via SB adapters 240. Application server 232 is also connected to adapter 250 and FTP server 246, which is connected to NEs 234. Application server 232 may include multiple independent application servers to form a server cluster. A load balancing scheme may be designed to associate NB adapters

4

with application servers, and to associate SB adapters with application servers, an embodiment discussed further in conjunction with FIG. 3.

NB gateway 204 relays management information and operations between server 232 and an external OSS 208. Information includes data, messages, events, or other information that can be communicated in NMS 202. For example, NB gateway 204 can provide network topology and configuration retrieval and provisioning services, and facilitate the integration with OSS 208 for fault management and flow through provisioning. External OSS 208 can communicate with NB gateway 204 via the SNMP, TLI, CORBA or XML protocol as NB interfaces. In some embodiments, NB gateway 204 includes a protocol adapter for each type of protocol, to convert messages of a specific protocol into a common message type, and vice versa. The common message type may be a proprietary message type. NB gateway 204 can communicate with server 232 through RMI interfaces. With NB gateway 232, many functions, such as trap detector/listener, can be efficiently designed to support all NB interfaces with various protocols.

Information is transferred from application server 232 to NB gateway 204 which processes and distributes the information appropriately to adapters 216-219. Processes common to adapters 216-219 can be performed prior to transferring the information to adapters 216-219. NB gateway 204 may include multiple NB gateways, each of which includes a set of NB adapters. The information is then transferred from adapters 216-219 to OSS 208 (292).

Adapters include software modules which can be standalone Java services that run on separate Java Virtual Machines (JVM). The modules can connect to an external system using various protocols and connect back to NMS server 232 via an RMI interface. NMS 202 is shown to include SNMP, CORBA, XML, and TLI NB adapters. NMS 202 can include any number of NB adapters each associated with any protocol. The following are examples of NB adapter communication within network 200.

SNMP NB adapter 216 is the SNMP interface between external OSS 208 and NMS 202. NMS 202 acts as an SNMP agent. In some embodiments, OSS 208 sends SNMP Set, Get, and GetBulk commands to SNMP NB adapter 216. SNMP NB adapter 216 translates the messages into native Java messages and sends them to application server 232. Application server 232 executes the commands and returns the responses to SNMP NB adapter 216. SNMP NB adapter 216 then converts the responses into SNMP messages and sends the messages back to external OSS 208.

An OSS that wishes to receive traps from NMS 202 can register itself through SNMP NB adapter 216 via the SNMP Set command. SNMP NB adapter 216 will then forward trap messages from application server 232 to the registered OSS. SNMP NB adapter 216 can also translate traps from SNMP v1 format to SNMP v2 format, and vice versa.

XML NB adapter 218 communicates with an external system using XML data. XML NB adapter 218 converts an XML message to a native Java message, and vice versa. In some embodiments, XML NB adapter 218 includes two adapters: XML command adapter and XML event adapter.

The XML command adapter receives a command from application server 232 and converts it to XML data. Then it creates a TCP/IP socket connection with the corresponding external system, and sends the XML data to the external system over the output stream of the connection. The XML command adapter then waits for the response on the input

US 8,782,282 B1

5

stream of the connection. It converts XML data received in response to java.util.Map and returns this map to the invoker of the command.

Application managers that wish to receive events from external systems can register with the XML event adapter. The XML event adapter receives XML messages from external systems over a TCP/IP socket connection and translates the messages into name value maps. The XML event adapter then sends the name value maps to each registered application manager.

TL1 NB adapter 219 communicates with an external system using the TL1 protocol. The TL1 NB adapter converts TL1 commands and autonomous messages to a native Java message, and vice versa.

CORBA NB adapter 217 provides a CORBA interface to external OSS's. CORBA NB adapter 217 receives CORBA requests from external OSS's, translates the requests into a Java native message format and sends the messages to application server 232. Application server 232 performs the requested operations and sends the response back to CORBA NB adapter 217. CORBA NB adapter 217 then translates the response into CORBA messages and sends them to the invoking external OSS.

Application server 232 includes support for various management services, including the typical carrier-class fault-management, configuration, accounting, performance, and security (FCAPS) functions via Configuration Manager, Fault Manager, Performance Manager, Event Log Manager and Security Manager. For example:

Configuration Manager: A configuration manager is responsible for providing configuration services, including discovering, configuring, and provisioning managed NEs in the network. It provides support for defining and manipulating configuration of network physical inventory, facilities, and connections. It also supports the diagnostic testing of the network elements.

Fault Manager: A fault manager is responsible for monitoring fault conditions and notifying the OSS and other management systems. It collects fault notifications from NEs, analyzes the notifications, and communicates the appropriate information to the OSS and other management systems.

Performance Manager: A performance manager allows users to proactively manage the network's health and performance. At a high level, the Performance Manager can be divided into two functions: collecting performance data from NEs, and presenting performance information to a GUI client or other NB performance monitoring (PM) systems. PM data collectors can collect performance data from NEs using various collection schemes and protocols, then either store the data in an NMS database or directly pass the data to requesting parties, such as a GUI client or an NB third party PM system.

Event Log Manager: An event log manager collects and records various events from the network. Some examples of an event include an SNMP trap from an NE, periodic performance monitoring (PM) data from an NE, an alarm from an NE or other network device, a security audit log from a server, an SNMP command sent from the NMS to an NE, and the NMS shutting down. The event log manager is both an event recorder and an event publisher.

Security Manager: A security manager is a service manager that maintains information about users and their access rights to operations and system resources. It is also responsible for security auditing.

6

Storage Manager: A storage manager is responsible for managing NMS storage database tables and alarms/events files.

In some embodiments, NMS 202 follows a typical Java 2 Platform Enterprise Edition (J2EE)-based three-tier distributed model: a Java GUI front end tier, a J2EE Application Server tier, and a database tier which can be any Java Database Connectivity (JDBC) compliant database. Other distribution models and protocols are used in various other embodiments. Specifically, the server tier may include a set of backend server modules running in a J2EE Application Server environment, which provide the actual execution of the management functionality. In this embodiment, a complete server configuration includes a J2EE application server 232 with all the Enterprise Java Beans (EJB) running on it, a set of SB protocol adapters 240, an integrated FTP server 246, and a data services layer 258 which provides caching, meta-data repository, and data persistency services.

All NMS management services, such as configuration management, fault management, performance management, security management, event management, and other operation support functionality, may be implemented as EJB or as remote method invocation (RMI) Objects working in conjunction with EJBs. The adapters can run on a separate JVM and communicate back to the EJBs or RMI servers via RMI interfaces. The application server can communicate with external systems using various protocols, including SNMP, CORBA, XML, TL1, and other proprietary interfaces. The FTP server can facilitate large data transfers between the NMS and other external systems.

NMS applications can be implemented as J2EE applications. Bean managed data persistency can be used to overcome the limitation of the default J2EE container managed persistency design, which might be more suitable for e-commerce applications than for OSS/NMS types of application.

NMS 202 is shown to include SNMP and XML SB adapters each associated with any protocol. The following are examples of SB adapters used for communicating with the network 234.

SNMP SB adapter 242 supports communication between application server 232 and SNMP agents running on NEs in network 234. For example, a trap may be sent from an NE to application server 232. In some embodiments, communication between SNMP SB adapter 242 and application server 232 is implemented using Java RMI. SNMP SB adapter 242 actually can include two adapters: SNMP command adapter and SNMP trap adapter. SNMP command adapter is an adapter that communicates using SNMP. It can be used to send SNMP commands such as SNMP Get, Set, GetNext, GetBulk from application server 232 to the agent running on each NE and return responses to application server 232. The SNMP trap adapter receives traps from SNMP agents, converts them into native Java messages and sends the messages to application server 232. The SNMP trap adapter may also be responsible for synchronizing the traps between NMS 202 and all the managed NEs. The trap synchronization process can either be initiated by the configuration manager or by the trap adapter itself. In some embodiments, each trap from a node contains a trap sequence number. The trap adapter uses this sequence number to ensure that it receives all the traps from all the managed NEs. If the trap adapter detects that traps are missing from a node, it may perform appropriate trap synchronization operations depending on the amount of missing traps.

In some embodiments, if a few traps are missed, the trap adapter requests the node to replay the missing traps. If a large

US 8,782,282 B1

7

number of traps are missed, it requests the node to save the missing traps into an event log file and ftp the file over. If too many traps are detected missing and it is infeasible to retrieve all the missing traps, the trap adapter gives up retrieving missing traps, and asks the node to save currently active alarms into an active alarm log file and FTP the file over. In the meantime, the trap adapter will notify the configuration manager to start the configuration check process.

In some embodiments, the trap adapter parses and processes active alarm log files and event log files from NEs in network 234. The active alarm log files and event log files contain the protocol description units (PDU) of the traps from the NE. The SNMP trap adapter extracts each PDU, converts it into a name value map, and then sends the name value map to all the registered application managers.

XML SB adapter 243 communicates with NEs in network 234 using XML data. XML SB adapter 243 converts an XML message to a native Java message, and vice versa.

NMS 202 may also include SB adapter 250 to communicate with another vendor's EMS through standard SNMP or any mutually agreed proprietary API. For example, a mutually agreed proprietary API may be based on proprietary information the other vendor uses for service provisioning, such as proprietary MIB tables or proprietary API functional calls. Accordingly, a carrier can perform end-to-end service provisioning across different vendors' NEs for network expansion. A new vendor's NEs can be inserted to a carrier's installed network with minimal interruption for end-to-end service deployment.

In some embodiments, NMS 202 includes an internal FTP server 246. FTP server 246 provides file transfer functionality between NMS 202 and external systems. In one embodiment, application managers or adapters that expect to transfer files to or from an external system register with FTP server 246 and provide FTP server 246 with a callback interface. Upon successful registration, FTP server 246 returns a unique, one-time-use username and password to the requester. The requester then sends the username and password to the external system. The external system can then use the received username and password to connect to FTP server 246 and start a file transfer. After the file transfer is completed, FTP server 246 invokes a corresponding callback function.

FIG. 3A is a diagram illustrating NMS 300 using application server cluster and load balancing between NB gateway (adapters) and NMS server instances, and between SB adapters and NMS server instances. NMS 300 includes NB gateway 304, GUI 312, server cluster 332, database 354, SB adapters 340 and 344, load balancer 358 (with shared bus 370) between NB gateway and NMS server cluster, and load balancer 374 (with shared bus 372) between SB adapters and NMS server cluster. The carrier's OSS may be connected to NB adapters via NB gateway 304. NB gateway 304 includes SNMP adapter 316, CORBA adapter 317, XML adapter 318, and TL1 adapter 319. NMS 300 communicates with NEs 334 via SB adapters 340 and 344.

GUI 312, NB gateway 304, and database 254 are connected to server cluster 332 via bus 370 controlled by the load balancer 358. Server cluster 332 is connected to SB adapters 340 and 344 via bus 372 controlled by the load balancer 374.

Service cluster 332 and load balancers 358 and 374 are introduced for managing large or expanding networks. Server cluster 332 includes NMS servers 362-364. Server cluster 332 may include any number of servers, or server modules (or instances). NMS 300 is dynamic and scalable as the network grows. High scalability is facilitated by using server clustering and distributed adapter architecture, with the load balancing scheme to connect the server cluster and NB and SB

8

adapters in northbound and southbound directions respectively. Note that the clustering of server modules and distribution of adapter modules can be completely transparent to the GUI client. A GUI client can still view the whole network topology without knowledge of the existence of multiple servers and adapters.

Servers 362-364 may be separate physical or logical server modules, or a combination of physically or logically separated server modules. In some embodiments, NMS 300 uses J2EE application server architecture in which each server may be an independent server instance in a J2EE application server. Accordingly, multiple instances of such application servers can run simultaneously to distribute a workload and protect each other. Each server instance by itself is a complete functioning NMS server that runs independently, and can be run on separate physical machines. Each server instance can be run on the same physical machine or distributed among several physical machines. These NMS server instances work together, forming the "server cluster".

Specifically, each server instance can be associated with the following software modules: GUI 312 and NB gateway 304 via load balancer 358 in the northbound direction, and SB adapters 340 and 344 via load balancer 374 in southbound direction. In some embodiments, there are multiple NB gateways, each of which includes a set of NB adapters performing a specific set of functions. Additional physically or logically separate NB gateways can be added as the network grows. When a first request comes from a functional entity, such as NB gateway, or GUI, or database, load balancer 358 is consulted to locate a server instance according to an algorithm based on certain criterions (e.g., selecting the lightest loaded server at that time), and then communication is established between the functional entity and the selected server instance. Similarly, when a first request comes from a service instance going southbound, the load balancer 374 is consulted to locate a SB adapter according to a method based on certain criteria, and then the communication is established between the server instance and the selected SB adapter.

FIG. 3B is a flowchart illustrating a downlink information flow in which OSS 308 or NMS GUI 312 is the originator of the information while NE 334 or application server (362, or 363, or 364) is the recipient of the information. When the information is originated from OSS (380), it is transferred via a certain protocol (e.g., SNMP, CORBA, XML, or TL1) to NB gateway 304. The NB gateway processes the information and then transfers it to an associated NB adapter based on the received protocol type (382). Alternatively, the information could be originated from GUI 312 where, for example, a user could enter a command on GUI 312 (381). The arriving information is then transferred to a selected server or servers according to load balancer 358 (384). Load balancer 358 may be a software module physically located on any device in NMS 300. Load balancer 358 may use any load balancing algorithm that is appropriate. For example, load balancer 358 may use a round robin scheme, or distribute the load based on CPU usage on each server or servers. In some embodiments, from then on, all information from NB gateway 304 (or GUI 312) is passed to the selected server for processing (385). Alternatively, the selected server may convert the format of the received information to a new format at particular times. The information is then transferred from the server to a selected SB adapter according to load balancer 374 (386). Load balancer 374 may use any load balancing algorithm that is appropriate. The information is then transferred from the SB adapter to the destined NE in network 334 (387). The response from the NE or NMS server follows the reverse information flow to the OSS or GUI.

US 8,782,282 B1

9

FIG. 3C is a flowchart illustrating an information flow in which NE 334 is the originator of the information while OSS 308 or NMS GUI 312 is the recipient of the information. Management information (e.g., traps/alarms) is originated from an NE in network 334 (390). The information is transferred to a pre-configured SB adapter. The arriving information at the SB adapter is then transferred to a selected server or servers according to load balancer 374 (391). Load balancer 374 may be a software module physically located on any device in NMS 300. Load balancer 374 may use any load balancing algorithm that is appropriate. For example, load balancer 374 may use a round robin scheme, or distribute the load based on CPU usage on each server or servers. In some embodiments, from then on, all information from the SB adapter is passed to the selected server for processing (392). Alternatively, the selected server may convert the format of the received information to new format at particular times. Depending on the destination, the information is then transferred from the server to a selected NB gateway (393), or the NMS GUI (394). When the information arrives at the NB gateway, it is transferred to a registered NB adapter based on the NB interface (I/F) protocol for communicating with the OSS (395). The information is then transferred from the NB adapter to the OSS (396).

The NMS architecture presented can provide multiple, significant benefits with the design of NB distributed gateway (NB adapters), distributed SB adapters, NMS application server clusters, and load balancing schemes to inter-connect between NB gateway and application server(s), and between SB adapters and application server(s). Three such examples follow.

First, the NB gateway can serve as a single point for receiving different types of information (e.g., network events such as traps) from NEs or the NMS server for distributing to registered NB adapters, and then to the OSS. A NB gateway-based architecture allows the information common to different NB adapters to be sent to the NB gateway just once, instead of multiple copies, and then the NB gateway multicasts the information to multiple destined NB adapters. With this architecture of an NB gateway decoupled from NMS application servers, multiple NB gateways, each of which includes a certain number of NB adapters, can be designed and distributed on different workstations for scalability and performance optimization. In one embodiment, the NB gateways running on different workstations communicate with each other via RMI transporting over TCP/IP.

Secondly, as a network grows to an increasing large scale, more processing power in the NMS servers may be needed for managing the network. With this server cluster-based NMS architecture, new NMS server instances can be incrementally started and added into server cluster 332 without affecting existing operations. The server cluster can be logically and physically distributed, so servers in a cluster can run on different workstations for increasing processing power. The load balancer allows the management work load to be distributed among all server instances in any desired fashion, which results in maximal efficiency and flexibility for any management policy to be implemented as carriers wish. An instance of the server can also be shut down for any reason without interrupting the server functionality as a whole. When a server is shutdown, its associated software modules (NB gateway 304, GUI 312, or SB adapters 340 or 344) automatically re-establish the association with another server instance (one of existing servers 362-364 or a standby server) based on certain criterion, such as selecting the lightest loaded server.

Thirdly, the distributed SB adapter-based NMS architecture can support a flexible network partitioning to manage

10

different management domains based on the amount of management traffic in each domain in a large scale network. All NEs in a management domain are associated with a SB adapter to communicate with the NMS servers. That is, the events in each partitioned domain are monitored by a designated SB adapter. With the server cluster, server instances can work with multiple SB adapters simultaneously, allowing a distributed SB adapter infrastructure to support a large number of NEs or a geographically separated network topology. Each SB adapter can select an instance of service using the load balancer based on certain criterion (e.g., selecting the lightest loaded server) to establish the association between the SB adapter and server instance. SB adapter modules can also be separated from NMS server 332 and run on separate workstations. Thus the network can be logically or physically partitioned in different management domains by configuring for each NE a SB adapter to handle events from that NE.

FIG. 3D is a flowchart illustrating a technique for transferring information (e.g., traps) from an NE in a partitioned network to server cluster 332. More specifically, the network is partitioned to different management domains in which each NE belongs to one management domain (396). Each domain is associated with one SB adapter (397). The information that originated from the NEs in a management domain is transferred to a configured SB adapter (398). That is, a configured SB adapter is pre-selected to handle events from the NEs in a management domain. For example, an adapter can register its IP address in all NEs in a management domain so that all NEs send traps to that SB adapter. From then on, the information follows the uplink information flow in FIG. 3C to be passed to a specific server instance and then to the OSS for processing (399). In some embodiments, the information is transferred to a designated application server or servers within cluster 332 wherein the designation was predetermined. That is, the SB adapter can be configured to communicate with certain registered server modules (instances). Because all the server instances are writing to the same database, the overall network view can be accessed from any partitioned region. In one embodiment, the SB adapters running on different workstations communicate with each other via RMI transporting over TCP/IP.

The NMS architecture presented can provide significant benefits of scalability and performance optimization. It can enable incremental addition of network management resources (such as server processing power, database memory) on an as needed basis without network operation interruption as the network grows. The NMS based on this architecture can truly serve carriers' large scale network management requirements in a most optimized way.

Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

What is claimed is:

1. A method, comprising:

receiving, at a first application server instance selected from a plurality of application server instances based on a load balancing process, first adapter processed information from a first adapter, wherein the first adapter processed information comprises event information received by the first adapter from a network element and processed by the first adapter based on a first communication protocol;

US 8,782,282 B1

11

processing, by the first application server instance, the first adapter processed information based on an event management service to produce application processed information;

5 sending, by the first application server instance, the application processed information to a gateway device, wherein the gateway device is one of a plurality of gateway devices respectively associated with the plurality of application server instances and is configured to transfer the application processed information to a second adapter of a plurality of second adapters configured to process the application processed information based on a second communication protocol to produce second adapter processed information and transfer the second adapter processed information to an operation support system device; and

10 in response to determining that the first application server instance has become disabled, facilitating establishing an association between the first adapter and a second application server instance of the plurality of application server instances and between the gateway device and the second application server instance.

2. The method of claim 1, wherein the first application server instance is configured to execute on a separate physical machine from the first adapter.

3. A system, comprising:

a first application server instance configured to receive first adapter processed information from a first adapter process the first adapter processed information based on an event management service to yield application processed information, and send the application server processed information to a gateway device, wherein the first adapter processed information comprises event information from a network element that has been processed by the first adapter based on a first communication protocol; and

a load balancing component configured to select the first application server instance from a plurality of application server instances based on a load balancing process; wherein the gateway device is one of a plurality of gateway devices respectively associated with the plurality of application server instances and is configured to transfer the application server processed information to a second adapter of a plurality of second adapters configured to process the application server processed information based on a second communication protocol to yield second adapter processed information, and send the second adapter processed information to an operation support system device, and

wherein, the first adapter and the gateway device are further configured to, in response to disablement of the first application server instance, establish an association with a second application server instance of the plurality of application server instances.

4. The method of claim 1, further comprising converting, by the second adapter, a protocol specific message associated with the first application server instance to a formatted message associated with the second communication protocol.

5. The method of claim 1, further comprising selecting the first application server instance based on a determination that the first application server instance has a lowest processing load of the plurality of application servers instances.

6. The method of claim 1, wherein the first communication protocol and the second communication protocol comprise one or more communication protocols associated with at least

12

one of extensible markup language, simple network management protocol, common object request broker architecture, or transaction language 1.

7. The method of claim 1, further comprising at least one of collecting, recording, or publishing the event information in accordance with the event management service for access by the operation support system device.

8. The method of claim 1 wherein the plurality of gateway devices comprise a plurality of physically or logically separated gateway devices.

9. The method of claim 1, wherein the gateway device is a physically and logically separate machine from the first application server instance.

10. The method of claim 1, further comprising converting, by the first adapter, a message associated with the first communication protocol to a protocol specific message associated with the first application server instance.

11. The method of claim 1, further comprising processing, by the gateway device, a function associated with the application server processed information.

12. The method of claim 1, wherein the event information relates to a configuration of the network element.

13. The method of claim 1, further comprising executing the first adapter and the second adapter on one or more virtual machines.

14. The method of claim 1, wherein the first adapter and the second adapter are configured to communicate with the first application server instance over a remote method invocation interface.

15. The system of claim 3, wherein the event information is associated with a configuration of the network element.

16. The system of claim 3, wherein the first application server instance comprises a performance manager component configured to collect performance data from a plurality of network elements respectively associated with a plurality of first adapters including the first adapter.

17. The system of claim 16, wherein the performance manager component is further configured to deliver at least a subset of the performance data to one or more of the plurality of network elements.

18. The system of claim 3, wherein the first communication protocol and the second communication protocol comprise one or more communication protocols associated with at least one of extensible markup language, simple network management protocol, common object request broker architecture, or transaction language 1.

19. The system of claim 3, wherein at least one of the first adapter or the second adapter are executed on one or more virtual machines.

20. The system of claim 3, wherein the first adapter and the second adapter are configured to communicate with the first application server instance over a remote method invocation interface.

21. The system of claim 3, wherein the load balancing component is configured to select the first application server instance based on a determination that the first application server instance has a lowest processing load of the plurality of application server instances.

22. The system of claim 3, wherein the plurality of gateway devices comprises a plurality of physically or logically separated gateway devices.

* * * * *

EXHIBIT B



US009485176B2

(12) **United States Patent**
Pan et al.

(10) **Patent No.:** **US 9,485,176 B2**

(45) **Date of Patent:** ***Nov. 1, 2016**

(54) **GLOBAL IP-BASED SERVICE-ORIENTED NETWORK ARCHITECTURE**

(71) Applicant: **Brixham Solutions Ltd.**, Tortola (VG)

(72) Inventors: **Ping Pan**, San Jose, CA (US); **Richard Gitlin**, Little Silver, NJ (US)

(73) Assignee: **Brixham Solutions Ltd.**, Tortola (VG)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/864,843**

(22) Filed: **Sep. 24, 2015**

(65) **Prior Publication Data**

US 2016/0021004 A1 Jan. 21, 2016

Related U.S. Application Data

(63) Continuation of application No. 14/469,427, filed on Aug. 26, 2014, now Pat. No. 9,172,638, which is a continuation of application No. 11/890,308, filed on Aug. 3, 2007, now Pat. No. 8,848,711.

(60) Provisional application No. 60/835,794, filed on Aug. 4, 2006.

(51) **Int. Cl.**
H04L 12/721 (2013.01)
H04L 12/725 (2013.01)
H04L 12/741 (2013.01)

(52) **U.S. Cl.**
CPC **H04L 45/68** (2013.01); **H04L 45/304** (2013.01); **H04L 45/74** (2013.01)

(58) **Field of Classification Search**
None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,920,705	A	7/1999	Lyon
6,167,051	A	12/2000	Nagami
6,347,088	B1	2/2002	Katou
6,430,184	B1	8/2002	Robin
6,546,427	B1	4/2003	Ehrlich
6,574,477	B1	6/2003	Rathunde
6,621,793	B2	9/2003	Widegren et al.
6,665,273	B1	12/2003	Goguen et al.
6,674,744	B1	1/2004	Doshi et al.
6,680,943	B1	1/2004	Gibson
6,813,271	B1	11/2004	Cable
6,845,389	B1	1/2005	Sen et al.
6,985,488	B2	1/2006	Pan et al.
7,050,396	B1	5/2006	Cohen et al.
7,200,104	B2	4/2007	Saleh
7,436,782	B2	10/2008	Ngo et al.

(Continued)

OTHER PUBLICATIONS

Shah, et al., Internet Draft, ARP Mediation for IP Interworking of Layer 2 VPN, Jul. 2007.

(Continued)

Primary Examiner — Hassan Phillips

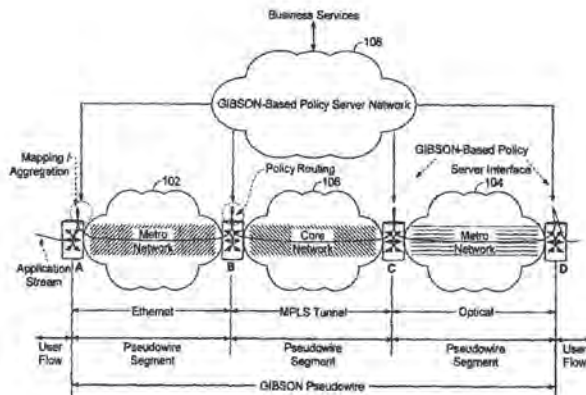
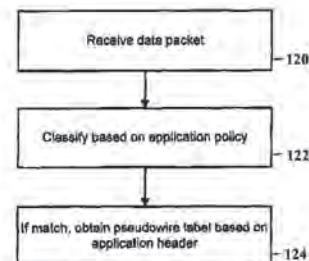
Assistant Examiner — Saba Tsegaye

(74) *Attorney, Agent, or Firm* — Patent and Licensing LLC; Daniel W. Juffernbruch; John G. Fijolek

(57) **ABSTRACT**

Data is transferred. A data packet associated with an application flow is received. A Pseudowire label is determined based at least in part on an application header associated with the data packet. The data packet is encapsulated with the Pseudowire label. The data packet is transferred over a Pseudowire using the Pseudowire label.

20 Claims, 15 Drawing Sheets



US 9,485,176 B2

Page 2

(56)

References Cited

U.S. PATENT DOCUMENTS

7,697,528 B2	4/2010	Parry et al.	
7,990,888 B2	8/2011	Nadeau et al.	
8,160,055 B1	4/2012	Nadeau et al.	
2001/0021175 A1	9/2001	Haverinen	
2001/0023453 A1	9/2001	Sundqvist	
2002/0112072 A1	8/2002	Jain	
2002/0141393 A1	10/2002	Eriksson et al.	
2002/0146026 A1	10/2002	Unitt	
2003/0002482 A1	1/2003	Kubler	
2003/0039237 A1	2/2003	Forslow	
2003/0117950 A1	6/2003	Huang	
2004/0017796 A1	1/2004	Lemieux et al.	
2004/0105459 A1	6/2004	Mannam	
2004/0114595 A1	6/2004	Doukai	
2004/0133692 A1	7/2004	Blanchet	
2004/0156313 A1	8/2004	Hofmeister	
2004/0165605 A1	8/2004	Nassar	
2004/0174865 A1	9/2004	O'Neill	
2004/0196840 A1	10/2004	Amrutur et al.	
2004/0252717 A1	12/2004	Solomon et al.	
2005/0010653 A1 *	1/2005	McCanne	H04L 69/329 709/219
2005/0010685 A1	1/2005	Ramath et al.	
2005/0018605 A1	1/2005	Footo	
2005/0021789 A1	1/2005	Iloglu et al.	
2005/0044262 A1	2/2005	Luo	
2005/0220148 A1	10/2005	DelRegno	
2005/0237927 A1	10/2005	Kano	
2006/0002423 A1	1/2006	Rembert	
2006/0018252 A1	1/2006	Sridhar	
2006/0046658 A1	3/2006	Cruz	
2006/0047851 A1	3/2006	Voit	
2006/0090008 A1	4/2006	Guichard	
2006/0146832 A1	7/2006	Rampal et al.	
2006/0182122 A1	8/2006	Davie et al.	
2006/0227767 A1	10/2006	Johnson et al.	
2006/0233167 A1	10/2006	McAllister et al.	
2006/0291445 A1 *	12/2006	Martini	H04L 45/50 370/351
2007/0053366 A1	3/2007	Booth et al.	
2007/0127479 A1	6/2007	Sinicrope et al.	
2007/0206607 A1	9/2007	Chapman et al.	
2007/0237150 A1	10/2007	Wood	
2008/0031129 A1	2/2008	Arseneault	
2008/0084891 A1	4/2008	Balus et al.	
2010/0014538 A1	1/2010	Asati et al.	
2012/0307830 A1	12/2012	DelRegno et al.	

OTHER PUBLICATIONS

Martini, et al., Internet Draft, Dynamic Placement of Multi Segment Pseudo Wires, Jul. 2007.
 Martini, et al., "Internet Draft, Segmented Pseudo Wire," Jul. 2007.
 Pan, et al., "Internet Draft, Pseudo Wire Protection," Jul. 2006.
 Rosen, et al., Internet Draft, PWE3 Congestion Control Framework, Mar. 2004.
 Rosen, et al., BGP/MPLS IP Virtual Private Networks (VPNs), Feb. 2006.

Martini, et al., Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP), Apr. 2006.
 Ping Pan, internet Draft, Dry-Martini: Supporting Pseudo-wires in Sub-IP Access Networks, Jul. 2005.
 McPherson, et al., Pseudowire Emulation Edge to Edge (pwe3) Jun. 13, 2007, <http://www.ietf.org/html.charters/pwe3-charter.html>.
 Vasseur, et al., Path Computation Element (pce), May 9, 2007, <http://www.ietf.org/html.charters/pce-charter.html>.
 Chen, The LSP Protection/Restoration Mechanism in GMPLS, Internet Citation, Online, (Oct. 1, 2002) XP002239552. Retrieved from Internet URL <http://www.site.uottawa.ca/~hochmann/dsrg/PublicDocuments/Master-theses/Chen,%20Ziyang%20%20-%202002.pdf>.
 Allerton, Ethernet Transport over Wide Area Networks, Packet-Aware Transport for Metro Networks, IEEE Communications Magazine, pp. 120-127, Mar. 2004.
 Anderson, et al., LDP Specification, Network Working Group, Jan. 2001.
 Martini, et al., Encapsulation Methods for Transport of Ethernet over MPLS Networks, Network Working Group, Apr. 2006.
 Martini, et al., Encapsulation Methods for Transport of Frame Relay Over MPLS Networks, Network Working Group, Feb. 2006.
 Metz, et al., Pseudowire Attachment Identifiers for Aggregation and VPN Autodiscovery, PWE3 Working Group, Feb. 25, 2006.
 Martini, et al., Dynamic Placement of Multi Segment Pseudo Wires, PWE3 Working Group, Jun. 2006.
 Martini, et al., Pseudowire Setup and Maintenance using LDP, Network Working Group, Mar. 2005.
 Braden, et al., "Integrated Services in the Internet Architecture: an overview", Network Working Group, Jun. 1994.
 Bryant, et al., "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", Network Working Group, Mar. 2005.
 Blake, et al., "An Architecture for Differentiated Services," Network Working Group, Dec. 1998.
 Theimer, et al., "Requirements for OAM Functionality in MPLS", Oct. 1999, Watersprings.
 Harry Newton, "Newton's Telecom Dictionary", 23rd Updated and Expanded Edition, p. 825, p. 239, Flatiron Publishing, New York, Mar. 2007.

Office Action dated Jun. 30, 2011 for U.S. Appl. No. 11/890,308, 9 pages.
 Office Action dated Jan. 5, 2011 for U.S. Appl. No. 11/890,308, 8 pages.
 Office Action dated Jul. 19, 2010 for U.S. Appl. No. 11/890,308, 8 pages.
 Office Action dated Sep. 25, 2009 for U.S. Appl. No. 11/890,308, 7 pages.
 Office Action dated Jul. 31, 2012 for U.S. Appl. No. 11/890,308, 12 pages.
 Office Action dated Jan. 11, 2012 for U.S. Appl. No. 11/890,308, 9 pages.
 Office Action dated Oct. 24, 2013 for U.S. Appl. No. 11/890,308, 23 pages.
 Office Action dated Feb. 6, 2013 for U.S. Appl. No. 11/890,308, 11 pages.
 Office Action dated Jan. 23, 2015 for U.S. Appl. No. 14/469,427, 26 pages.

* cited by examiner

U.S. Patent

Nov. 1, 2016

Sheet 1 of 15

US 9,485,176 B2

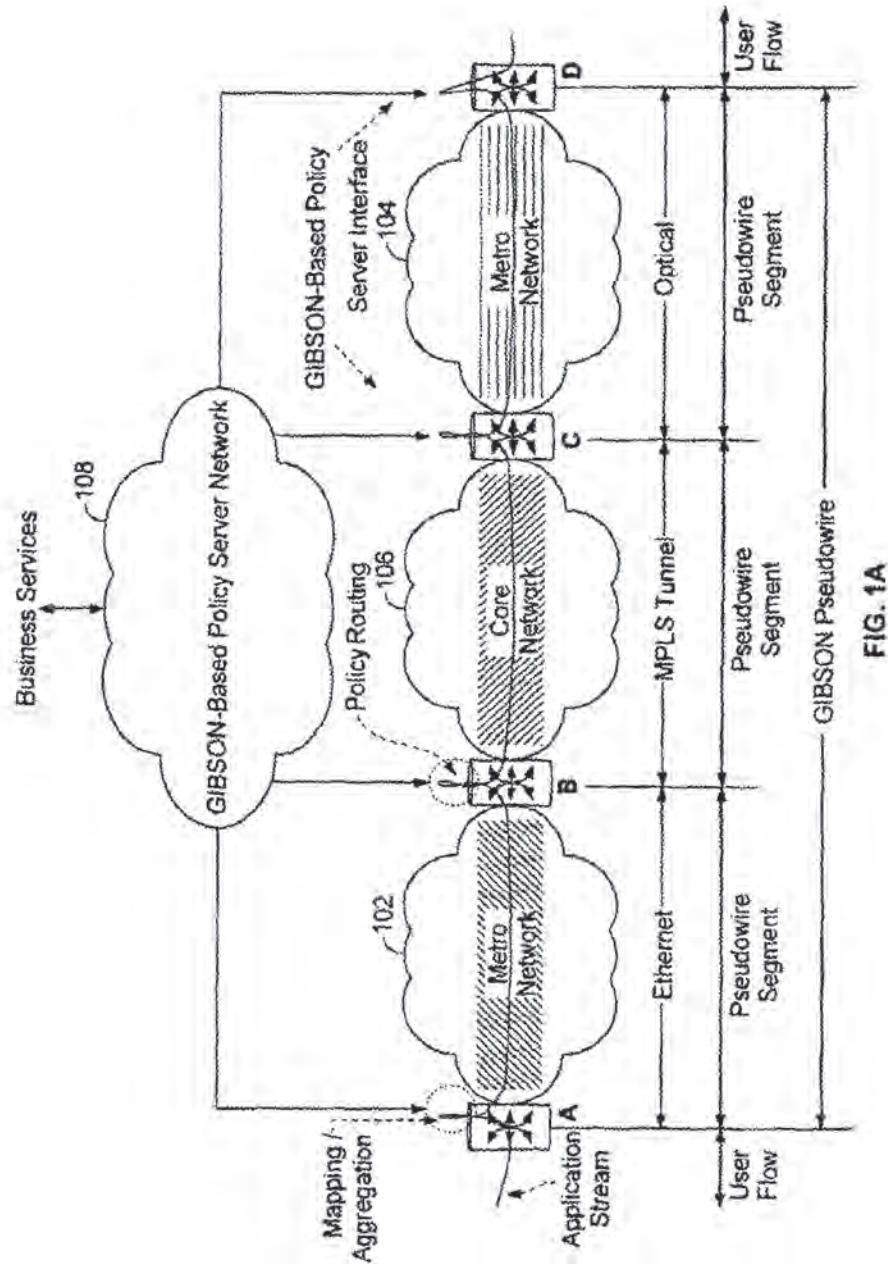


FIG. 1A

U.S. Patent

Nov. 1, 2016

Sheet 2 of 15

US 9,485,176 B2

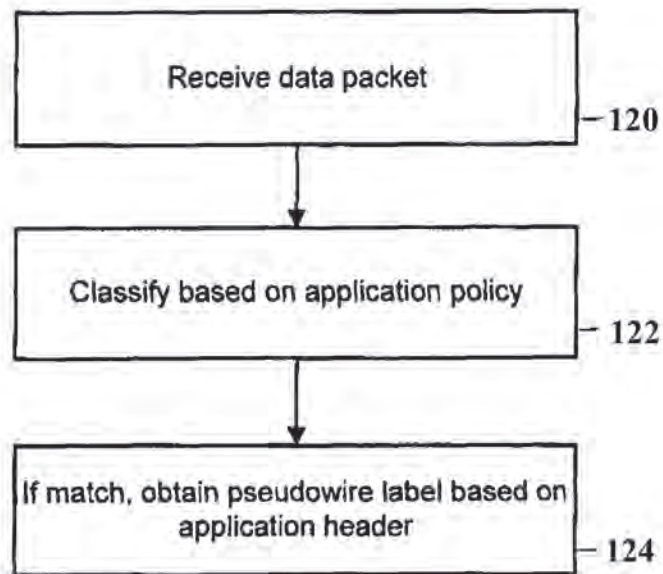


FIG. 1B

U.S. Patent

Nov. 1, 2016

Sheet 3 of 15

US 9,485,176 B2

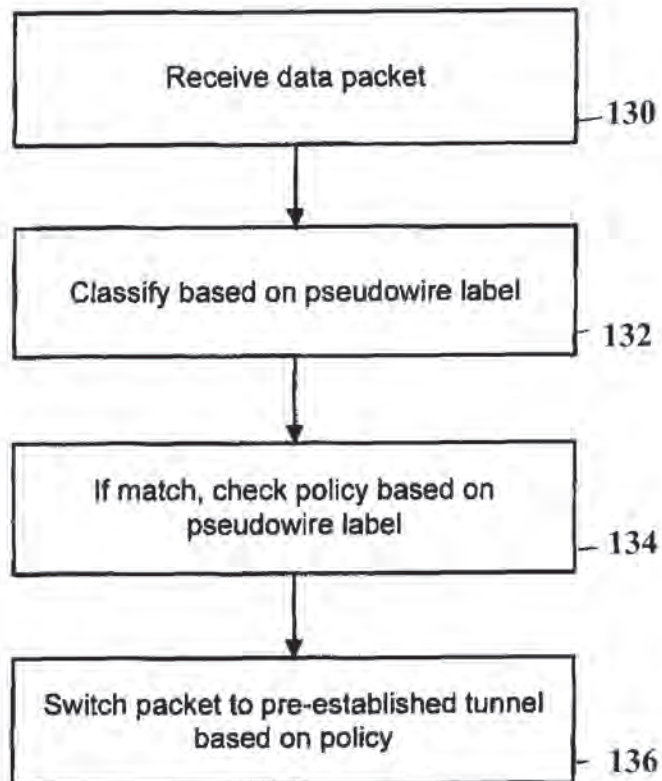


FIG. 1C

U.S. Patent

Nov. 1, 2016

Sheet 4 of 15

US 9,485,176 B2

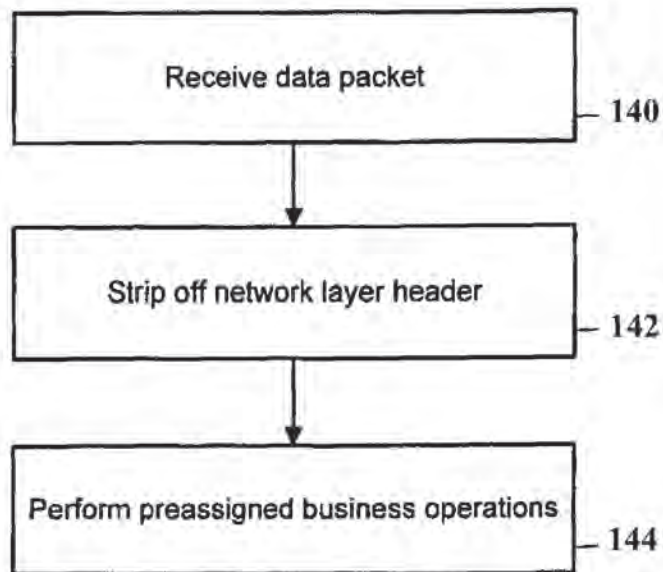


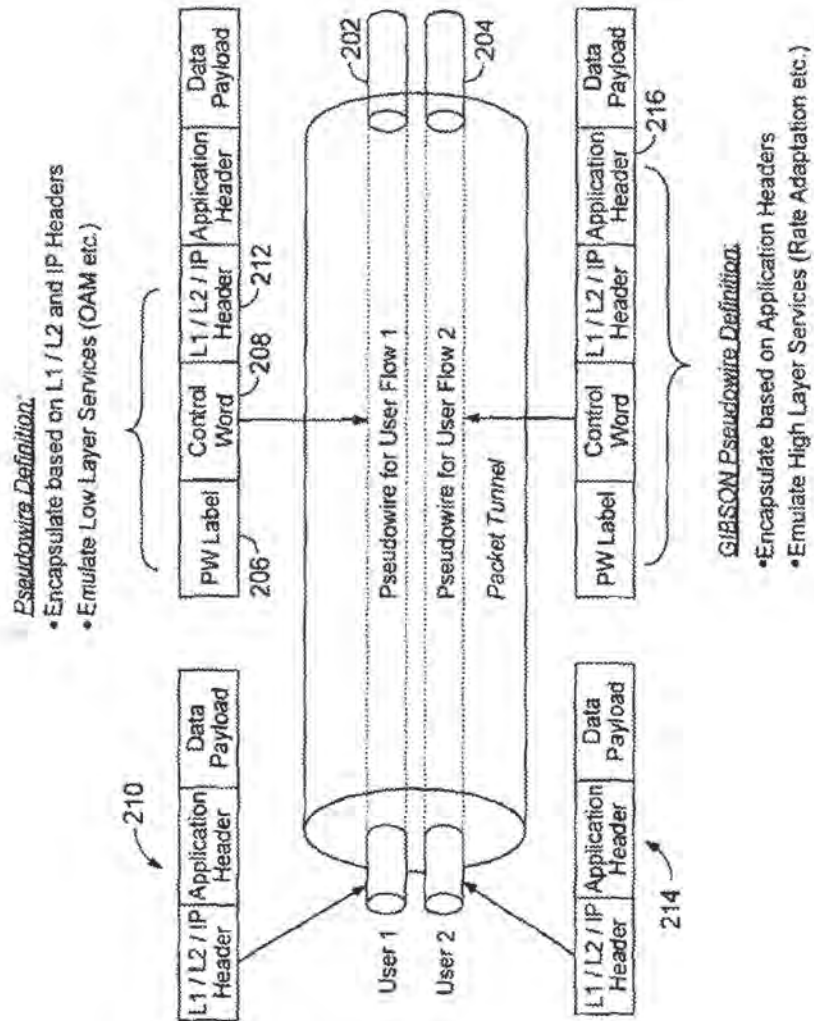
FIG. 1D

U.S. Patent

Nov. 1, 2016

Sheet 5 of 15

US 9,485,176 B2



U.S. Patent

Nov. 1, 2016

Sheet 6 of 15

US 9,485,176 B2

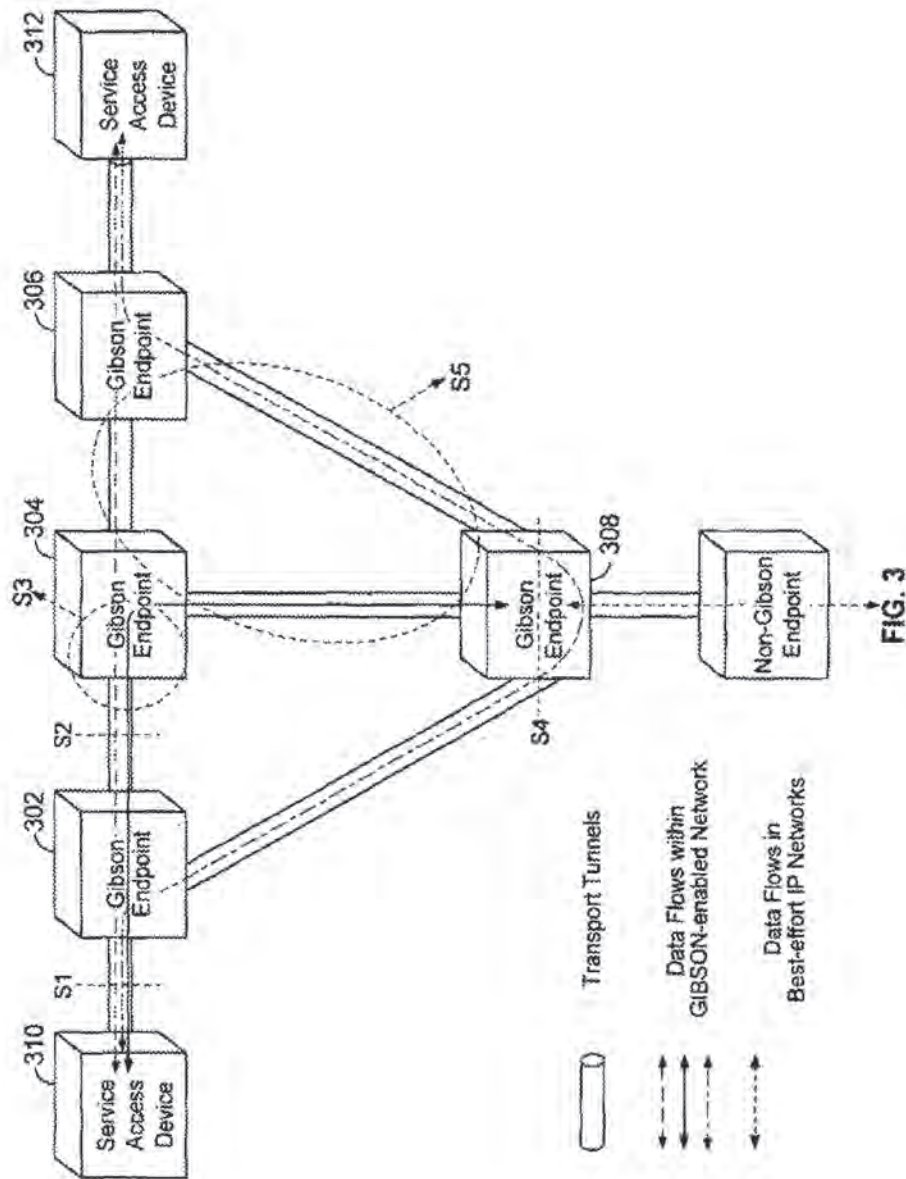


FIG. 3

U.S. Patent

Nov. 1, 2016

Sheet 7 of 15

US 9,485,176 B2

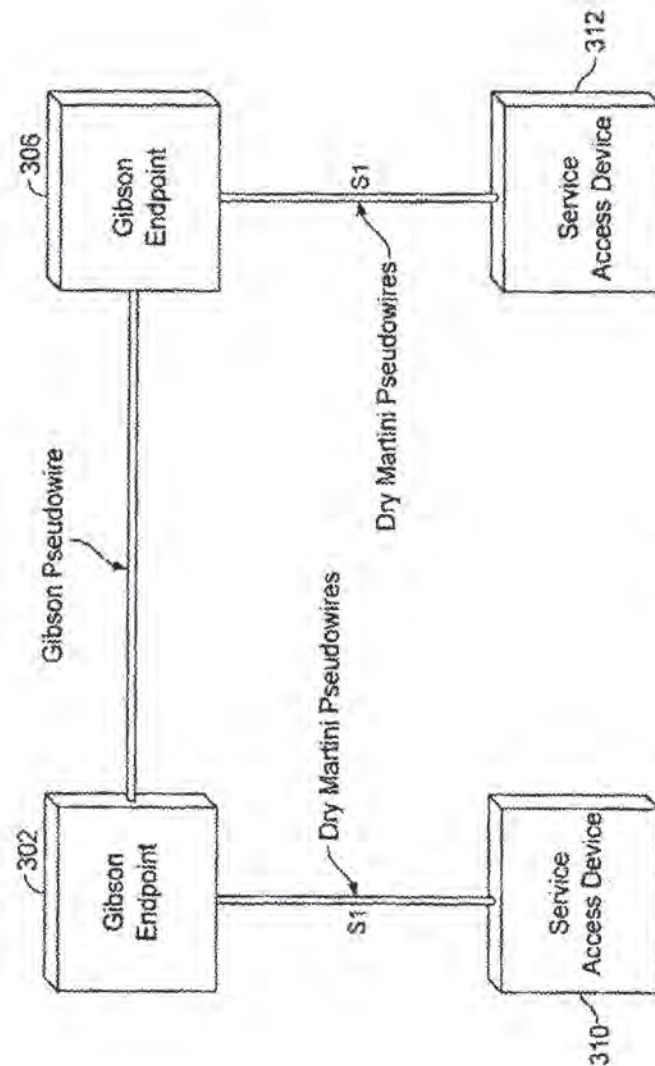


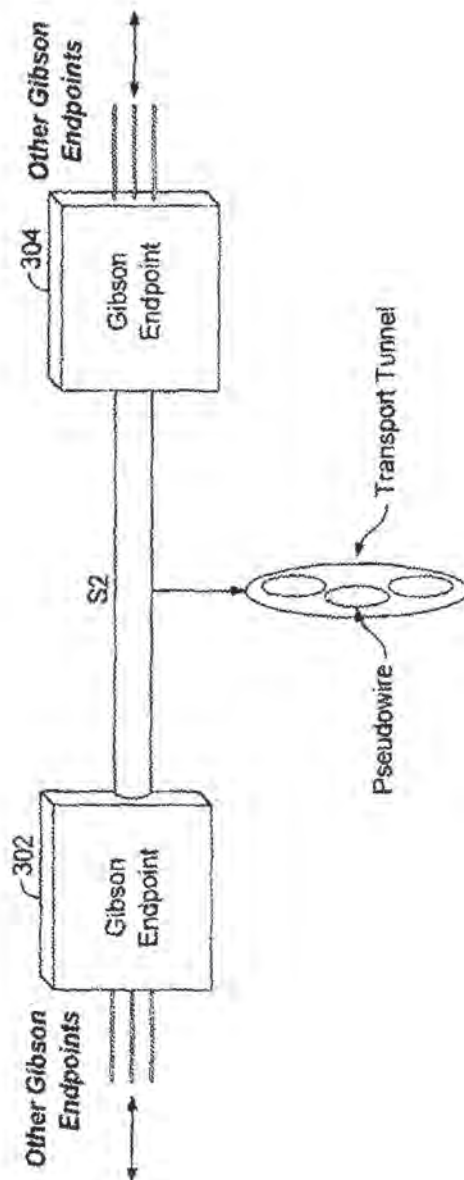
FIG. 4

U.S. Patent

Nov. 1, 2016

Sheet 8 of 15

US 9,485,176 B2



U.S. Patent

Nov. 1, 2016

Sheet 9 of 15

US 9,485,176 B2

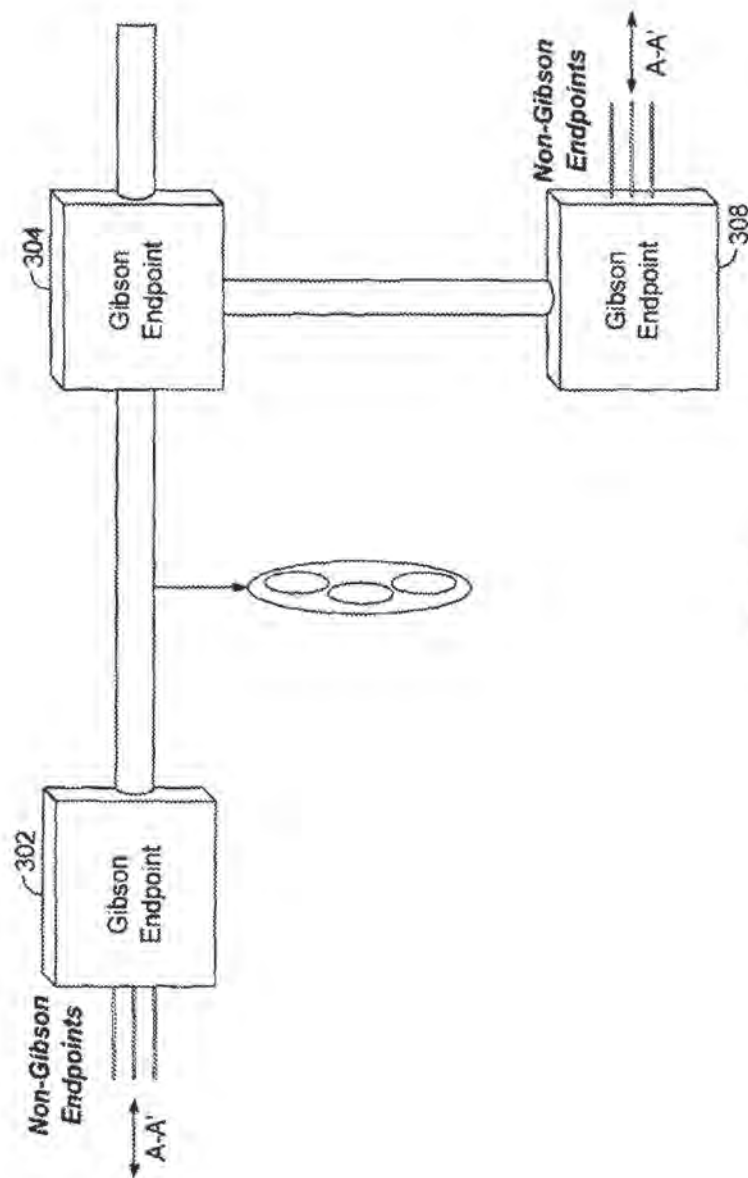


FIG. 6

U.S. Patent

Nov. 1, 2016

Sheet 10 of 15

US 9,485,176 B2

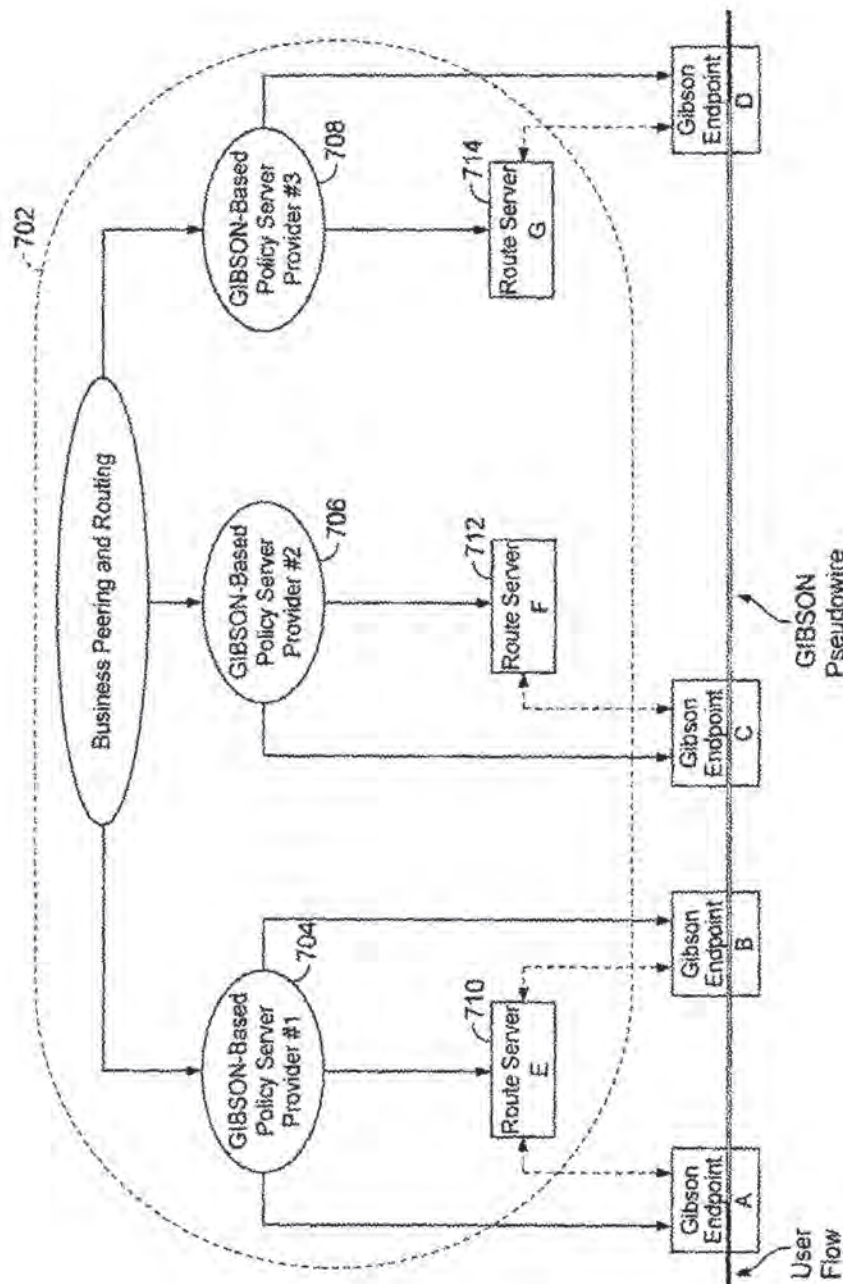


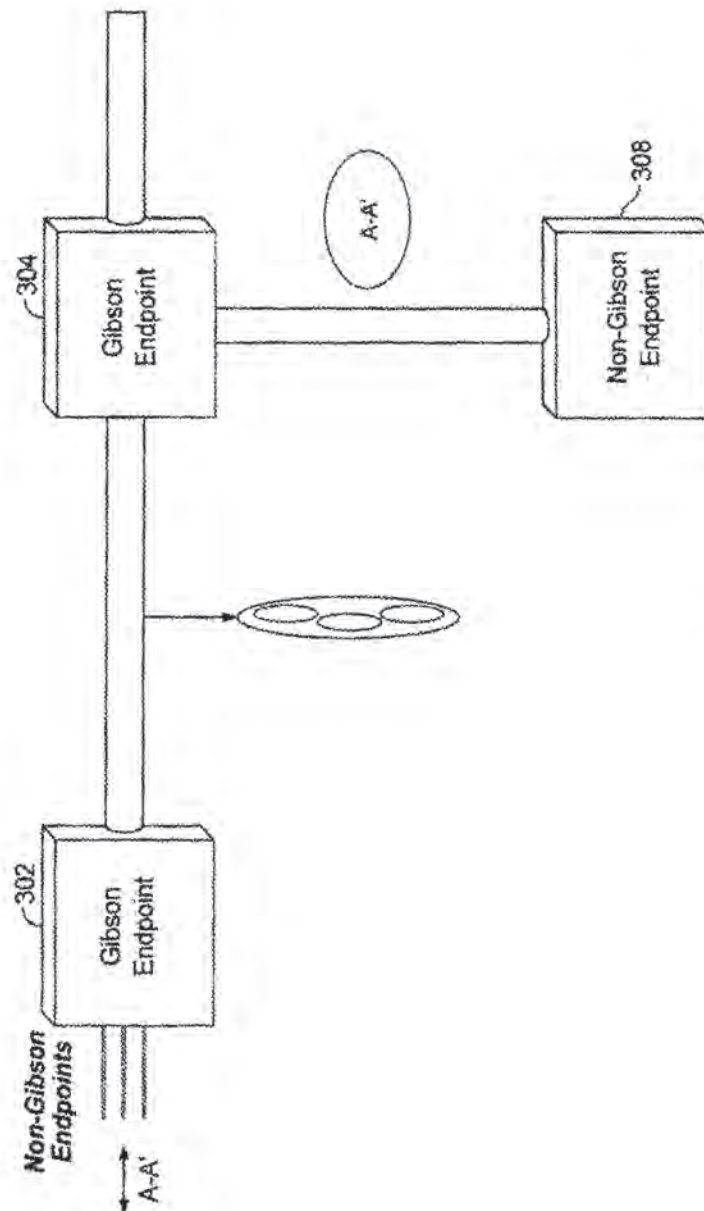
FIG. 7

U.S. Patent

Nov. 1, 2016

Sheet 11 of 15

US 9,485,176 B2



U.S. Patent

Nov. 1, 2016

Sheet 12 of 15

US 9,485,176 B2

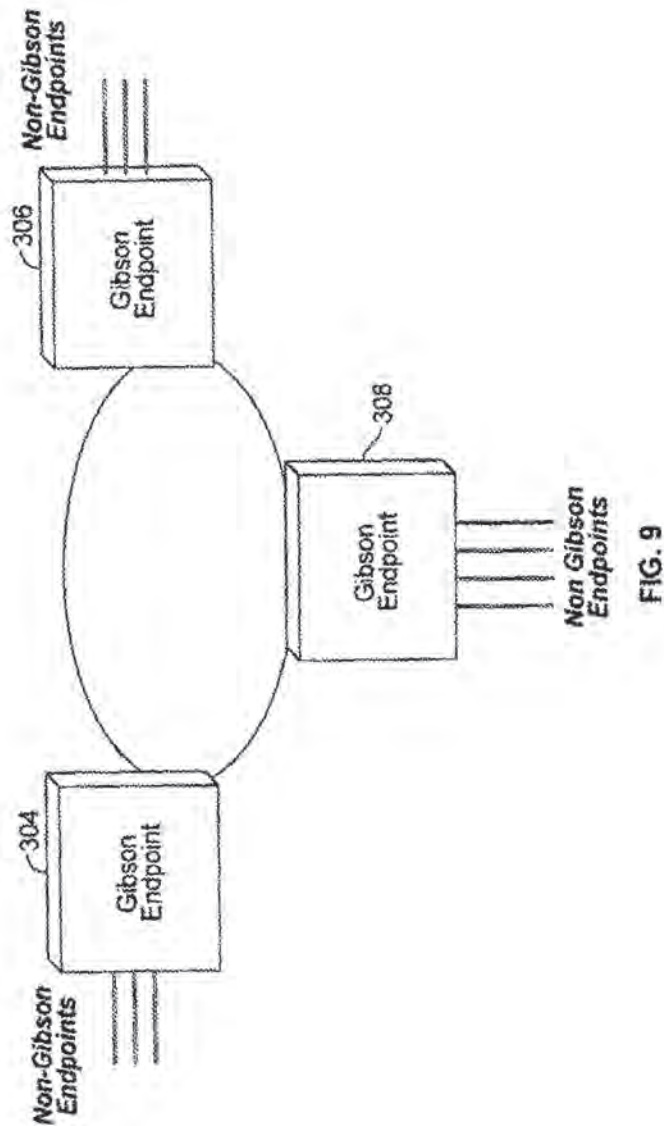


FIG. 9

U.S. Patent

Nov. 1, 2016

Sheet 13 of 15

US 9,485,176 B2

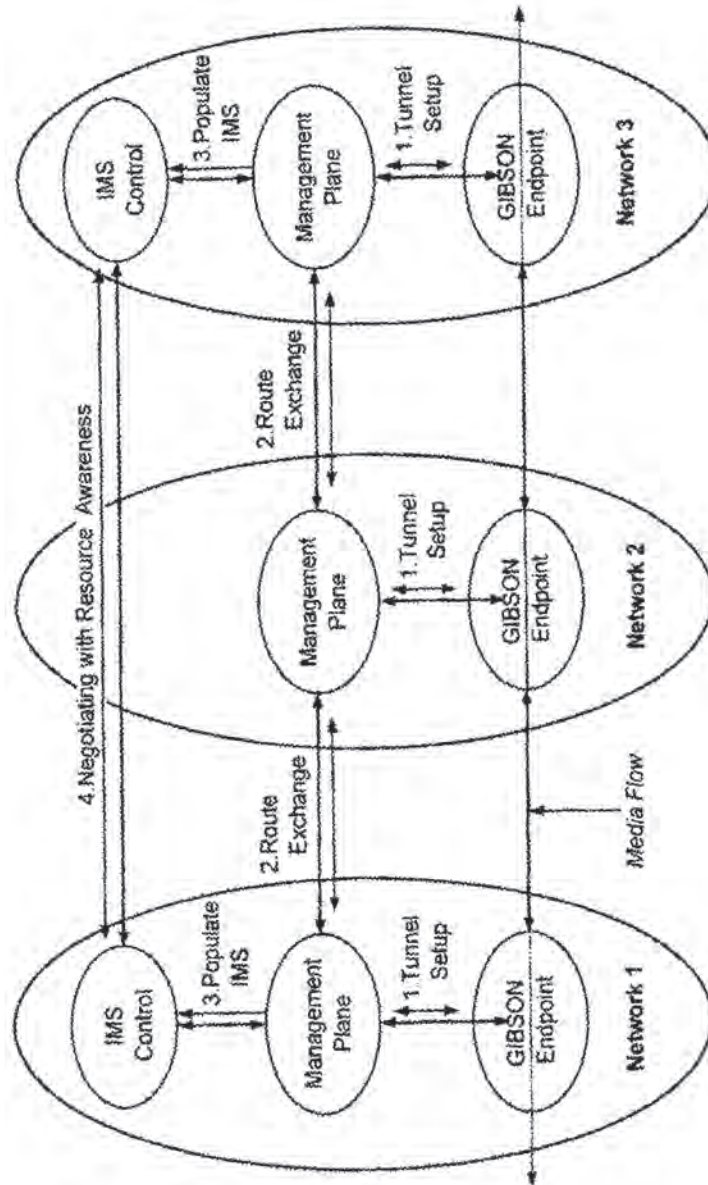


FIG. 10

U.S. Patent

Nov. 1, 2016

Sheet 14 of 15

US 9,485,176 B2

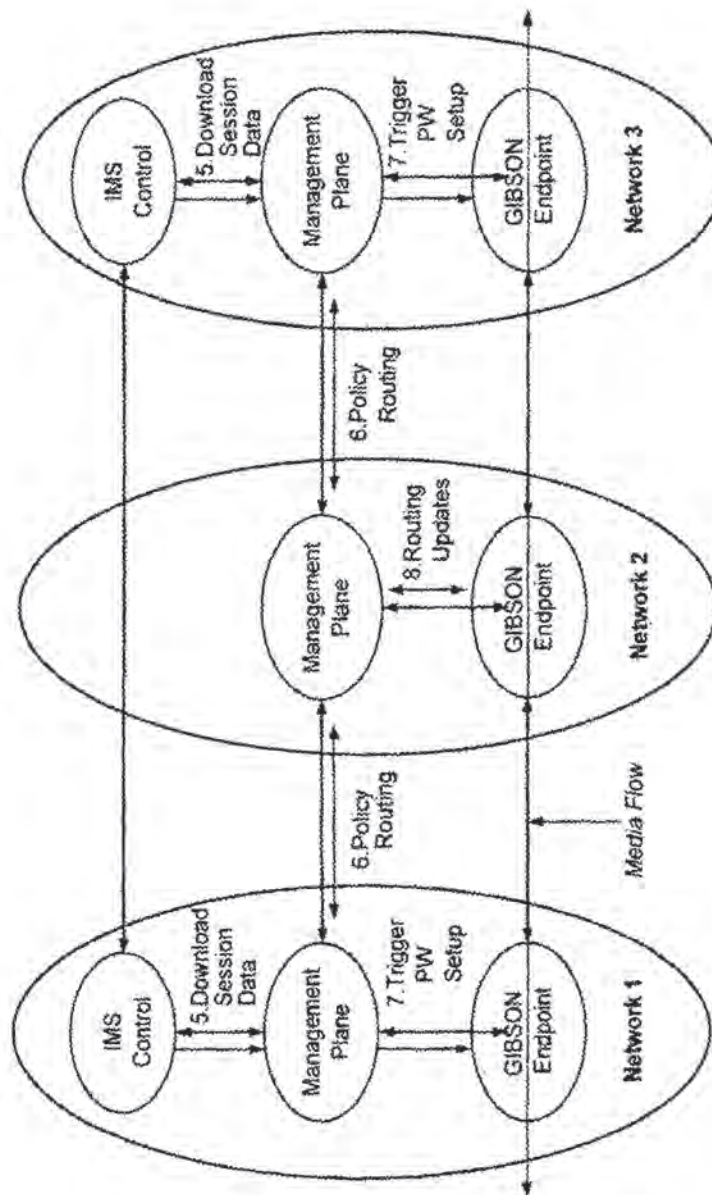


FIG. 11

U.S. Patent

Nov. 1, 2016

Sheet 15 of 15

US 9,485,176 B2

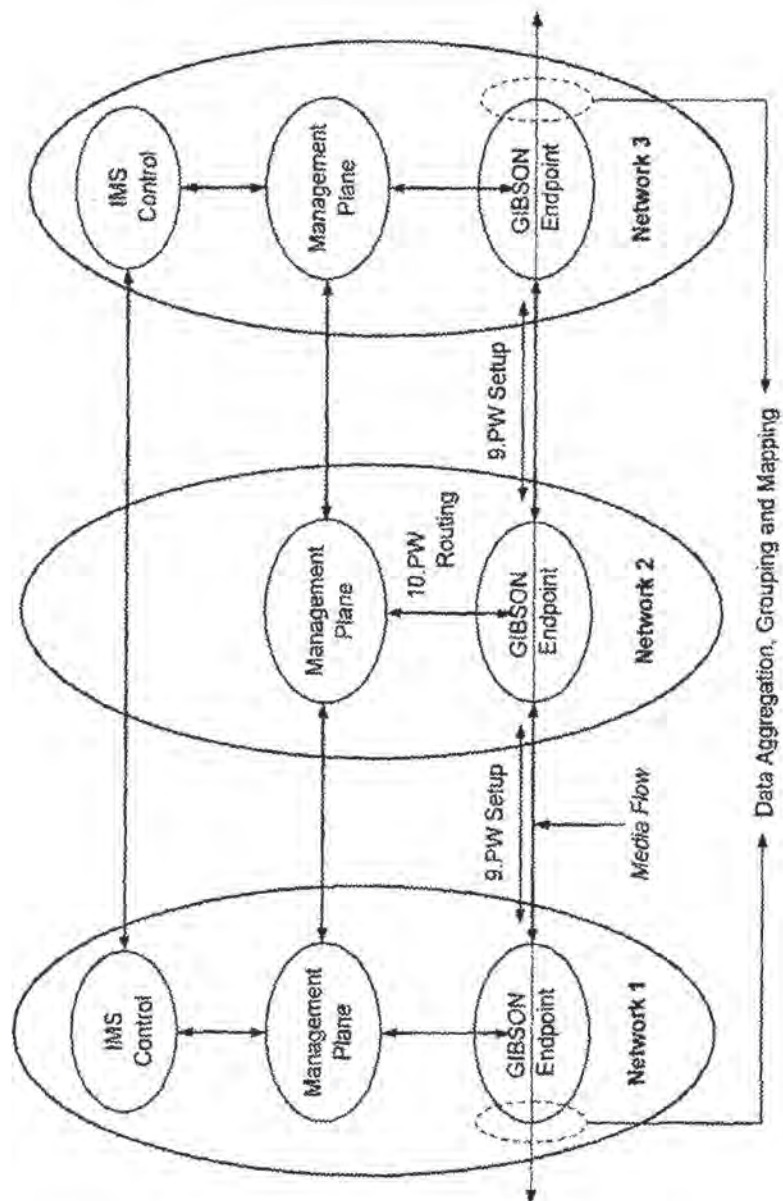


FIG. 12

US 9,485,176 B2

1

**GLOBAL IP-BASED SERVICE-ORIENTED
NETWORK ARCHITECTURE****CROSS-REFERENCE TO RELATED
APPLICATIONS**

This application is a continuation of, and claims priority to, U.S. patent application Ser. No. 14/469,427, filed on Aug. 26, 2014, and entitled "GLOBAL IP-BASED SERVICE-ORIENTED NETWORK ARCHITECTURE," (issued as U.S. Pat. No. 9,172,638 on Oct. 27, 2015), which is a continuation of U.S. patent application Ser. No. 11/890,308, filed on Aug. 3, 2007, and entitled "GLOBAL IP-BASED SERVICE-ORIENTED NETWORK ARCHITECTURE," (issued as U.S. Pat. No. 8,848,711 on Sep. 30, 2014), which claims priority to U.S. Provisional Patent Application No. 60/835,794, filed on Aug. 4, 2006, and entitled "GLOBAL IP-BASED SERVICE ORIENTED NETWORK ARCHITECTURE OVERVIEW AND IMS USER CASE." The entireties of these related applications are incorporated herein by reference.

BACKGROUND OF THE INVENTION

Providing new services may face challenges in creating a common service conception in a diversely owned and multi-technology network of the future. The following are examples of potential challenges:

1. Access/metro and backbone networks may belong to different carriers or business entities. For example, the access networks may belong to wireless service providers, while the backbone networks may belong to a national or global carrier that provides data transport services to multiple access or metro networks.

2. There may be underlying data transport technology differences among providers and also often between metro/access and core networks of the same provider.

3. The combination of ownership diversity and technology diversity is reflected in a more complex set of management interfaces to control infrastructure, and this complexity may create problems if it is reflected upward to the service, business, and operations management layers.

4. There may be a considerable variability in the "value" of service relationships and thus in the per-service handling that can be justified. Some customer data flows may be handled individually (video, for example) and others may likely be handled in aggregated form (voice).

5. There may be regulatory issues such as intercept/surveillance that may have to be applied, or that may have to be routed around to avoid.

6. Since user traffic is transported as IP packets throughout the network, the backbone carriers may not have the ability or incentive to provide special treatment to important user flows. Subsequently, "hot-potato" type routing policies are applied to inter-carrier traffic. The end users can only rely on application-level congestion and flow control, such as TCP, to regulate traffic. This practice may not likely scale or economical as end-user applications become more bandwidth-intensive and delay-sensitive.

7. There may be business issues associated with route selection that cannot be reflected in ordinary IP route processing using mechanisms like OSPF or IS-IS.

8. Services may have to be created at the network edge and border. Service providers may offer new services, such as voice, video, security and VPN, from a network edge. Given the competition from application service providers, the cost in operation may become an issue.

2

Solutions to one or more of these problems would be desirable.

BRIEF DESCRIPTION OF THE DRAWINGS

Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

FIG. 1A is a diagram illustrating an embodiment of a service facilitation architecture.

FIG. 1B is a flowchart illustrating an embodiment of a process for receiving a data packet at an ingress node.

FIG. 1C is a flowchart illustrating an embodiment of a process for receiving a data packet at a transit node.

FIG. 1D is a flowchart illustrating an embodiment of a process for receiving a data packet at a termination or egress node.

FIG. 2 is a diagram illustrating an embodiment of a GIBSON Pseudowire.

FIG. 3 is a diagram illustrating an embodiment of a GIBSON architecture.

FIG. 4 is a diagram illustrating an embodiment of a GIBSON S1 interface.

FIG. 5 is a block diagram illustrating an embodiment of a GIBSON S2 interface.

FIG. 6 is a block diagram illustrating an embodiment of a GIBSON S3 interface.

FIG. 7 is a block diagram illustrating an embodiment of the operation of GIBSON-based Pseudowire routing.

FIG. 8 is a block diagram illustrating an embodiment of a GIBSON S4 interface.

FIG. 9 is a block diagram illustrating an embodiment of a GIBSON S5 interface.

FIGS. 10-12 are block diagrams illustrating an embodiment of an example user case for IMS.

DETAILED DESCRIPTION

The invention can be implemented in numerous ways, including as a process, an apparatus, a system, a composition of matter, a computer readable medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or communication links. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. A component such as a processor or a memory described as being configured to perform a task includes both a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. In general, the order of the steps of disclosed processes may be altered within the scope of the invention.

A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the

US 9,485,176 B2

3

invention has not been described in detail so that the invention is not unnecessarily obscured.

FIG. 1A is a diagram illustrating an embodiment of a service facilitation architecture. In this example, a service facilitation layer is built above some network protocols but maps downward to other network technologies. An expansion to the Pseudowire specification may enable this new layer to create all of the service relationships (e.g. point-to-point, multipoint, etc.) and support a full range of business and residential services. In some embodiments, controlling this layer requires a single management interface per provider jurisdiction, and this may reduce operations cost and complexity. As used herein, this new architectural layer is referred to as GIBSON (Global IP-Based Service-Oriented Network).

The GIBSON architecture provides a solution for providers to transport service-guaranteed user traffic over a multi-provider network. In some embodiments, it interfaces with a provider's management plane for service discovery and mapping, and leverages standard-based MPLS Pseudowire techniques to interface with network routers and switches. The GIBSON architecture binds business services to a network data-plane, and enables providers to provision, manage and monitor customer waffle for new service, such as IMS and VoD (video-on-demand), or other services.

For purposes of explanation, IMS-based management-plane techniques may be used in some of the examples described herein; however, in various embodiments, any appropriate policy server network and business policies may be used.

The GIBSON architecture may include one or more of the following features:

1. Open interface for business service creation and provisioning
2. Operate in both intra-provider and inter-provider environment
3. Provide consistent edge-to-edge per-flow forwarding behavior
4. Flow type agnostic capable of processing flows in any format
5. Support for "nesting" of Pseudowires to facilitate traffic management and virtual service creation
6. Independent of underlying network transport tunneling mechanism
7. Applicable to all service devices, with less dependency on IP routing

To achieve the above claims, GIBSON in some embodiments defines a set of rules for interfacing with network edge nodes, and leverages and extends the MPLS PWE3 mechanism for data transport and network device interfacing.

For example, as shown in FIG. 1A, a provider network consists of two access networks 102 and 104 and one core network 106, running Ethernet, optical (SONET/SDH) and IP/MPLS, respectively. Each network uses different underlying data transport technology, and is administrated separately. A provider needs to support multiple services, including private leased line, video distribution and residential broadband data access.

In the example, the provider is to deliver high-quality, high-premium and long-duration video streams between end users. Through business arrangements and network planning, the provider decides to deliver user video traffic over border node A, B, C and D. Between each pair of border nodes, there may be multiple routers and switches operating with different types of control protocols. The network between A and B may be Ethernet network running IEEE 802.1ah Provider Backbone Bridging (PBB) and Provider

4

Backbone Transport (PBT), the network between B and C may be running MPLS traffic engineering, and, finally, the network between C and D may operate over GMPLS.

The provider enables GIBSON-based policy server network 108 to distribute policy information. At connection setup time, GIBSON-based policy server network 108 may download the service-specific parameters, such as packet identification (e.g., RTP port numbers), a globally unique flow-id, and QoS information to edge nodes A and D. Further all the nodes may get policy routing information from GIBSON-based policy server network 108. Each policy routing entry has information such as "for flow-id X, go to node Y".

In this example, upon the reception of policy information, edge node A may trigger the establishment of an MPLS Pseudowire as defined in IETF PWE3 WG. The Pseudowire setup sequence may follow the sequence as defined in the IETF standard body. Specifically, the Pseudowire type may be IP as defined in the IETF standard titled "ARP Mediation for IP Interworking of Layer 2 VPN" Setting up Pseudowires with QoS has been defined in the IETF standard titled "Dynamic Placement of Multi Segment Pseudo Wires".

When the Pseudowire setup messages arrive at node B or C, the node may extract the flow-id information, search the policy routing database provided by GIBSON-based policy server network 108, and route the Pseudowires accordingly. This may result in an edge-to-edge multiple-hop Pseudowire from A to D through B and C.

For instance, when multimedia traffic arrives at edge nodes A and D, they may map incoming packets that have the same RTP port numbers as provided from GIBSON-based policy server network 108 to the established Pseudowire. At each hop, the traffic may receive the QoS guarantees as specified by the Pseudowire.

As shown in the example, GIBSON interfaces with policy server network 108 and leverages Pseudowire technology to guarantee service-oriented traffic over the network. The Pseudowires that operate in the context of GIBSON are referred to herein as "GIBSON Pseudowires", which is more fully described below.

In various embodiments, each of nodes A-D may be an IP router, Ethernet switch, other switch, session border controller (SBC), server, end user client, a personal computer (PC), etc. In various embodiments, networks 102, 104, and 106, may operate using a variety of network technologies, such as IP, Layer 2 Ethernet, MPLS, etc. Each network may have one or more pre-established tunnels.

In some embodiments, business policies are downloaded to one or more of edge nodes A-D. In some embodiments, the business policies are periodically downloaded. In some embodiments, the business policies are event triggered. For example, an edge node may request at least a portion of a business policy and receive it in response to the request.

In this example, traffic flow is bidirectional; that is an application flow may go from node A to node D or vice versa. However, the GIBSON concept could apply to both bidirectional and unidirectional traffic.

FIG. 1B is a flowchart illustrating an embodiment of a process for receiving a data packet at an ingress node. For example, this process may be performed at node A or D in FIG. 1A, if an application stream is sent from node A or node D, respectively.

At 120, a data packet is received. For example, at node A, a data packet associated with an application stream is received. The application stream is associated with a service, such as VoIP, video, or applications such as web 2.0. At 122,

US 9,485,176 B2

5

the data packet is classified based on an application policy. For example, the packet is inspected and compared against preloaded business arrangement policy information to see if it belongs to a particular flow. If the data packet satisfies a business arrangement, at 124, a Pseudowire label is obtained based on the application header. A mechanism for obtaining Pseudowire labels is defined in IETF. However, the GIBSON architecture includes the action of mapping application flows into Pseudowires. The data packet is encapsulated with the Pseudowire label. The data packet is aggregated into a transport tunnel that is prearranged by the provider. Examples of transport network tunnels include Ethernet VLAN, optical DWDM cross connection, or IP/MPLS LSP (label switched path). The data packet is transferred over a Pseudowire in the transport tunnel using the Pseudowire label. In some embodiments, each application stream is associated with a different Pseudowire or Pseudowire label. This can be done by encapsulating the packet based on the application header, such as an TCP, HTTP, or MPEG header. Thus, each application flow is unique to a Pseudowire label. In contrast, some Pseudowires are encapsulated based on IP or layer 2 headers only. In some embodiments, one or more headers associated with layer 4 and above are used to obtain a Pseudowire label for the packet.

FIG. 1C is a flowchart illustrating an embodiment of a process for receiving a data packet at a transit node. For example, this process may be performed at node B or C in FIG. 1A, if an application stream is sent from node A to node D or vice versa. The transit node is sitting between two or more networks that operate with different technologies.

At 130, a data packet is received. For example, at node B, a data packet associated with an application stream is received. For example, the data packet could be a data packet sent at 124 in FIG. 1B. At 132, the data packet is classified based on the Pseudowire label. At 134, a policy is checked based on the Pseudowire label. For example, the transit node interfaces with a policy server to determine where to switch the packet and what kind of service agreement needs to be enforced. At 136, the packet is switched to a pre-established tunnel based on the policy. For example, the packet is switched based on the Pseudowire application label. Further, bandwidth enforcement, and/or traffic shaping may be performed here.

In the case of a transit node, in this example, classification is based on the Pseudowire label only for the purpose of the ease of operation, in contrast to the case of an ingress node, in which classification is based on the application. By checking a policy or interfacing with a policy server, the data packet can be switched based on business policies in addition to (or instead of) just using topology routing to switch the packet.

FIG. 1D is a flowchart illustrating an embodiment of a process for receiving a data packet at a termination or egress node. For example, this process may be performed at node D in FIG. 1A, if an application stream is sent from node A to node D.

At 140, a data packet is received. For example, at node D, a data packet associated with an application stream is received. For example, the data packet could be a data packet sent at 136 in FIG. 1C. At 142, the network layer header is stripped off or removed. At 144, preassigned business operations are performed. For example, QoS, bandwidth enforcement, and/or traffic shaping are performed. The termination node has sufficient security information to prevent denial of service (DoS) attacks as part of a business arrangement.

6

The GIBSON architecture uses Pseudowires to transport data packets over multiple networks; however, it extends the use of the Pseudowire concept as defined in IETF PWE3 WG, to handle upper layer (that is, above IP) applications, such as video and voice. Pseudowires operating with the newly defined extension in operation are referred to as "GIBSON Pseudowires".

The extension is in the method of packet classification. Instead of looking through Layer-1 or Layer-2 headers as IETF PWE3 WG defines Pseudowires, GIBSON Pseudowires search through application headers to identify data flows. In some embodiments, the application information is located above the IP headers.

When an application data flow has been identified, the devices supporting GIBSON architecture will encapsulate all packets that belong to the specific flow in an IP Pseudowire and transport them over the provider network.

FIG. 2 is a diagram illustrating an embodiment of a GIBSON Pseudowire.

In this example, an example Pseudowire is shown, which works as follows: to aggregate data flows over a shared physical or logical tunnel between network edges, the ingress edge node encapsulates a Pseudowire header to the packets. This header consists of a Pseudowire label 206, and a control word 208. At the egress edge node, it may strip off the header, and forward the original packets. Each individual data flow has a unique Pseudowire label 206. The control word 208 can be used for congestion control and OAM purposes. The edge nodes use MPLS signaling protocols to set up Pseudowires over the network.

Some features of Pseudowires include the ability to switch Pseudowires at a network edge, provide QoS and OAM on a per-Pseudowire basis, and support for protection and restoration. For example, IETF PWE3 WG defines some of these features.

Pseudowires have the following characteristics:

Transport agnostic: Pseudowires can transport data traffic over any physical or logical data tunnel which may be IP, MPLS, Ethernet, or optical cross-connection.

IP-Friendly: Pseudowires are provisioned, controlled and operated via IP control plane

Inter-network capable: PWE3 multi-hop (IETF Draft, L. Martini, et al, "Dynamic Placement of Multi Segment Pseudo Wires") and switching (IETF Draft, L. Martini, et al, "Segmented Pseudo Wire") techniques enable providers to provision Pseudowires over multiple intra-domain or inter-domain networks.

VPN capable: Pseudowire has been extended in IETF to create a nested topology for VPN applications, which include VPLS, VPWS and IPLS.

SLA capable: Pseudowire techniques can provide QoS (IETF Draft, L. Martini, et al, "Dynamic Placement of Multi Segment Pseudo Wires"), protection and restoration (IETF Draft, P. Pan, et al, "Pseudowire Protection") and congestion control (IETF Draft, P. Pan, et al, "Pseudowire Congestion Control") functionality on a per-flow basis.

Flow type agnostic: per IETF PWE3 WG, Pseudowires can encapsulate any type of Layer-1 and Layer-2 data flow. Pseudowires can encapsulate Layer-1 flows in SONET/SDH format (the technique is known as Circuit Emulation), Layer-2 flows such as ATM, Frame Relay, PPP and Ethernet, and IP. In some embodiments, all packets within a Pseudowire receive the same packet forwarding treatment throughout the network.

Based on the last point, GIBSON Pseudowires add an application-awareness dimension to Pseudowires. The deployment of new data services may require service pro-

US 9,485,176 B2

7

viders to control and manage user traffic at per-application-stream granularity. An application stream may be encapsulated in RTP for session-based applications such as VoD and VoIP, or in MPEG for multimedia applications.

Multimedia applications may bring an entirely different set of service requirements to provider networks. For example, some applications can tolerate out-of-order packet delivery, some applications can tolerate packet drop, but not delay, and some applications require user traffic to adapt to a change of available link bandwidth, but maintain constant-bit-rate at all times. The existing Layer-2 and Layer-3 QoS mechanisms (IEEE 802.1p or DiffServ) may not be adequate to handle such applications.

To support the new services, GIBSON Pseudowires extend the concept of IETF PWE3 WG Layer-1 and Layer-2 based Pseudowires, and add a new dimension for new applications. GIBSON Pseudowires may include the following attributes:

GIBSON Pseudowires map and aggregate data flows from any layer (i.e., layer 1 to 7). The number of user flows to be aggregated into each Pseudowire depends on the service. For example, for high-bandwidth and long-duration VoD streams, the edge nodes may initiate and maintain one Pseudowire per stream. For low-speed and short-lived VoIP sessions, the edge nodes may aggregate a large number of sessions into a single Pseudowire. Once again, all packets within each Pseudowire may receive the same SLA treatment throughout the network.

At a network border, GIBSON Pseudowires are switched based on business-driven routing. As shown in FIG. 1A, nodes B and C are situated at the border between metro and core networks, and are connected to edge nodes A and B over physical or logical tunnels. When they receive data packets from GIBSON Pseudowires, the Pseudowire traffic is forwarded to other tunnels based on the business bilateral/multilateral agreement.

As shown in FIG. 2, Pseudowire 202 encapsulates data packet 210 based at least in part on layer 1/layer 2 and IP header 212. By contrast, Pseudowire 204 encapsulates data packet 214 based at least in part on application header 216. As a result, Pseudowire 204 is unique to an application stream associated with data packet 214.

Another concept in the GIBSON architecture is the definition of business policy interfacing between the management-plane and network nodes.

In some applications, such as IMS, the user flow and QoS information may be derived from the management plane. The information can be piggybacked by the Pseudowire-initiating GIBSON-enabled devices into the setup messages. The transit network nodes may use this information for routing. Another alternative is to store the QoS information on each provider's Router Servers.

FIG. 7 is a block diagram illustrating an embodiment of the operation of GIBSON-based Pseudowire routing. Network 702 is an example of GIBSON-based policy server network 108.

There are two types of routing in this example: business-based, and topology-based. Business-based routing is conducted between service providers 704-708. As shown here, providers 1, 2 and 3 define the business routing constraints from their inter-provider bilateral or multilateral agreement. Through the management-plane, the business routing constraints may be downloaded to Route Servers 710-714 within each provider network. Thus, a centralized policy is distributed to multiple GIBSON endpoints.

An example Router Server can be the one defined and studied in IETF PCE WG. It is to combine business routing

8

constraints and network internal topology and resource information, and compute the optimal path between network edges.

In the context of GIBSON, it does not define the messaging protocols between the management-plane and network nodes. Rather, GIBSON defines the content of the business policies and how they are processed on network nodes.

In FIG. 7, there may be multiple routers and switches between GIBSON Endpoints A-D. After mapping the data flow into Pseudowires, GIBSON Endpoint A may interface with Route Server E to find a suitable path to GIBSON Endpoint B. On transit GIBSON Endpoint C, it may again interface with Route Server F for the optimal path to reach GIBSON Endpoint D. This is how inter-domain GIBSON Pseudowires are established in some embodiments.

There are two groups of policies:

(a) The pre-negotiated business policies among providers 704-707, which include application-level policies and inter-provider policies.

(b) The internal network engineering (such as routing) policies within each provider 704-707

The eventual policies received by GIBSON nodes A-D are a combination of (a) and (b) above.

An example of an interprovider bilateral policy is the following:

For traffic going two Providers A and Provider B,

All voice traffic must traverse through Provider C with the following constraints:

(i) via a pre-established data tunnel Ethernet-Connection-X

(ii) the maximum bandwidth for the voice traffic is 150 Mbps

(iii) the maximum number of simultaneous voice session is 5,000

(iv) a small amount of packet loss, in the range of 0.3-0.5% of the total traffic, is permitted in case of network congestion, however, all packets must not experience any queuing delay during transmission due to the delay-sensitive nature of voice traffic

(v) the above criteria always applies to bi-directional traffic

All video traffic must traverse through Provider D with the following constraints:

(i) via a pre-established optical tunnel DWDM-Connection-Y

(ii) the maximum bandwidth for the video traffic is 20 Gbps

(iii) the maximum number of simultaneous video session is 5,000

(iv) some packet delay, in the range of 50-200 msec, is permitted in case of network congestion, however, no packet can be dropped throughout the transmission due to the loss sensitivity of video traffic

(v) the above criteria only applies to uni-directional traffic

An example of an application policy at node A is the following:

For video flow from YouTube (IP address=1.2.3.4), with RIP session information of source port=10, destination port=20,

(i) transmit packets to Node B through Pseudowire with a specifically allocated Pseudowire label

(ii) use at most 10 Mbps from 1:00 am to 4:00 pm, after which release all network resources including bandwidth and Pseudowire labels

US 9,485,176 B2

9

(iii) to transport through the provider networks, use the interprovider policy and direct the traffic through DWDM-Connection-Y (see above interprovider policy example)

Upon the reception of the policies, the GIBSON-enabled network nodes will apply the policies in its packet classification and QoS, as described previously.

FIG. 3 is a diagram illustrating an embodiment of a GIBSON architecture. In the example shown, GIBSON endpoints (or GIBSON-Enabled Nodes) 302-308 are devices that are responsible for processing user data flows by interfacing with a GIBSON-based policy server network. Between GIBSON endpoints, there can be one or multiple networks. GIBSON endpoints always operate at a network edge and/or border.

Interfaces in the GIBSON architecture are indicated by S1, S2, S3, S4, and S5. S1 is an access interface, S2 is a data aggregation interface, S3 is a Pseudowire routing interface, S4 is a Pseudowire termination interface, and S5 is a multipoint transport interface. In some embodiments, in GIBSON-enabled networks, all data flows, best-effort or otherwise, are provisioned and established through the interface with a GIBSON-based policy server network.

FIG. 4 is a diagram illustrating an embodiment of a GIBSON S1 interface. In the example shown, GIBSON Endpoints 302 and 306 aggregate user flows from service access devices 310 and 312. The service access devices 310 and 312 may include a wide range of equipment including IP DSLAM, PON, SONET/SDH MSPP and wireless base-stations. The service access devices 310 and 312 do not need to be fully IP routing capable. They are efficient in supporting the services that they are designed for in some embodiments.

In various embodiments, service access devices 310 and 312 can deliver user flows in any native format (such as Ethernet VLAN and IP). Upon the reception of user flows from service access devices, GIBSON endpoints 302 and 306 classify the incoming traffic based on application criteria provided from the management-plane.

For example, two service devices 310 and 312 have established an IMS session via SIP. To provide service guarantees, the GIBSON Endpoints 302 and 306 may read the IP source and destination address, and UDP source and destination port numbers for each incoming packet, and match theca against customer flow policies. If there is a match, GIBSON Endpoint 302 or 306 may encapsulate the packet with a Pseudowire header, and forward it over a pre-established Pseudowire. Each Pseudowire is provisioned with the SLA parameters provided by the management-plane.

FIG. 5 is a block diagram illustrating an embodiment of a GIBSON S2 interface. Between two GIBSON endpoints 302 and 304, user data flows are encapsulated as Pseudowires and aggregated into transport tunnels according to the criteria provided from the management-plane.

Each GIBSON Pseudowire may consist of multiple user data flows. As an example, multiple VoIP calls (all in RTP) going between two GIBSON endpoints may share the same Pseudowire header. In this case, the GIBSON Pseudowire may be over-provisioned with a fixed bandwidth, which is computed based on call arrival and departure distribution at the business level, and downloaded to the GIBSON endpoints via the management plane. This may be a good technique to transport a large number of short-lived voice calls over packet networks with service guarantees. This can potentially reduce the number of control-plane messages during call setup.

10

Each transport tunnel may aggregate multiple GIBSON Pseudowires. The transport tunnel could be any type preferred by service providers. In addition, GIBSON supports the nesting of Pseudowires so that Pseudowires can be used to create transport tunnels that transit multiple lower-level tunnel technologies. See the description on "virtual segments" below.

The Pseudowire aggregation process may be bounded by the business policies distributed via the management-plane. The policies may determine the allocation of Pseudowires into transport tunnels, and the modification of transport tunnels to accommodate Pseudowire network resource consumption.

FIG. 6 is a block diagram illustrating an embodiment of a GIBSON S3 interface. Within the network, the intermediate GIBSON endpoints 302, 304, and 306 may terminate the transport tunnels, and switch the Pseudowires into another set of tunnels toward their destination. At GIBSON Pseudowire setup time, each Pseudowire request message may carry information such as QoS, protection and congestion control data and user flow information.)

FIG. 8 is a block diagram illustrating an embodiment of a GIBSON S4 interface. When interfacing with non-GIBSON-enabled nodes, the GIBSON endpoints may terminate the Pseudowires and forward the original user's traffic. If the network between GIBSON and Non-GIBSON Endpoints does not have per-flow service guarantees, the service providers may be notified about partial service guarantees on data flows, flow information carried at Pseudowire setup time may permit the terminating process to map the flow correctly onto the egress network.

A GIBSON Pseudowire termination is a routable entity in GIBSON, so traffic can be routed onto a transport tunnel for delivery to the location where that tunnel terminates, using the nested Pseudowire property of GIBSON that is analogous to nested LSPs or the ATM VCI/VPI hierarchy. Disclosed is an additional enhancement to GIBSON to facilitate the definition of a set of GIBSON Pseudowires as a virtual segment.

A virtual segment is a collection of GIBSON Pseudowires that operate as a transport subnetwork. The virtual segment is bounded by GIBSON endpoints, and at these endpoints the services of the subnetwork are uniformly available. This virtual segment is treated as a GIBSON segment, so that traffic can be routed onto it. When the GIBSON virtual segment is addressed as a hop in a GIBSON Pseudowire, the routing logic may resolve the request to the nearest GIBSON endpoint on-ramp to the virtual segment.

GIBSON virtual segments can enclose any of the following:

1. A network of GIBSON Pseudowires.
2. A network of MPLS LSPs or other tunnels.
3. A multipoint network based on 2547bis (IETF RFC 4364, E. Rosen, et al, "BGP/MPLS IP Virtual Private Networks (VPNs)") or other multipoint technologies.

The last option is more fully described below.

FIG. 9 is a block diagram illustrating an embodiment of a GIBSON S5 interface. In some embodiments, GIBSON supports natural multipoint service behavior by enveloping the multipoint technology as a virtual segment. GIBSON Pseudowires routed to the multipoint virtual segment may be forwarded to the nearest on-ramp (a GIBSON endpoint), where the outer GIBSON envelope may be stripped and the GIBSON endpoint destination address may be decoded from the header. The packet may then be forwarded to the GIBSON endpoint destination using the multipoint technology of the virtual segment. At that endpoint, a GIBSON

US 9,485,176 B2

11

header may be added and the Pseudowire may continue as though the tunnel was continuous, but no Pseudowire meshing may be required within the virtual segment.

The GIBSON endpoints can interface with the management-plane to discover network topology. In turn, it can use a VPN mechanism, such as the ones used in MPLS, to construct point-to-multipoint VPN networks. Note that the Pseudowire is not multipoint in itself, but it can be routed over a multipoint transport process.

FIGS. 10-12 are block diagrams illustrating an embodiment of an example user case for IMS. The GIBSON architecture can apply to a number of services. As shown in FIG. 1, it can provide service guarantees for multimedia applications in a heterogeneous networking environment. In this example, an example using an IMS application is presented.

IMS uses SIP for end-to-end session setup. Each Session can be a VoIP call, a VoD session or a text messaging connection. The default data transport protocol is RTP. One of the characteristics of SIP-based communication is that the control-plane is out-of-band. As a result, media traffic may take a path that is completely different from the one taken by SW control messages. In some networks, service providers cannot control the media traffic other than forwarding them as IP packets, and rely on DiffServ for QoS.

Since VoIP traffic does not require much bandwidth and is well behaved (mostly CBR), service providers do not need to be overly concerned about end-to-end service guarantees. However, for high-volume broadband customers, video stream service guarantee may become important.

How GIBSON can provide service guarantees for SIP-based data traffic is presented.

The following steps correspond to FIGS. 10-12.

1. Initially, GIBSON Endpoints in Networks 1, 2 and 3 may set up transport tunnels among each other. The transport tunnels are either initiated by the management-plane or by the network operators. In the latter case, the tunnel information may be reported to the management-plane.

2. Through the management-plane, the networks may exchange resource and topology information. The information may only be specific and relevant to the services that the network owners have agreed to support.

3. Access networks 1 and 3 have their own IMS (a.k.a. IMS domains). Through the management-plane, the IMS may populate the database (e.g. HSS) with relevant network resource information.

4. The end users in both networks may negotiate multimedia sessions via CSCF. During session negotiation, network resource availability may become one of the key parameters. If there are not enough resources between Networks 1, 2 and 3 for a particular session, CSCF may reject the session.

5. When the sessions have been established, IMS may notify the management-plane about the session data flow information (that is, RTP session).

6. The management-plane exchanges network resource information among each other.

7. The management-plane downloads the data flow information to the GIBSON Endpoints in Networks 1 and 3.

8. In transit network 2, the management-plane may compute the routes from Networks 1 and 3, and download the routing information to the GIBSON Endpoint. The route computation algorithm is governed by the service itself, which may override a SPP/BGP path computation. Further, the management-plane is not necessarily the right place for route computation. As described before, the management-plane may interface with Route Servers for such tasks.

12

9. The GIBSON Endpoints in Networks 1 and 3 may setup Pseudowires for the session media flow. The Pseudowire type depends on the application itself. In this case, a GIBSON Endpoint may choose IP as the Pseudowire type.

10. When Pseudowire setup messages arrive at Network 2, the GIBSON Endpoints may use pre-installed policy routes to direct the Pseudowires toward Network 3.

11. When end-user data traffic in Networks 1 and 3 arrive at the GIBSON Endpoints, they may be mapped to the corresponding Pseudowires. In this case, the GIBSON Endpoints may classify each packet based on its IP source and destination address, and LOP source and destination port numbers, all of which have been downloaded from the management-plane in Step (7).

In this case, two levels of admission control may take place. At the control-plane, management-plane provides network resource information to IMS, which may result in call admission control at SIP setup time. At the data-plane, management-plane provides per-session flow information to GIBSON Endpoints, which may aggregate each user flow in the form of a Pseudowire to transport tunnels.

As a result, data flows may have QoS guarantees throughout the network.

Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

What is claimed is:

1. A method, comprising:

encapsulating, by a first node device of a first network associated with a first service provider identity, a data packet with a pseudowire label determined based on an application flow specified by an application header of the data packet; and

selecting, based on the application flow, a routing policy from a set of application-specific routing policies defined for the first network, wherein the routing policy specifies that the data packet is to traverse at least a second network, comprising a second node device and associated with a second service provider identity, in transit to a third network comprising a third node device and associated with a third service provider identity.

2. The method of claim 1, further comprising:

selecting, by the first node device, a pseudowire spanning the first network and the third network and corresponding to the pseudowire label, and

sending, by the first node device, the data packet via the pseudowire.

3. The method of claim 2, wherein the selecting comprises selecting the pseudowire from a set of pseudowires associated with respective different application flows including the application flow.

4. The method of claim 1, wherein the first network and the third network are associated with respective different network technologies, and at least one of the respective different network technologies comprises at least one of an Ethernet technology, a multiprotocol label switching technology, a provider backbone bridging/provider backbone transport technology, or an optical technology.

5. The method of claim 1, further comprising facilitating, by the first node device, a determination of the application flow specified by the application header in response to determining that the data packet satisfies a business policy associated with the first service provider identity.

US 9,485,176 B2

13

6. The method of claim 5, further comprising receiving information defining the business policy from a server device associated with the first service provider identity.

7. The method of claim 1, further comprising receiving, as the data packet, at least one of a voice data packet, an audio data packet, or a video data packet.

8. The method of claim 1, wherein the encapsulating comprises encapsulating the data packet in response to a determination that the pseudowire label has not been established for the application flow.

9. A system, comprising:

a processor, coupled to a memory that stores instructions, that executes or facilitates execution of the instructions to at least:

encapsulate a data packet, received by a first node device of a first network associated with a first service provider entity, with a pseudowire label determined based on an application flow identified by an application header of the data packet; and

select, based on the application flow, a routing policy from a set of application-specific routing policies defined for the first network, wherein the routing policy instructs that the data packet is to traverse at least a second network, comprising a second node device and associated with a second service provider entity, in transit to a third network comprising a third node device and associated with a third service provider entity.

10. The system of claim 9, wherein the processor further executes or facilitates execution of the instructions to send the data packet via a pseudowire corresponding to the pseudowire label and spanning the first network and the third network.

11. The system of claim 10, wherein the processor further executes or facilitates execution of the instructions to select the pseudowire from a plurality of pseudowires associated with respective different application flows including the application flow.

12. The system of claim 10, wherein the routing policy specifies a maximum bandwidth for voice data traffic via the pseudowire.

13. The system of claim 9, wherein at least one of the first network or the third network comprises at least one of an Ethernet technology, a multiprotocol label switching technology, a provider backbone bridging/provider backbone transport technology, or an optical technology.

14. The system of claim 9, wherein the processor further executes or facilitates execution of the instructions to initiate a determination of the application flow identified by the

14

application header in response to a determination that the data packet satisfies a business policy associated with the first service provider entity.

15. The system of claim 14, wherein the processor further executes or facilitates execution of the instructions to receive information specifying the business policy from a server device associated with the first service provider identity.

16. The system of claim 9, wherein the processor further executes or facilitates execution of the instructions to receive, as the data packet, at least one of a voice data packet, an audio data packet, or a video data packet.

17. The system of claim 9, wherein the processor further executes or facilitates execution of the instructions to encapsulate the data packet with the pseudowire label in response to a determination that the pseudowire label has not been established for the application flow.

18. A non-transitory computer-readable medium comprising instructions that, in response to execution, cause a first node device, which comprises a processor and is part of a first network associated with a first service provider identity, to perform operations, the operations comprising:

encapsulating a data packet with a pseudowire label determined based on an application flow specified by an application header of the data packet; and

determining, based on the application flow, a routing policy from multiple application-specific routing policies defined for the first network, wherein the routing policy specifies that the data packet is to traverse at least a second network, comprising a second node device and associated with a second service provider identity, in transit to a third network comprising a third node device and associated with a third service provider identity.

19. The non-transitory computer-readable medium of claim 18, the operations further comprising:

selecting a pseudowire spanning the first network and the third network and corresponding to the pseudowire label, and

sending the data packet via the pseudowire.

20. The non-transitory computer-readable medium of claim 19, wherein the selecting comprises selecting the pseudowire from a set of pseudowires associated with respective different application flows including the application flow.

* * * * *

EXHIBIT C



US010735320B2

(12) **United States Patent**
Pan et al.

(10) **Patent No.: US 10,735,320 B2**(45) **Date of Patent: *Aug. 4, 2020**(54) **APPLICATION WIRE**(71) Applicant: **Global Innovation Aggregators LLC.**,
Pasadena, CA (US)(72) Inventors: **Ping Pan**, San Jose, CA (US); **Richard D. Gitlin**, Little Silver, NJ (US)(73) Assignee: **K.Mizra LLC**, Los Angeles, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/536,103**(22) Filed: **Aug. 8, 2019**(65) **Prior Publication Data**

US 2019/0363980 A1 Nov. 28, 2019

Related U.S. Application Data

(63) Continuation of application No. 15/838,014, filed on Dec. 11, 2017, now Pat. No. 10,411,999, which is a continuation of application No. 14/919,687, filed on Oct. 21, 2015, now Pat. No. 9,843,509, which is a continuation of application No. 14/055,721, filed on (Continued)

(51) **Int. Cl.****H04L 29/06** (2006.01)**H04L 12/721** (2013.01)**H04L 12/701** (2013.01)**H04L 12/723** (2013.01)

(Continued)

(52) **U.S. Cl.**CPC **H04L 45/68** (2013.01); **H04L 45/00** (2013.01); **H04L 45/38** (2013.01); **H04L 45/50** (2013.01); **H04L 45/74** (2013.01); **H04L 47/24** (2013.01); **H04L 65/1013** (2013.01); **H04L 69/22** (2013.01)(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited****U.S. PATENT DOCUMENTS**

5,920,705 A 7/1999 Lyon et al.

6,167,051 A 12/2000 Nagami et al.

(Continued)

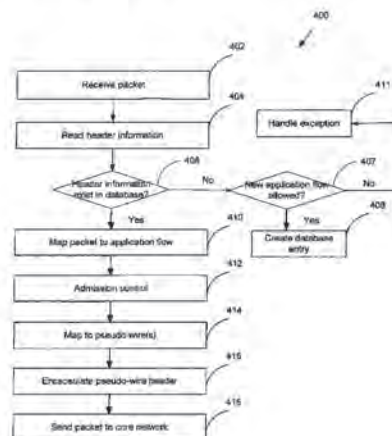
OTHER PUBLICATIONS

Allerton, Thomas S. et al., Ethernet Transport over Wide Area Networks.

(Continued)

Primary Examiner — Brandon M Renner(74) *Attorney, Agent, or Firm* — Kinney & Lange, P.A.(57) **ABSTRACT**

A method includes, at a node associated with a multiprotocol label switching system (MPLS) network, identifying information associated with an application flow based on one or more unencapsulated packet headers of the application flow or based on an ingress data stream that includes the application flow. The method further includes, in response to identifying the information, and based on stored data that maps application flows with pseudowires, determining a number of pseudowires corresponding to paths through the MPLS network, where the stored data indicates, for a sending device application, a distributed mapping of the application flow via at least one of the number of pseudowires, and communicating data related to the sending device application via at least one of the number of pseudowires.

20 Claims, 9 Drawing Sheets

US 10,735,320 B2

Page 2

Related U.S. Application Data

- Oct. 16, 2013, now Pat. No. 9,197,675, which is a continuation of application No. 11/543,727, filed on Oct. 5, 2006, now Pat. No. 8,588,061.
- (60) Provisional application No. 60/725,038, filed on Oct. 7, 2005.

(51) Int. Cl.

H04L 12/741 (2013.01)

H04L 12/851 (2013.01)

(56) References Cited

U.S. PATENT DOCUMENTS

- 6,347,088 B1 2/2002 Katou et al.
 6,430,184 B1 8/2002 Robins et al.
 6,477,166 B1 11/2002 Sanzi et al.
 6,546,427 B1 4/2003 Ehrlich et al.
 6,574,477 B1 6/2003 Rathunde
 6,621,793 B2 9/2003 Widegren et al.
 6,665,273 B1 12/2003 Goguen et al.
 6,680,943 B1 1/2004 Gibson et al.
 6,751,684 B2 6/2004 Owen et al.
 6,813,271 B1 11/2004 Cable
 6,845,389 B1 1/2005 Sen et al.
 6,985,488 B2 1/2006 Pan et al.
 7,050,396 B1 5/2006 Cohen et al.
 7,200,104 B2 4/2007 Saleh et al.
 7,436,782 B2 10/2008 Ngo et al.
 7,590,070 B1 9/2009 Asawa et al.
 7,697,528 B2 4/2010 Parry et al.
 9,843,509 B2 12/2017 Pan et al.
 2001/0021175 A1 9/2001 Haverinen
 2001/0023453 A1 9/2001 Sundqvist
 2001/0043603 A1 11/2001 Yu
 2002/0112072 A1 8/2002 Jain
 2002/0141393 A1 10/2002 Eriksson et al.
 2002/0146026 A1 10/2002 Unitt et al.
 2003/0002482 A1 1/2003 Kubler et al.
 2003/0039237 A1 2/2003 Forslow
 2003/0117950 A1 6/2003 Huang
 2004/0105459 A1 6/2004 Mannam
 2004/0114595 A1 6/2004 Doukai
 2004/0133692 A1 7/2004 Blanchet et al.
 2004/0156313 A1 8/2004 Hofmeister et al.
 2004/0174865 A1 9/2004 O'Neill
 2004/0252717 A1 12/2004 Solomon et al.
 2005/0018605 A1 1/2005 Foote et al.
 2005/0044262 A1 2/2005 Luo
 2005/0080890 A1 4/2005 Yang et al.
 2005/0080911 A1 4/2005 Stiers et al.
 2005/0093770 A1* 5/2005 de Bonet G06F 13/387
 345/10
 2005/0220148 A1 10/2005 Delregno et al.
 2005/0237927 A1 10/2005 Kano et al.
 2005/0259586 A1 11/2005 Hafid et al.
 2006/0002423 A1 1/2006 Rembert et al.
 2006/0018252 A1 1/2006 Sridhar et al.
 2006/0046658 A1 3/2006 Cruz et al.
 2006/0047851 A1 3/2006 Voit et al.
 2006/0090008 A1 4/2006 Guichard et al.
 2006/0146832 A1 7/2006 Rampal et al.
 2006/0227767 A1 10/2006 Johnson et al.

- 2006/0233167 A1 10/2006 McAllister et al.
 2007/0038921 A1 2/2007 Pekonen et al.
 2007/0053366 A1 3/2007 Booth et al.
 2007/0070893 A1 3/2007 Butenweg et al.
 2007/0127479 A1 6/2007 Sinicrope et al.
 2007/0206607 A1 9/2007 Chapman et al.
 2008/0031129 A1 2/2008 Arseneault et al.
 2008/0144632 A1 6/2008 Rabie et al.

OTHER PUBLICATIONS

- Afferton, Thomas S. et al., Ethernet Transport over Wide Area Networks, Packet-Aware Transport for Metro Networks, IEEE Communications Magazine, pp. 120-127, Mar. 2004.
- Anderson, L. et al., LDP Specification, Network Working Group, Jan. 2001.
- Blake et al., "An Architecture for Differentiated Services," Network Working Group, Dec. 1998.
- Braden et al., "Integrated Services in the Internet Architecture: an overview," Network Working Group, Jun. 1994.
- Bryant et al., "Pseudo wire Emulation Edge-to-Edge (PWE3) Architecture," Network Working Group, Mar. 2005.
- Harry Newton, "Newton's Telecom Dictionary", 23rd Updated and Expanded Edition, p. 825,p. 239, Flatiron Publishing, New York, Mar. 2007.
- International Search Report for PCT Application Serial No. PCT/US2006/039257, dated Apr. 18, 2007, 2 pgs. Final Office Action dated Mar. 9, 2010 for U.S. Appl. No. 11/543,727, 17 pages.
- Martini, L. et al., Pseudowire Setup and Maintenance using the Label Distribution Protocol (LDP), Network Working Group, Apr. 2006.
- Martini, Luca et al., Dynamic Placement of Multi Segment Pseudo Wires, PWE3 Working Group, Jun. 2006.
- Martini, Luca et al., Encapsulation Methods for Transport of Ethernet over MPLS Networks, Network Working Group, Apr. 2006.
- Martini, Luca et al., Internet Draft, Segmented Pseudo Wire, Network Working Group, Jul. 2007.
- Martini, Luca et al., Pseudowire Setup and Maintenance using LDP, Network Working Group, Mar. 2005.
- Martini, Luca, et al., Encapsulation Methods for Transport of Frame Relay Over Ethernet over MPLS Networks, Network Working Group, Feb. 2006.
- McPherson et al., Pseudowire Emulation Edge to Edge (PWE3) Jun. 13, 2007.
- Metz, Chris et al., Pseudowire Attachment Identifiers for Aggregation and VPN Autodiscovery, PWE3 Working Group, Feb. 25, 2006.
- Pan, P. et al., Internet Draft, Pseudo Wire Protection, Jul. 2006.
- Pan, Ping, Internet Draft, Dry-Martini: Supporting Pseudo-wires in Sub-IP Access Networks, Network Working Group, Jul. 2005.
- Rosen, E. et al., BGP-MPLS IP Virtual Private Networks (VPN), Network Working Group, Feb. 2006.
- Rosen, Eric C. et al., Internet Draft, PWE3 Congestion Control Framework, Network Working Group, Mar. 2004.
- Shah, Flimianshu et al., Internet Draft, ARP Mediation for IP Interworking of Layer 2 VPN, L2VPN Working Group, Jul. 2007.
- Theimer, T. et al., "Requirements for OAM Functionality in MPLS", Oct. 1999, Watersprings.
- Vasseur, et al., Path Computation Element (pce), May 9, 2007, <http://www.ietf.org/html.charters/pce charter.html>.

* cited by examiner

U.S. Patent

Aug. 4, 2020

Sheet 1 of 9

US 10,735,320 B2

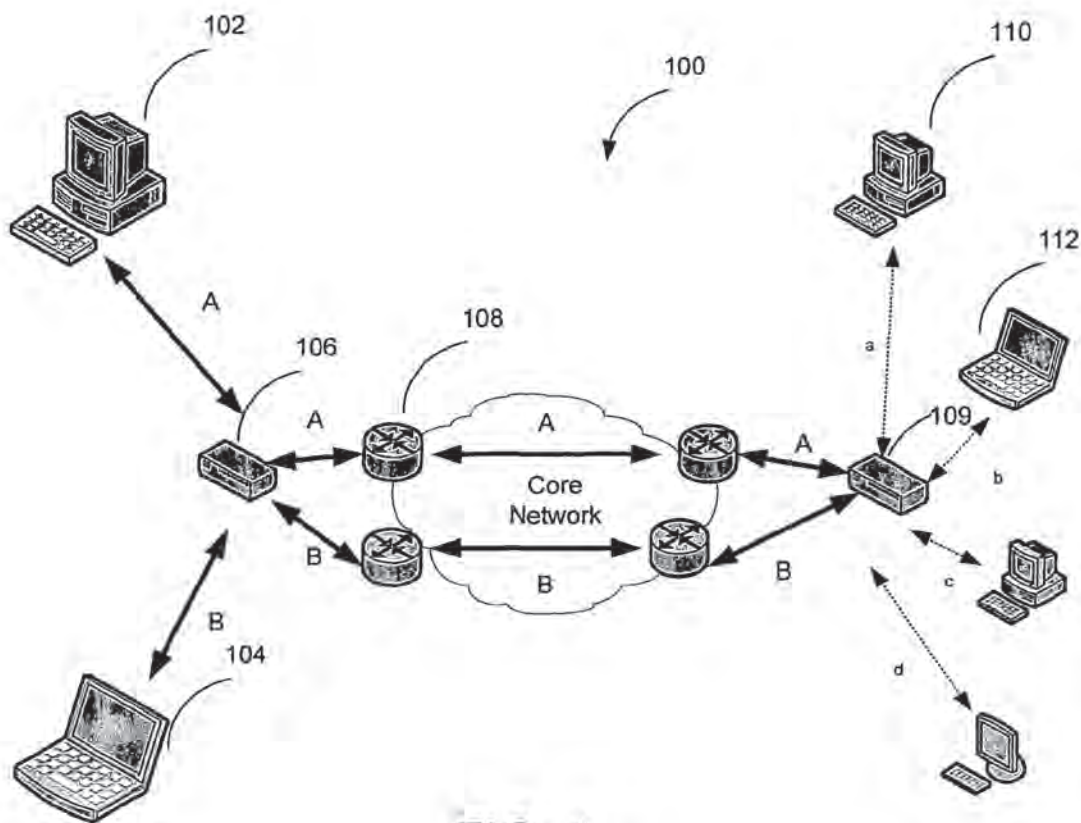


FIG. 1

U.S. Patent

Aug. 4, 2020

Sheet 2 of 9

US 10,735,320 B2

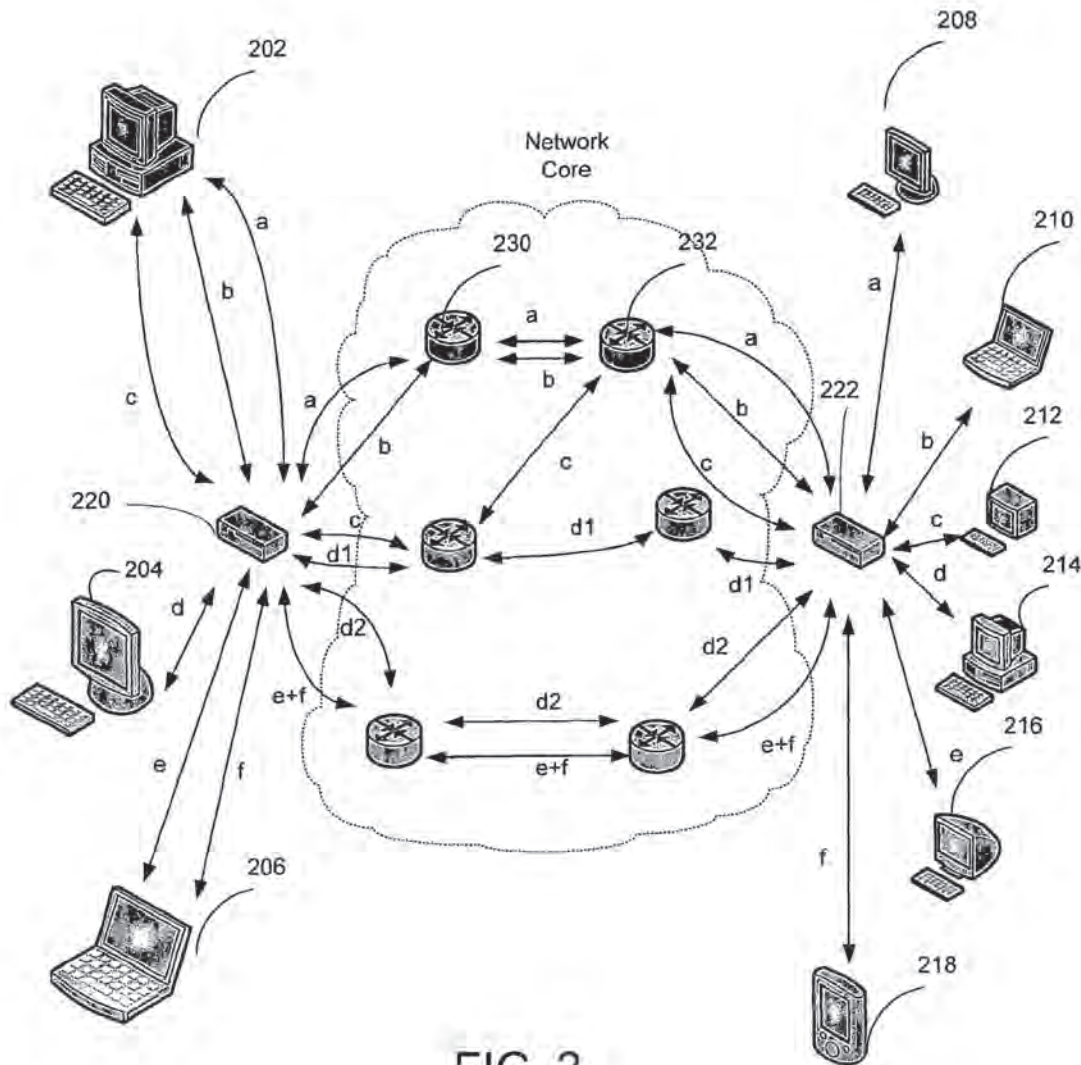


FIG. 2

U.S. Patent

Aug. 4, 2020

Sheet 3 of 9

US 10,735,320 B2

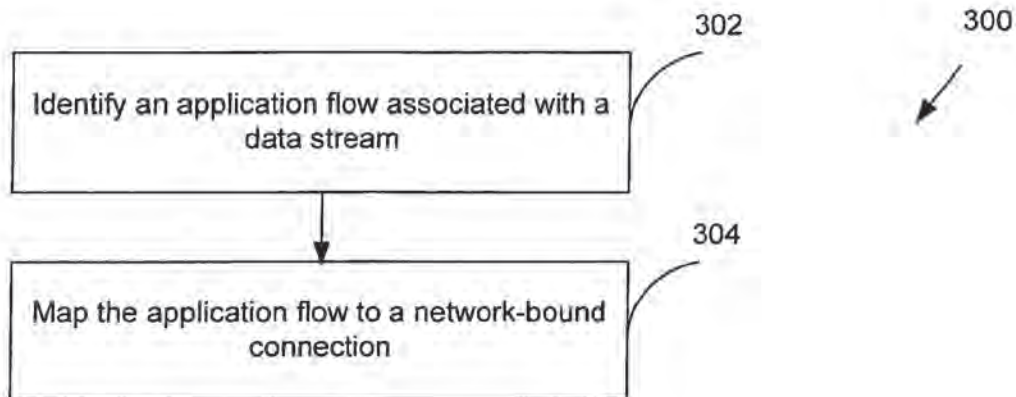


FIG. 3

U.S. Patent

Aug. 4, 2020

Sheet 4 of 9

US 10,735,320 B2

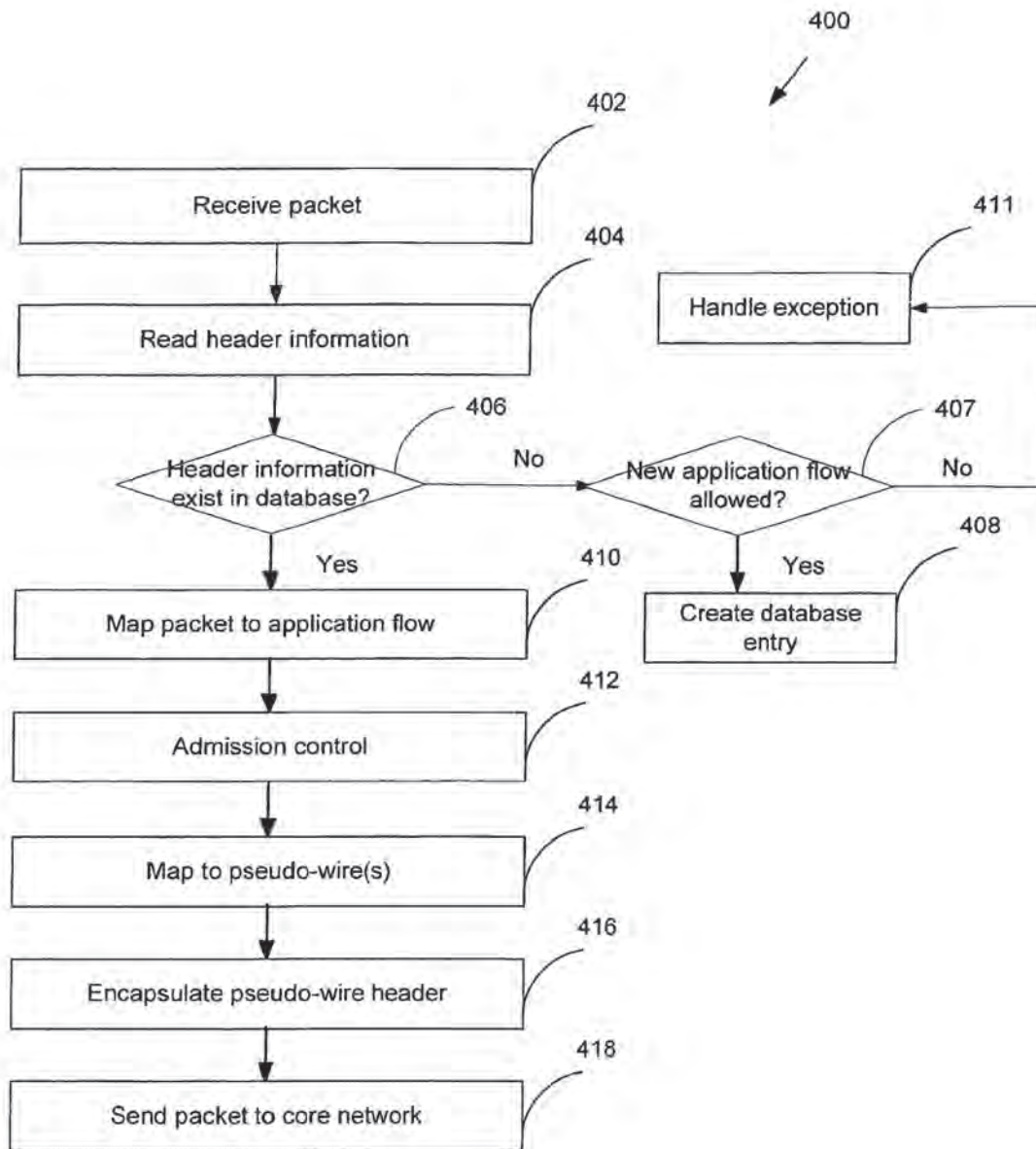


FIG. 4

U.S. Patent

Aug. 4, 2020

Sheet 5 of 9

US 10,735,320 B2

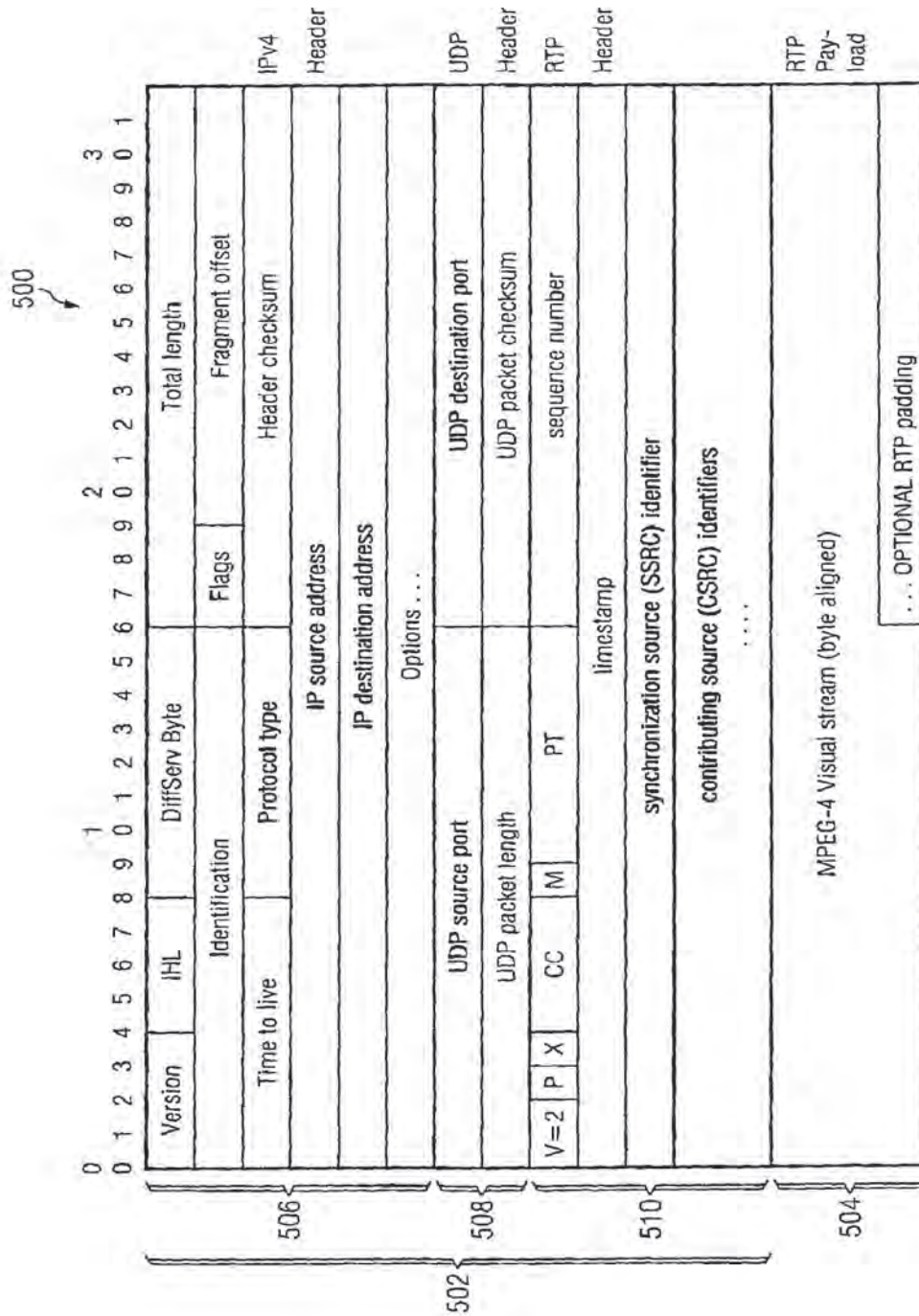


FIG. 5

U.S. Patent

Aug. 4, 2020

Sheet 6 of 9

US 10,735,320 B2

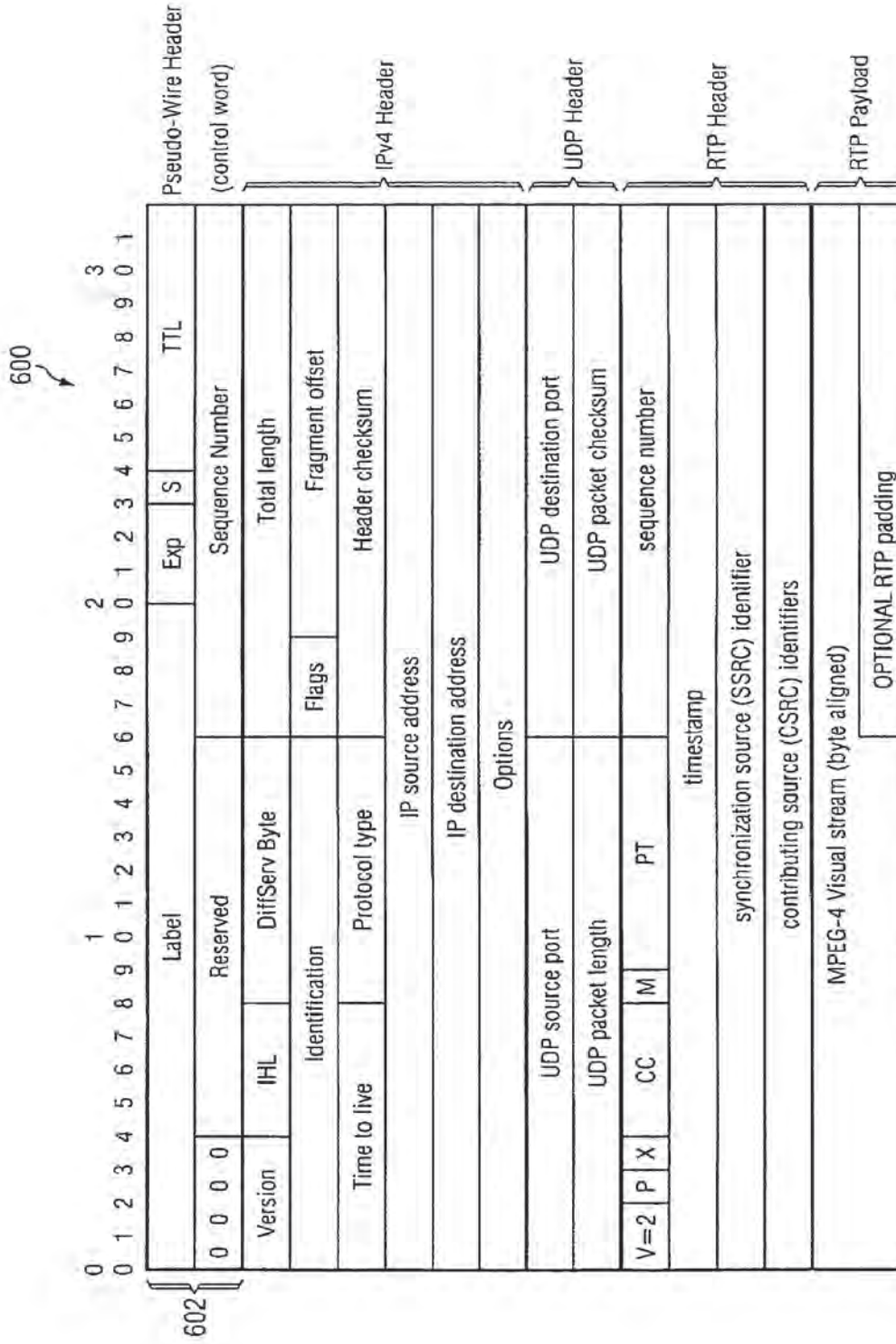


FIG. 6

U.S. Patent

Aug. 4, 2020

Sheet 7 of 9

US 10,735,320 B2

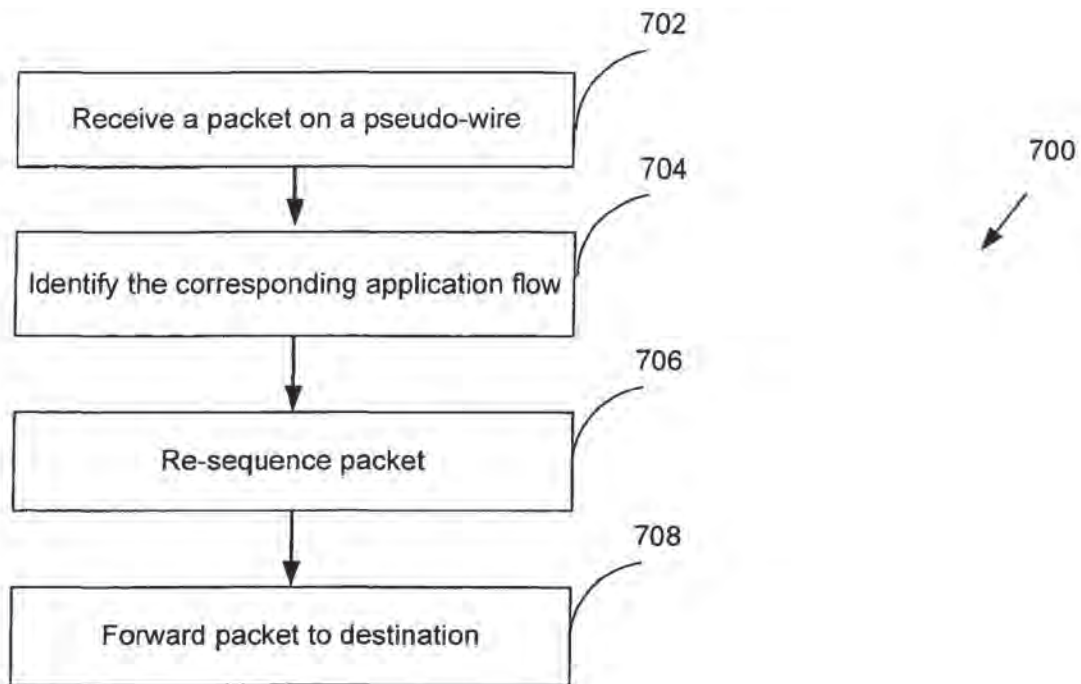


FIG. 7

U.S. Patent

Aug. 4, 2020

Sheet 8 of 9

US 10,735,320 B2

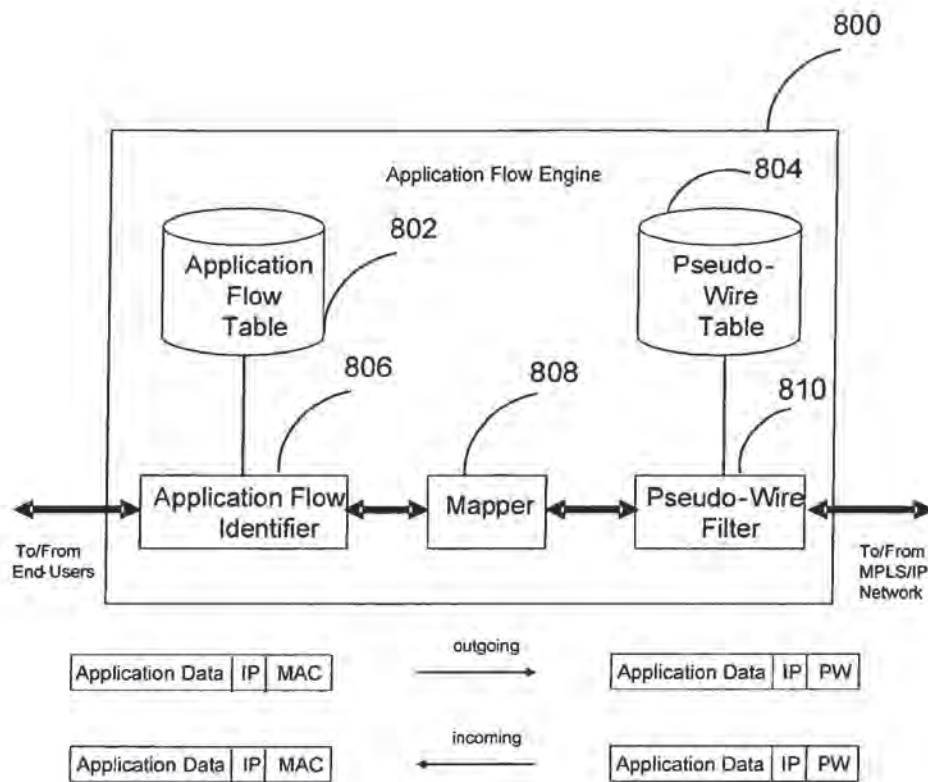


FIG. 8

U.S. Patent

Aug. 4, 2020

Sheet 9 of 9

US 10,735,320 B2

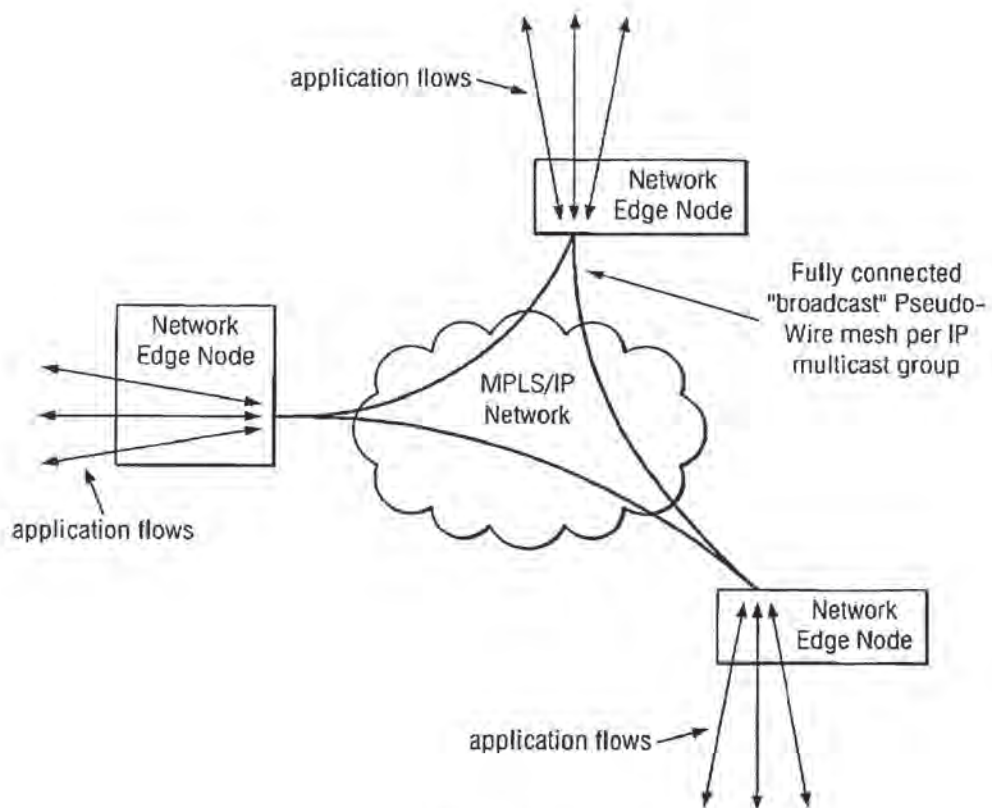


FIG. 9

US 10,735,320 B2

1

APPLICATION WIRE

CROSS REFERENCE TO OTHER APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 15/838,014, filed Dec. 11, 2017, and entitled "Application Wire," which is a continuation of U.S. patent application Ser. No. 14/919,687, filed Oct. 21, 2015, and entitled "Application Wire," which is a continuation of U.S. patent application Ser. No. 14/055,721, filed Oct. 16, 2013, and entitled "Application Wire," which is a continuation of U.S. patent application Ser. No. 11/543,727, filed Oct. 5, 2006, and entitled "Application Wire," which claims priority to U.S. Provisional Application No. 60/725,038, filed Oct. 7, 2005 and entitled "Application wire: mapping application streams to pseudo-wires." The entireties of these related applications are incorporated herein by reference.

BACKGROUND OF THE INVENTION

In recent years, network service providers have been upgrading and managing networks based on Multi Protocol Label Switching (MPLS) technology. MPLS has been deployed in most backbone networks. MPLS provides capabilities such as Quality of Service (QoS), redundancy, Operations Administration and Maintenance (OAM), and Virtual Private Network (VPN). MPLS is typically used to provision and manage data streams at individual flow levels. Each flow is known as a Label Switched Path (LSP). Existing MPLS systems typically handle data traffic at the Layer-3 (IP) level and below.

Some MPLS networks use Pseudowires to map Open System Interconnections (OSI) Layer-1 or Layer-2 traffic flows into "virtual circuits." A Pseudowire refers to the emulation of a Layer-1 or Layer-2 native service over a network. Examples of native services include Asynchronous Transfer Mode (ATM), Frame Relay, Ethernet Virtual Local Area Network (VLAN), Time Division Multiplexing (TDM), Synchronous Optical Network (SONET), Synchronous Digital Hierarchy (SDH), etc. In the control plane, the Pseudowires are maintained and managed using a simplified version of Label Distribution Protocol (LDP), the Target LDP. Each Pseudowire is associated with an MPLS label for packet forwarding and a control word for flow management.

Since existing MPLS networks only allow Layer-1 or Layer-2 connections to be mapped to Pseudowires in a one-to-one mapping, the system typically cannot guarantee the QoS for individual applications that generate application data in Layer-3 or above. QoS behavior in the application layer is sometimes different from the behavior in Layer-1 or Layer-2. For example, packet video streams can generally tolerate out-of-sequence delivery, and packet voice traffic can sometimes tolerate packet loss but is sensitive to packet delay. Existing Layer-1 and Layer-2 systems, however, typically do not address network-level QoS for these voice and video applications.

Some proposed IP-based models have been developed to address the QoS requirement associated with applications, but some issues remain. For example, the IntServ/RSVP model identifies connections by applications based on the IP addresses of the source and destination, the protocol type, and the protocol's source and destination port number (together known as the 5-tuple). Each connection is required to comply with a number of service parameters such as bandwidth consumption and delay budget. As a result, the intermediate nodes (such as the core routers) are required to

2

store the identity of all the connections, perform deep packet inspection, and implement extensive QoS mechanisms to satisfy the service parameters for each flow. Network service providers tend to find this model limiting because it is not very scalable as the number of users grow.

The DiffServ model addresses the scalability problems associated with the IntServ/RSVP model. Instead of handling QoS on a per flow basis, the user applications are classified into a small number of uniformly defined traffic classes. Each data packet stores its traffic class information in its IP header. At each intermediate node, the packet receives appropriate QoS treatment according to its traffic class. Since DiffServ provides relative QoS, in order to guarantee QoS to a particular flow, the model typically requires the network bandwidth to be over-provisioned. Further, the model only incorporates a subset of available QoS technology, such as priority queuing and Random Early Discard (RED) in dealing with temporary traffic congestion. The model is often not applicable in networks where physical links cannot be sufficiently over-provisioned.

It would be useful to have a way to better manage application traffic over a carrier network without requiring changes to the intermediate nodes. It would also be desirable if QoS guarantee can be achieved at per-application flow level. Furthermore, the solution should be scalable.

BRIEF DESCRIPTION OF THE DRAWINGS

Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

FIG. 1 is a system diagram illustrating an example of an MPLS based network supporting Pseudowires.

FIG. 2 is a system diagram illustrating an example of a network supporting Application Wires.

FIG. 3 is a flowchart illustrating an embodiment of a process for transferring data.

FIG. 4 is a flowchart illustrating another embodiment of a process for handling ingress data streams.

FIG. 5 is a diagram illustrating the format of a Real Time Protocol (RTP) packet example.

FIG. 6 is a diagram illustrating an example of a Pseudowire encapsulated MPEG-4 packet.

FIG. 7 is a flowchart illustrating an embodiment of a process for handling data traffic in the egress direction.

FIG. 8 is a block diagram illustrating an embodiment of an application flow engine.

FIG. 9 is a diagram illustrating an example of a multicast environment supporting Application Wires.

DETAILED DESCRIPTION

The invention can be implemented in numerous ways, including as a process, an apparatus, a system, a composition of matter, a computer readable medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or communication links. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. A component such as a processor or a memory described as being configured to perform a task includes both a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. In general, the order of the steps of disclosed processes may be altered within the scope of the invention.

US 10,735,320 B2

3

A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

Transferring data over a network using Application Wires is disclosed. An Application Wire refers to the emulation of a virtual circuit or a transparent wire for transferring one or multiple application flows. An Application Wire maps one or more application flows into Pseudowires, and is at the same time aware of the application protocol and the protocol requirements associated with the application flows. As used herein, an application flow refers to a set of packets exchanged between two or more devices for accomplishing a specific function. Application flow data includes data associated with Layer-4 or above as defined by the OSI protocol stack. In some embodiments, an application flow includes data packets transmitted and received by an application, such as a Voice over IP (VoIP) session, instant messaging, Video-on-Demand (VoD), etc. The application may be configured to operate on various wired, wireless, or hybrid devices. The interface between the application and the underlying network is provided by protocols such as the Session Initialization Protocol (SIP) and the Real-time Transport Protocol (RTP). From the perspective of the application, transferring data over an Application Wire has the same effect as transferring data over a dedicated wire. As will be shown in more detail below, in some embodiments, Application Wires are formed by mapping application flows to Pseudowires.

FIG. 1 is a system diagram illustrating an example of an MPLS based network supporting Pseudowires. In this example, client devices such as 102 and 104 reside on an edge network and transfer data to an edge device (also referred to as an edge node) 106. The edge node, for example an edge router, supports MPLS and is capable of mapping Layer-1 and Layer-2 data streams into Pseudowires. Each data stream is mapped to a single Pseudowire in a one-to-one mapping. Each packet in the Pseudowire is encapsulated with an MPLS label for forwarding, and includes a control word for flow management. The edge device forwards the packet to a core network that includes core routers such as 108. The core network is compatible with MPLS and IP. The end user traffic flows are mapped to Pseudowires and then fed to the core network. The Pseudowires are maintained throughout the core network. The Pseudowires terminate at edge node 109, which receives the Pseudowire traffic and forwards the packets to their appropriate destinations such as devices 110 and 112. Traffic from devices such as 110 and 112 to devices such as 102 and 104 is processed similarly.

Since the mapping of one data stream to one Pseudowire does not account for the bandwidth demand of individual applications generating traffic on the client devices, it is often difficult to guarantee the quality of service (QoS) for these individual applications. For example, assuming that Pseudowires A and B each support a data rate of 50 Mbps,

4

and that the application executing on device 102 require 70 Mbps of bandwidth while the application on device 104 only requires 20 Mbps. Because of the one-to-one mapping, the bandwidth requirement of device 102 is not met by Pseudowire, even though there is excess capacity on the network overall.

Application Wires improve on the Pseudowire scheme described above. FIG. 2 is a system diagram illustrating an example of a network supporting Application Wires. In this example, client devices 202-206 are configured to communicate with client devices 208-218 in the following manner: device 202 communicates with devices 208, 210, and 212; device 204 with device 214; device 206 with devices 216 and 218. Specifically, one or more applications executing on each client device send data to and receive data from applications executing on other client devices. Application flows a-f are shown between devices 202-206 and 208-218.

At the edge of the core network, edge nodes 220 and 222 are configured to transfer the data streams between a core network (such as a backbone network of a service provider) and the client devices. As used herein, data traffic is said to be in the ingress direction if it is being transferred from client devices to the core network, and in the egress direction if it is being transferred from the core network to clients devices. A data connection that transfers data in the ingress direction is referred to as a network-bound connection. Depending on the direction of the data flow, an edge node may be referred to as an ingress node or an egress node.

As will be shown in more detail below, the edge nodes map the application flows into Pseudowires in the ingress direction. A number of mapping schemes are possible, such as a one-to-one mapping, a distributed mapping where an application flow is mapped to multiple Pseudowires, or an aggregated mapping where multiple flows are mapped to a single Pseudowire. In the example shown, application flows a and b are one-to-one mapped to a separate Pseudowire each, application flow d is distributed to Pseudowires d1 and d2, and application flows e and f are aggregated to a single Pseudowire (e+f). The mapping scheme for each application flow is selected based at least in part on the bandwidth and traffic requirement associated with the application. In the egress direction, packets transferred on the Pseudowires are reassembled to the corresponding application flows and sent to the appropriate destinations. Each Pseudowire may span a plurality of intermediate nodes such as core routers 230 and 232. Unlike data transfer schemes where deep packet inspection is required at each intermediate node, the intermediate nodes used in this example can be standard MPLS devices and no change is required to make them support the Application Wire scheme.

FIG. 3 is a flowchart illustrating an embodiment of a process for transferring data. Process 300 may be implemented on an edge node and can be used to process data streams in the ingress direction. In this example, the process initiates by identifying an application flow associated with a data stream being transferred over the network (302). Depending on the data stream, there may be one or more application flows within the same data stream. The identification may be achieved, for example, by inspecting the headers of the packets in the data stream. Further details of the identification process are discussed below. Once identified, the application flow is mapped to one or more network-bound connections such as Pseudowires (304) in accordance with the requirements of the application, forming one or more Application Wires.

FIG. 4 is a flowchart illustrating another embodiment of a process for handling ingress data streams. Process 400 may

US 10,735,320 B2

5

be implemented on an edge node. In this example, process 400 initiates when a data packet is received (402). The header information of the received packet is read (404). The header information is used to identify the application flow. For purposes of example, it is assumed that the data stream carries IP data and that the data packet is an IP packet. Other types of data can be processed similarly based on the corresponding header formats. In this example, the IP packet includes a Layer-2 MAC header having fields such as the Ethernet addresses of the source and the destination. The IP packet further includes higher layer headers such as Layer-4 application protocol headers. The combination of various headers is used to identify specific application flows.

It is useful to inspect an example of a packet to understand how the application flow identification is done. FIG. 5 is a diagram illustrating the format of a Real Time Protocol (RTP) packet example, Packet 500 shown in the example is an MPEG-4 packet. It includes a header portion 502 and a payload portion 504. The header portion includes a Layer-3 (IPv4) header 506, and Layer-4 headers which in this case include UDP header 508 and RTP header 510. Several fields from each of the headers are extracted to provide information useful for identifying the application flow, including the IP source address and IP destination address, protocol type (which is UDP in this example), UDP source port, UDP destination port, synchronization source (SSRC) identifier, and contributing source (CSRC) identifier. Some of the fields are optional in some embodiments. Other types of applications such as Voice over IP or instant messaging can be identified using a similar technique, although different headers and fields may be used.

Returning to FIG. 4, the header information associated with the packet is looked up in a database of application flows (406). If the header information is not found in the database, it is determined whether a new application flow can be created based on the header information (407). If so, a new entry that includes information identifying the new application flow is created in the application flow database (408). If a new application flow cannot be created, the packet is discarded and appropriate error handling such as event logging is optionally performed. New application flows are disallowed in some embodiments where the system is configured to only allow pre-configured application flows.

If, however, the header information is found in the database, the packet is mapped to an application flow (410). Admission control is optionally performed on the flow (412). In various embodiments, admission control includes shaping traffic by changing the packets priority, applying a policy/rule, tagging, dropping the packet, etc. If the packet is not dropped by admission control, it is mapped to one or more Pseudowires configured to service the application flow (414). In some embodiments, a database of available Pseudowires is searched to find one or more suitable Pseudowires for carrying the application flow. The mapping is based on, among other things, IP routing or manual configuration.

As previously discussed, the mapping of application flow to Pseudowire may be one-to-one, N-to-one, or one-to-N. One-to-one mapping is the most straightforward. Sometimes multiple application flows are aggregated into a single flow (N-to-one). Aggregation is appropriate when, for example, the application flows are similar and have the same priority level. Sometimes, an application flow is distributed into multiple streams and transferred over the network via multiple Pseudowires (one-to-N). For example, a large flow exceeding a certain data rate threshold may be split into several Pseudowires to better utilize the available band-

6

width. The division of the application flow into multiple streams is based at least in part on application-specific parameters. For example, a large RTP stream is sometimes split based on SSRC or pay-load frame type. In one example, an application flow involves a large RTP stream having a large amount of MPEG traffic over a network without any per flow QoS guarantee. To reduce the impact of dropped packets, the more important packets such as M-frames in the application flow are separated from the rest. The important packets are mapped to a Pseudowire with a higher priority level. The rest of the packets are mapped to one or more lower priority Pseudowires.

Returning to FIG. 4, once the appropriate Pseudowire for sending the packet is determined, the packet is encapsulated with a Pseudowire header (416) and sent to the core MPLS/IP network (418). FIG. 6 is a diagram illustrating an example of a Pseudowire encapsulated MPEG-4 packet. In this example, a Pseudowire header 602 is pre-pended to packet 600. The Pseudowire header includes packet label information, which has the same format as the of an MPLS packet. In addition to the label information, several other fields are updated to provide information useful for the Application Wire. The sequence number field is used to keep packets in the application flow in the correct order. Ingress packets are assigned sequence numbers in the order they are received by the edge node. The EXP field is used to store service differentiation information such as priority level. The differentiation information is encoded according to the Internet Engineering Task Force (IETF)'s Request For Comments (RFC) 3270. The differentiation information, which is derived based on the service parameters associated with the application flow, gives service providers greater control over service quality for individual flows. In some embodiments, the reserved field in the control word is used for functions such as OAM (e.g. the VCCV function), service guarantee, protection, and flow control.

Since the resulting packet is an MPLS formatted packet, it can be processed by any intermediate nodes on the network (e.g. network routers and switches) as a regular MPLS packet. So long as the intermediate node is a standard MPLS enabled device, no modification is required of the device for processing an Application Wire related packet.

FIG. 7 is a flowchart illustrating an embodiment of a process for handling data traffic in the egress direction. Process 700 may be implemented on an edge node on the termination end of a Pseudowire. In this example, process 700 initiates when a packet is received on a Pseudowire (702). The application flow that corresponds to the Pseudowire is identified (704). In some embodiments, the identification is accomplished by looking up in a database that maps Pseudowires to application flows. In the event that the Pseudowire is configured to carry more than one application flow, the packet header is further inspected to locate the matching application flow.

Since it is possible for packets sent on different Pseudowires to arrive out of order, the packets are re-sequenced as appropriate (706). In some embodiments, the re-sequencing includes re-sequencing at the Pseudowire level. The sequence number field in the Pseudowire header is examined and used to sort the packets in the appropriate sequence. In some embodiments, the re-sequencing includes an application flow level re-sequencing. Application header and/or payload information is used to sort packets belonging to the same application flow in the appropriate order. For example, the SSRC and the sequence numbers in the RTP header, as well as the payload data are used in some embodiments to re-sequence an RTP flow. Once re-se-

US 10,735,320 B2

7

quenced, the Pseudowire header of the packet is removed and the packet is forwarded to its destination (708).

In some embodiments, processes 300, 400 and 700 are carried out by an application flow engine (AFE). FIG. 8 is a block diagram illustrating an embodiment of an application flow engine. In this example, AFE 800 is included in an edge node device. The components of the AFE may be implemented as software, firmware, hardware or a combination thereof. The AFE is configured to send data streams from the client devices to the core network as well as to receive data streams from the network designated for client devices on the edge network.

When handling ingress data streams, the AFE identifies and maps application flows in the data streams to a plurality of Pseudowires. The application flows are denoted as $F = \{f.sub.1, f.sub.2, \dots, f.sub.n\}$ and the Pseudowires are denoted as $W = \{w.sub.1, w.sub.2, \dots, w.sub.m\}$. An application flow identifier 806 identifies new application flows in the data stream, and stores information associated with the application flows in a database labeled as an application flow table (AFT) 802. The AFT is also used to identify data packets that match application flows already stored in the AFT. Information stored in the AFT includes, among other things, flow identification information and service parameters. The flow identification information includes attributes used to identify the specific application flow and may vary depending on the application. For example, for an RTP-based application flow, the corresponding IP source and destination addresses, UDP protocol type, UDP source and destination port number, SSRC and CSRC are recorded in the AFT. Examples of the service parameters include various measured or assigned characteristics, such as the average and peak bandwidth of the flow, the burst size, the importance level of the flow (for example, emergency 911 traffic is assigned the highest importance and can preempt other flows at runtime), sub-flow information such as the bandwidth and importance levels associated with different sources, as well as other application dependent information such as whether to allow out-of-sequence packets in the flow. In some embodiments, at least a part of the AFT is populated ahead of time by the service provider. For example, the service parameters may be manually configured or populated using a configuration file when the system is initialized. Having a pre-populated AFT allows the service providers to offer different levels of services, and/or provide QoS guarantee based on subscription.

In FIG. 8, a mapper 808 maps incoming data packets to appropriate application flows if possible, and optionally performs admission control functions on the data flows. The mapper also maps each application flow to one or more Pseudowires based on information stored in a Pseudowire table (PWT) 804. A Pseudowire filter 810 encapsulates the packets with Pseudowire headers. The encapsulated packets are sent to the core network.

In some embodiments, the PWT maintains the network-bound Pseudowires, $W = \{w.sub.1, w.sub.2, \dots, w.sub.m\}$. For each Pseudowire, the following attributes are stored in one example: MPLS label for in packet encapsulation, QoS information indicating the level of QoS to be applied to the Pseudowire, Protection Path information identifying one or more backup Pseudowires used to protect this Pseudowire, OAM capability information used for error detection and loop-back, Multicast grouping information such as group ID used to transport multicast traffic over the MPLS/IP network.

When handling egress data streams, a process similar to 700 is carried out by the AFE. The PWT is used to look up

8

the application flows that correspond to the packets received on various Pseudowires. The mapper re-sequences the packets, removes the Pseudowire headers, and forwards the packets to the destination.

The Application Wire techniques described above are also applicable for environments in which multimedia streams are multicast to multiple sites in the network. To support multicast over Application Wires, a fully-meshed Pseudowire network for each multicast group is set up. Various mechanisms for supporting Pseudowire based multicast can be used, including Virtual Private LAN Service (VPLS) and IP LAN Service (IPLS).

FIG. 9 is a diagram illustrating an example of a multicast environment supporting Application Wires. In the example shown, application flow mapping is performed at any given network edge node, and a copy of the data packet is forwarded to all the other edge nodes in the group. In some embodiments, a packet is transmitted following these steps: for an application flow, $f.sub.i.sup.G$, that belongs to a multicast group, G , the PWT is searched and the adjacencies (i.e., the other edge nodes of the group denoted as $A.sub.b.k.sup.G, A.sub.k+1.sup.G, \dots$) are obtained. A copy of the data packet is sent to each adjacency. Between a pair of edge nodes (i.e., one adjacency), there may be multiple Pseudowires, $A.sub.k.sup.G = \{w.sub.j.sup.G, w.sub.j+1.sup.G, \dots\}$. As described above, an application flow may be split among the Pseudowires, according to application-specific parameters.

On an egress network edge node, the Pseudowire headers of the packets are removed, the packets are reassembled and/or re-sequenced as necessary, and forwarded to the destination. Any IP or Layer-2 multicast scheme may be used to forward the packets to a destination beyond the network edge nodes.

An Application Wire based data transfer technique has been described. The technique gives service providers greater flexibility in providing services based on applications, without requiring changes to intermediate devices.

Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

What is claimed is:

1. A method comprising:

at a node associated with a multiprotocol label switching system (MPLS) network, performing:

identifying information associated with an application flow based on one or more unencapsulated packet headers of the application flow or based on an ingress data stream that includes the application flow;

in response to identifying the information, and based on stored data that maps application flows with pseudowires, determining a plurality of pseudowires corresponding to paths through the MPLS network, wherein the stored data indicates, for a sending device application, a distributed mapping of the application flow via at least one of the plurality of pseudowires; and communicating data related to the sending device application via at least one of the plurality of pseudowires.

2. The method of claim 1, wherein the stored data defines an application wire for use by the sending device application, the application wire configured to communicate par-

US 10,735,320 B2

9

particular data from a particular application flow of the sending device application to an edge node.

3. The method of claim 1, wherein the stored data further defines an application wire for use by the sending device application, the application wire configured to communicate particular data from an edge node through the MPLS network via the plurality of pseudowires.

4. The method of claim 1, wherein each of the plurality of pseudowires extends from the application flow in an ingress direction into the MPLS network.

5. The method of claim 1, wherein each of the plurality of pseudowires is virtually coupled between a particular device and a particular application being executed at a particular client device.

6. The method of claim 1, wherein the application flow includes data packets transmitted and received by the sending device application, wherein the data is communicated via the at least one of the plurality of pseudowires, and further comprising assigning, at an edge node, sequence numbers to ingress data packets in an order in which they are received by the node.

7. The method of claim 1, wherein the stored data maps the application flow to the plurality of pseudowires to create an application wire.

8. A device comprising:

a processor; and

a memory that stores instructions executable by the processor to:

identify information associated with an application flow based on one or more unencapsulated packet headers of the application flow or based on an ingress data stream that includes the application flow;

in response to identifying the information, and based on stored data mapping application flows to pseudowires, determine a plurality of pseudowires as paths through a multiprotocol label switching (MPLS) network for the application flow, wherein the stored data indicates, for a sending device application, a distributed mapping of the application flow via at least one of the plurality of pseudowires; and communicate data associated with the sending device application via at least one of the plurality of pseudowires.

9. The device of claim 8, wherein the stored data defines an application wire for use by the sending device application, the application wire configured to communicate particular data from a particular application flow of the sending device application to an edge node.

10. The device of claim 8, wherein the stored data further defines an application wire for use by the sending device application, the application wire configured to communicate particular data from an edge node through the MPLS network via the plurality of pseudowires.

11. The device of claim 8, wherein each of the plurality of pseudowires extends from the application flow in an ingress direction into the MPLS network.

10

12. The device of claim 8, wherein each of the plurality of pseudowires is virtually coupled between a particular device and a particular application being executed at a particular client device.

13. The device of claim 8, wherein:

the application flow includes data packets transmitted and received by the sending device application,

the data is communicated via the at least one of the plurality of pseudowires, and the instructions are executable by the processor to cause assigning, at an edge

node, of sequence numbers to ingress data packets in an order in which they are received by the node.

14. The device of claim 8, wherein the stored data maps the application flow to the plurality of pseudowires to create an application wire.

15. A computer-readable non-transitory medium storing instructions that are executable by a processor to initiate or perform:

identifying information associated with an application flow based on one or more unencapsulated packet headers of the application flow or based on an ingress data stream that includes the application flow;

in response to identifying the information, and based on stored data that maps application flows with pseudowires, determining a plurality of pseudowires corresponding to paths through a multiprotocol label switching system (MPLS) network, wherein the stored data indicates, for a sending device application, a distributed mapping of the application flow via at least one of the plurality of pseudowires; and

communicating data related to the sending device application via at least one of the plurality of pseudowires.

16. The computer-readable non-transitory medium of claim 15, wherein the instructions are executable to perform the identifying, the determining, and the communicating at a node associated with the MPLS network.

17. The computer-readable non-transitory medium of claim 15, wherein the stored data defines an application wire for use by the sending device application, the application wire configured to communicate particular data from a particular application flow of the sending device application to an edge node.

18. The computer-readable non-transitory medium of claim 15, wherein the stored data further defines an application wire for use by the sending device application, the application wire configured to communicate particular data from an edge node through the MPLS network via the plurality of pseudowires.

19. The computer-readable non-transitory medium of claim 15, wherein each of the plurality of pseudowires extends from the application flow in an ingress direction into the MPLS network.

20. The computer-readable non-transitory medium of claim 15, wherein each of the plurality of pseudowires is virtually coupled between a particular device and a particular application being executed at a particular client device.

* * * * *

EXHIBIT D



Ciena Corporate Headquarters

Attn: Mr. Raymond Gabriel, Sr. Intellectual Property Counsel

7035 Ridge Road

Hanover, Maryland 21076

Tel: 410-694-5700

Email: rgabriel@ciena.com

February 13, 2024

Re: K.Mizra LLC

Dear Mr. Gabriel,

I hope this letter finds you well. As you should be aware K.Mizra LLC ("K.Mizra") owns and licenses portfolios of patents, including portfolios that cover various aspects of pseudowire technology such as those made and used in Ciena products and is sold by Ciena Inc ("Ciena") and its affiliates.

This letter serves as notice to Ciena that Ciena's products have and are continuing to infringe various claims of K.Mizra's patents. Attached are sample claim charts and other evidence of use showing infringement by exemplary Ciena product.

See attached:

US 9,485,176 B2 patent vs. Ciena Blue Planet

US 10,735,320 B2 patent vs Ciena Blue Planet

US 8,782,282 B1 patent vs Ciena Blue Planet

US 8,213,311 B2 patent vs Ciena Blue Planet

US 9,749,249 B2 patent vs. Ciena Blue Planet

US 8,018,880 B2 patent vs. Ciena 5160

US 8,949,381 B1 patent vs. Ciena MCP

US 8,385,355 B1 patent vs. Ciena MCP

US 9,444,733 B2 patent vs. Ciena 3926

CHARLES HAUSMAN, CEO

Email: Chausman@kmizra.com

Mailing Address: 777 Brickell Ave #500-96031, Miami, FL 33131

US 7,535,895 B2 patent vs. Ciena 6500 PTS

US 9,264,354 B2 patent vs. Ciena 5142

US 7,609,621 B1 patent vs. Ciena 6500 PTS

US 7,899,916 B1 patent vs. Ciena 5144

These claim charts are by no means exhaustive of Ciena's infringing conduct, and K.Mizra believes that numerous additional Ciena products/features and K.Mizra patents are at issue.

K.Mizra has previously reached favorable resolutions regarding its portfolio with many multinational companies. In all matters, K.Mizra's preference is to regularize the activities of the infringing party through amicable licensing agreements rather than litigation.

We believe it is imperative that Ciena and K.Mizra reach a mutually agreeable resolution concerning Ciena's infringement of K.Mizra's patent portfolio. Please contact me to initiate licensing discussions.

Thank you for your prompt attention to this matter and I look forward to speaking with you soon.

Sincerely,



Chuck Hausman, Esq.

CEO



Mailing address: 777 Brickell Ave #500-96031, Miami, FL 33131



Ciena Corporate Headquarters

Attn: Mr. Robert Kucler, VP of Intellectual Property

7035 Ridge Road

Hanover, Maryland 21076

Tel: 410-694-5700

Email: rkuc1er@ciena.com

February 13, 2024

Re: K.Mizra LLC

Dear Mr. Kucler,

I hope this letter finds you well. As you should be aware K.Mizra LLC ("K.Mizra") owns and licenses portfolios of patents, including portfolios that cover various aspects of pseudowire technology such as those made and used in Ciena products and is sold by Ciena Inc ("Ciena") and its affiliates.

This letter serves as notice to Ciena that Ciena's products have and are continuing to infringe various claims of K.Mizra's patents. Attached are sample claim charts and other evidence of use showing infringement by exemplary Ciena product.

See attached:

US 9,485,176 B2 patent vs. Ciena Blue Planet

US 10,735,320 B2 patent vs Ciena Blue Planet

US 8,782,282 B1 patent vs Ciena Blue Planet

US 8,213,311 B2 patent vs Ciena Blue Planet

US 9,749,249 B2 patent vs. Ciena Blue Planet

US 8,018,880 B2 patent vs. Ciena 5160

US 8,949,381 B1 patent vs. Ciena MCP

US 8,385,355 B1 patent vs. Ciena MCP

US 9,444,733 B2 patent vs. Ciena 3926

CHARLES HAUSMAN, CEO

Email: Chausman@kmizra.com

Mailing Address: 777 Brickell Ave #500-96031, Miami, FL 33131

US 7,535,895 B2 patent vs. Ciena 6500 PTS

US 9,264,354 B2 patent vs. Ciena 5142

US 7,609,621 B1 patent vs. Ciena 6500 PTS

US 7,899,916 B1 patent vs. Ciena 5144

These claim charts are by no means exhaustive of Ciena's infringing conduct, and K.Mizra believes that numerous additional Ciena products/features and K.Mizra patents are at issue.

K.Mizra has previously reached favorable resolutions regarding its portfolio with many multinational companies. In all matters, K.Mizra's preference is to regularize the activities of the infringing party through amicable licensing agreements rather than litigation.

We believe it is imperative that Ciena and K.Mizra reach a mutually agreeable resolution concerning Ciena's infringement of K.Mizra's patent portfolio. Please contact me to initiate licensing discussions.

Thank you for your prompt attention to this matter and I look forward to speaking with you soon.

Sincerely,



Chuck Hausman, Esq.

CEO



Mailing address: 777 Brickell Ave #500-96031, Miami, FL 33131

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

K.Mizra LLC

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Folio Law Group PLLC
1200 Westlake Ave. N. Ste. 809, Seattle, WA, (206) 880-1802

DEFENDANTS

Ciena Corporation

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question
(U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity
(Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State | ☐ 1 | ☐ 1 | Incorporated or Principal Place of Business In This State | ☐ 4 | ☐ 4 |
| Citizen of Another State | ☐ 2 | ☐ 2 | Incorporated and Principal Place of Business In Another State | ☐ 5 | ☐ 5 |
| Citizen or Subject of a Foreign Country | ☐ 3 | ☐ 3 | Foreign Nation | ☐ 6 | ☐ 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance ☐ 120 Marine ☐ 130 Miller Act ☐ 140 Negotiable Instrument ☐ 150 Recovery of Overpayment & Enforcement of Judgment ☐ 151 Medicare Act ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans) ☐ 153 Recovery of Overpayment of Veteran's Benefits ☐ 160 Stockholders' Suits ☐ 190 Other Contract ☐ 195 Contract Product Liability ☐ 196 Franchise	PERSONAL INJURY ☐ 310 Airplane ☐ 315 Airplane Product Liability ☐ 320 Assault, Libel & Slander ☐ 330 Federal Employers' Liability ☐ 340 Marine ☐ 345 Marine Product Liability ☐ 350 Motor Vehicle ☐ 355 Motor Vehicle Product Liability ☐ 360 Other Personal Injury ☐ 362 Personal Injury - Medical Malpractice PERSONAL INJURY ☐ 365 Personal Injury - Product Liability ☐ 367 Health Care/Pharmaceutical Personal Injury Product Liability PERSONAL PROPERTY ☐ 370 Other Fraud ☐ 371 Truth in Lending ☐ 380 Other Personal Property Damage ☐ 385 Property Damage Product Liability	☐ 625 Drug Related Seizure of Property 21 USC 881 ☐ 690 Other LABOR ☐ 710 Fair Labor Standards Act ☐ 720 Labor/Management Relations ☐ 740 Railway Labor Act ☐ 751 Family and Medical Leave Act ☐ 790 Other Labor Litigation ☐ 791 Employee Retirement Income Security Act IMMIGRATION ☐ 462 Naturalization Application ☐ 465 Other Immigration Actions	☐ 422 Appeal 28 USC 158 ☐ 423 Withdrawal 28 USC 157 PROPERTY RIGHTS ☐ 820 Copyrights ☒ 830 Patent ☐ 835 Patent - Abbreviated New Drug Application ☐ 840 Trademark SOCIAL SECURITY ☐ 861 HIA (1395ff) ☐ 862 Black Lung (923) ☐ 863 DIWC/DIWW (405(g)) ☐ 864 SSID Title XVI ☐ 865 RSI (405(g)) FEDERAL TAX SUITS ☐ 870 Taxes (U.S. Plaintiff or Defendant) ☐ 871 IRS—Third Party 26 USC 7609	☐ 375 False Claims Act ☐ 376 Qui Tam (31 USC 3729(a)) ☐ 400 State Reapportionment ☐ 410 Antitrust ☐ 430 Banks and Banking ☐ 450 Commerce ☐ 460 Deportation ☐ 470 Racketeer Influenced and Corrupt Organizations ☐ 480 Consumer Credit ☐ 485 Telephone Consumer Protection Act ☐ 490 Cable/Sat TV ☐ 850 Securities/Commodities/Exchange ☐ 890 Other Statutory Actions ☐ 891 Agricultural Acts ☐ 893 Environmental Matters ☐ 895 Freedom of Information Act ☐ 896 Arbitration ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision ☐ 950 Constitutionality of State Statutes
REAL PROPERTY ☐ 210 Land Condemnation ☐ 220 Foreclosure ☐ 230 Rent Lease & Ejectment ☐ 240 Torts to Land ☐ 245 Tort Product Liability ☐ 290 All Other Real Property	CIVIL RIGHTS ☐ 440 Other Civil Rights ☐ 441 Voting ☐ 442 Employment ☐ 443 Housing/Accommodations ☐ 445 Amer. w/Disabilities - Employment ☐ 446 Amer. w/Disabilities - Other ☐ 448 Education PRISONER PETITIONS Habeas Corpus: ☐ 463 Alien Detainee ☐ 510 Motions to Vacate Sentence ☐ 530 General ☐ 535 Death Penalty Other: ☐ 540 Mandamus & Other ☐ 550 Civil Rights ☐ 555 Prison Condition ☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District (specify) ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
35 U.S.C. § 271

Brief description of cause:
Patent Infringement

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE _____

DOCKET NUMBER _____

DATE

11/25/2024

SIGNATURE OF ATTORNEY OF RECORD

/s/ Scott P. Amy

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
 United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.