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

MONARCH NETWORKING SOLUTIONS LLC **Plaintiff,** **v.** **CISCO SYSTEMS, INC.; CHARTER COMMUNICATIONS, INC.** **Defendants.**	§ § § § § § § § § § § § § §	**Civil Action No. _________** **Jury Trial Requested**

COMPLAINT FOR PATENT INFRINGEMENT

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff, Monarch Networking Solutions LLC ("Monarch"), for its Complaint against Defendants Cisco Systems, Inc. ("Cisco") and Charter Communications, Inc. ("Charter"), requests a trial by jury and alleges as follows upon actual knowledge with respect to itself and its own acts and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. This is an action for patent infringement. Monarch alleges that Cisco infringes U.S. Patent Nos. 8,451,844 ("the '844 Patent"), 8,451,845 ("the '845 Patent"), 9,019,965 ("the '965 Patent"), and 8,130,775 ("the '775 Patent"), (collectively, the "Asserted Patents"), copies of which are attached hereto as Exhibits A-D. In addition, Monarch alleges that Charter infringes the '844 and '845 Patents.

2. Monarch alleges that Cisco directly and indirectly infringes the Asserted Patents by making, using, offering for sale, selling and/or importing the Cisco Accused Products described below. Monarch further alleges that Cisco induces the infringement of other third parties, including Charter, through their use of the Cisco Accused Products as directed by Cisco. Monarch seeks damages and other relief for Cisco's infringement of the Asserted Patents.

3. Monarch alleges that Charter directly and indirectly infringes one or more of the Asserted Patents by making, using, offering for sale, selling and/or importing the Cisco Accused Products and/or Charter Accused Products described below as part of Charter's networks.

THE PARTIES

4. Monarch is a limited liability company organized under the laws of California with its principal place of business at 4 Park Plaza, Suite 550, Irvine, CA 92614.

5. Monarch is the assignee and owner of the '844 Patent, '845 Patent, '965 Patent, and '775 Patent through assignment as follows: 7/2/2013 assignment from France Telecom to Orange; 9/21/2017 assignment from Orange to Transpacific IP Group Limited; 3/29/2019 assignment from Transpacific IP Group Limited to Acacia Research Group LLC ("Acacia"); and 11/18/2019 assignment from Acacia to Monarch Networking Solutions LLC.

6. On September 6, 2019, Slingshot Technologies, LLC, filed a complaint in Delaware Chancery Court seeking to rescind the sales transaction that led to Acacia's (and subsequently Monarch's) acquisition of the Asserted Patents. Acacia vigorously denies the allegations in the Slingshot lawsuit, and Monarch's ownership of the patents is intact until such point, if ever, that Slingshot succeeds on the merits of its lawsuit. Nevertheless, out of an abundance of caution, Monarch herein discloses the existence of that lawsuit.

7. On information and belief, Defendant Cisco is a corporation organized under the laws of California with its principal place of business at 170 W. Tasman Dr., San Jose, CA 95134. Cisco is registered to do business in the state of Texas. Cisco has appointed the Prentice-Hall Corporation System, Inc., 211 E. 7th St., Suite 620, Austin, TX 78701 as its agent for service of process.

8. On information and belief, Cisco maintains regular and established places of business and does business in Texas and in the Eastern District of Texas, *inter alia*, at its campus at 2250 East President George Bush Turnpike, Richardson, Texas 75082, and at its data center at 2260 Chelsea Blvd., Allen, Texas 75013. Cisco's Richardson and Allen facilities were appraised and taxed together by the Collin County Appraisal District in 2019 at a combined value of over $300,000,000.

9. By registering to conduct business in Texas and by having facilities where it regularly conducts business in this District, Defendant Cisco has a permanent and continuous presence in Texas and a regular and established place of business in the Eastern District of Texas.

10. On information and belief, Defendant Charter Communications, Inc. is a corporation organized under the laws of Delaware with its principal place of business at 400 Atlantic Street, Stamford, CT 06901. Charter is registered to do business in the State of Texas. Charter has appointed the Corporation Service Company DBA CSC-Lawyers Inco, 211 E. 7th St. Suite 620, Austin, TX 78701 as its agent for service of process.

11. On information and belief, Charter maintains regular and established places of business and does business in Texas and in the Eastern District of Texas, *inter alia*, at its retail locations at

2430 S I-35E Suite 180 Denton, TX 76210; 3555 Legacy Drive Frisco, TX 75034; and 700 Alma Dr #101-103 Plano, TX 75075.

12. By registering to conduct business in Texas and by having facilities where it regularly conducts business in this District, Defendant Charter has a permanent and continuous presence in Texas and a regular and established place of business in the Eastern District of Texas.

JURISDICTION

13. This is an action arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. Accordingly, this Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

14. This Court has personal jurisdiction over Cisco due, *inter alia*, to its continuous presence in, and systematic contact with, this judicial district and its registration in Texas and domicile in this judicial district. Cisco is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and judicial district, including at least part of its past infringing activities, regularly doing or soliciting business at its Richardson and Allen facilities, and engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in the State of Texas, including in the Eastern District of Texas. Cisco directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this judicial district by, among other things, making, using, importing, offering for sale, and/or selling products and/or services that infringe the Asserted Patents.

15. This Court has personal jurisdiction over Charter due, *inter alia*, to its continuous presence in, and systematic contact with, this judicial district and its registration in Texas and domicile in this judicial district. Charter is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and judicial district, including at least part of its past infringing activities, regularly doing or soliciting business at its Denton, Frisco, and/or Plano facilities, and engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in the State of Texas, including in the Eastern District of Texas. Charter directly and/or through subsidiaries or intermediaries

(including distributors, retailers, and others), has committed and continues to commit acts of infringement in this judicial district by, among other things, making, using, importing, offering for sale, and/or selling products and/or services that infringe the Asserted Patents.

VENUE

16. Venue is proper in this judicial district pursuant to 28 U.S.C. §§1391(b), (c), (d) and 1400(b) because Cisco and Charter each have a permanent and continuous presence in, have committed acts of infringement in, and maintain regular and established places of business in this district. Upon information and belief, Cisco and Charter have each committed acts of direct and indirect infringement in this judicial district, including using and purposefully transacting business involving the Cisco Accused Products and Charter Accused Products in this judicial district such as by sales to one or more customers in the State of Texas, including in the Eastern District of Texas, and maintaining regular and established places of business in this judicial district, as set forth above.

JOINDER

17. Cisco and Charter are properly joined as co-defendants in this action under 35 U.S.C. § 299 because Monarch is asserting its right to relief against Cisco and Charter jointly, severally, and/or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences relating to the making, using, importing into the United States, offering for sale, or selling of the same accused products and/or processes including the Cisco Accused Products, and because Monarch alleges on information and belief that questions of fact common to all defendants will arise in this action.

FACTUAL ALLEGATIONS

Monarch Patents

18. The '844 Patent, '845 Patent, '965 Patent, and '775 Patent were all invented and developed by engineers at France Telecom in Paris, who was a leader and pioneer in the areas of networking specific to these patents.

19. The '844 Patent, entitled "Method of Receiving a Data Packet Coming from an IPv4 Domain in an IPv6 Domain, an Associated Device, and Associated Access Equipment," was duly and lawfully issued on May 28, 2013. Monarch is the owner of all right, title, and interest in the '844 Patent. The '844 Patent was filed on June 16, 2009 as Application No. 13/001,850 and is the U.S. national phase of the International Patent Application No. PCT/FR2009/051148, filed on June 16, 2009, which claims the benefit of French Application No. 08 54398, filed on June 30, 2008. A true and correct copy of the '844 Patent is attached hereto as Exhibit A.

20. The '844 Patent relates to IP telecommunications networks transporting data packets from a source terminal identified by a source IP address to a destination terminal identified by a destination IP address. At least by mid-2008, it was commonly accepted in the IP service provider community that IPv4 public addresses were going to run out. In anticipation of this problem, IPv6 was developed which supported IPv6 addresses comprising 128 bits, considerably more than the 32-bit IPv4 addresses that had been available previously. However, due to financial, strategic, and technical reasons linked to managing the complexity of transition and migration from IPv4 networks to IPv6 networks, IPv6 adoption has been slow.

21. The '844 Patent discloses and claims an improved system to facilitate the migration and transformation from IPv4 networks to IPv6 networks. This system, described below, addresses many of the drawbacks detailed above concerning the stateful techniques that were previously available. The '844 Patent solution provides for stateless translation between addresses used in an IPv4 domain to addresses used in an IPv6 domain (and vice versa), which provides an improved solution that permits service operators to migrate to IPv6 networks without requiring the complicated state tables required for the Double NAT (or Operator NAT) solutions previously used to facilitate the implementation of IPv6-to-IPv4 network communication.

22. The '844 Patent solution describes how IPv6 addresses are constructed for IPv4 addresses within a given IPv4 domain. Specifically, an IPv6 address is constructed by concatenating an operator prefix, an IPv4 address, and an IPv4 port number. Once the IPv6 address has been

constructed, the data packet can use that address so that the packet can be forwarded across an IPv6 domain.

23. The '845 Patent, entitled "Method of Receiving a Data Packet in an IPv6 Domain, an Associated Device and an Associated Home Gateway," was duly and lawfully issued on May 28, 2013. Monarch is the owner of all right, title, and interest in the '845 Patent. The '845 Patent issued from Application No. 13/001,907 and is the U.S. national phase of the International Patent Application No. PCT/FR2009/051228, filed on June 26, 2009, which claims priority to French Application No. 08 54405, filed on June 30, 2008. A true and correct copy of the '845 Patent is attached hereto as Exhibit B.

24. The '845 Patent also relates to IP telecommunication networks transporting data packets from a source terminal identified by a source IP address to a destination terminal identified by a destination IP address. The '845 Patent discloses and claims an improved system to facilitate the migration and transformation from IPv4 networks to IPv6 networks. The '845 solution is executed in a home gateway, which is any equipment for interconnecting a private network and a network operated by a service provider, the private network being either a home network or a business network. The solution includes receiving packets that comprise an IPv6 source address and an IPv6 destination address, wherein the IPv6 destination address is constructed by concatenating an IPv6 prefix, an IPv4 destination address and a port number. Based on these addresses, the gateway determines whether it needs to regularize either of the IPv6 addresses based on the networks to which the gateway is connected. Once the addresses have been regularized and the packet modified accordingly, the gateway routes the modified packet to its destination.

25. The '845 Patent solution constitutes an improvement over prior solutions because it permits the gateway to transform packets received from an IPv6 domain that includes IPv4 destination address and port number for delivery on an IPv4 network without being required to maintain state for all incoming and outgoing connections, as is required for the Operator NAT solution. It is unnecessary to store an IPv4 to IPv6 address translation table or to maintain states relating to sessions in the gateway connecting IPv4 domains and IPv6 domains. The elimination of such state

or translation tables improves the operation of the network, providing a more efficient and elegant solution for interconnecting IPv4 domains with IPv6 domains. This provides an efficient migration and transformation solution, allowing network operators to effectively address the problem of an exhausted IPv4 address space.

26. The ’965 Patent, entitled “Methods and Devices for Routing Data Packets Between IPv4 and IPv6 Networks,” was duly and lawfully issued on April 28, 2015. Monarch is the owner of all right, title, and interest in the ’965 Patent. The ’965 Patent was filed on October 20, 2010 as Application No. 13/503,070 and is the U.S. national phase of the International Patent Application No. PCT/FR2010/052229, filed on October 20, 2010, which claims the benefit of French Application No. 09 57709, filed on October 30, 2009. A true and correct copy of the ’965 Patent is attached hereto as Exhibit C.

27. The ’965 Patent also relates to the field of IP telecommunication networks transporting data packets from a source terminal identified by a source IP address to a destination terminal identified by a destination IP address. The ’965 Patent solution permits operators to connect private IPv4 network domains with IPv6 network domains without requiring the operator to maintain state and translation tables within its network, as required by the prior solutions such as Double NAT, Operator NAT, and/or DS-Lite.

28. The ’965 Patent solution permits IPv4 packets in a first IPv4 domain to be routed to terminals in a second IPv4 domain that is private via an IPv6 domain by using stateless address translation and encapsulation. One embodiment of the ’965 Patent solution is as follows. On receiving an IPv4 packet from a first IPv4 domain that is destined for a second private IPv4 domain, the terminal constructs a destination IPv6 address by combining an IPv6 prefix and the private IPv4 destination address. Once this address is constructed via stateless translation, the IPv4 packet is then encapsulated in an IPv6 packet using that constructed IPv6 address. Thereafter, the encapsulated packet can be routed through the IPv6 domain to its destination IPv4 domain that is private.

29. The '775 Patent, entitled "Method for Protecting a Pseudo-Wire," was duly and lawfully issued on March 6, 2012. Monarch is the owner of all right, title, and interest in the '775 Patent. The '775 Patent was filed on February 26, 2008 as Application No. 12/528,083 and is a Section 371 National Stage of International Application No. PCT/FR2008/050324 which claims the benefit of French Application No. 07 53489, filed on February 26, 2007. A true and correct copy of the '775 Patent is attached hereto as Exhibit D.

30. The '775 Patent relates to packet-switched networks in which data is transmitted in the form of packets processed by network routers until those packets reach their destination. Technologies for routing such data packets include, for example, the use of so-called "pseudo-wires" as defined by the IETF Pseudo-Wire Emulation Edge-To-Edge (PWE3) group in the document RFC 3985. Such pseudo-wires emulate a point-to-point link between two pieces of equipment (*e.g.* routers) of a packet-switched network based on IP/MPLS technology and enable data packets to be transmitted that do not conform to the Internet Protocol, for example data packets implementing the ATM protocol. For example, when such a pseudo-wire has been set up between two routers, the input router is able to transmit a data stream routed via the pseudo-wire to the output router. In this case, the pseudo-wire is composed of links beginning at the input router, passing through one or more intermediate routers, and terminating at the output router.

31. As one example where multiple pseudo-wires may be configured in the same network, the working group PWE3 proposed a solution that backs up the first pseudo-wire set up between an input router and an output router by using a second pseudo-wire serving as a back-up pseudo-wire so that, in the event of a fault affecting the output router constituting one end of the first pseudo-wire, the data packets are routed by the back-up pseudo-wire to a different output router. When the input router detects a fault in the output router, it triggers switching of the data stream from the first pseudo-wire to the second pseudo-wire, thus routing the data to a different output router. However, this use of multiple pseudo-wires has the disadvantage of consuming network resources, for example processing resources in the network equipment (storage capacity, computation capacity, etc.), signaling streams for setting-up two pseudo-wires, and bandwidth, even though the

pseudo-wires may share a portion of the delivery path. This increases the initial time required to set up the two pseudo-wires, and also increases the restore time in the event of a fault affecting an output router, with a negative impact on quality of service.

32. The '775 Patent discloses and claims improved systems and methods for setting up at least two pseudo-wires in a manner that avoids or mitigates the drawbacks described above. Rather than set up two pseudo-wires, each composed of entirely separate links, the '775 Patent enables the two pseudo wires to effectively share a link for at least a portion of each pseudo-wire, thus reducing or eliminating consumption of extra network resources that would otherwise be required to set up an additional link. For example, the '775 Patent teaches an embodiment in which a first pseudo-wire is set up between an input router of a packet-switched network and a first output router of said packet-switched network, and a second pseudo-wire is set up between the same input router and a second output router of the packet-switched network. In this configuration, a first link is configured between the input router and an intermediate router that is shared by both the first pseudo-wire and the second pseudo-wire. The first pseudo-wire also includes a second link set up between the intermediate router and the first output router, and the second pseudo-wire also includes a third link set up between the intermediate router and a second output router. This configuration technique is noteworthy in that a link is shared by the two pseudo-wires between the intermediate router and the input router.

33. The '775 Patent solution improves upon prior approaches because it optimizes the use of network resources, for example bandwidth, between the input router and the intermediate router by setting up between them a single link common to the two pseudo-wires. This solution is novel and distinct from prior approaches. This solution improves the operation of the network itself by making more efficient use of the network's resources. This solution also improves the functioning of the equipment that makes up the network, such as cables and routers, by reducing the extent to which their physical resources (*e.g.*, bandwidth, processor speed, switching speed, data storage, power consumption, and heat dissipation) are taxed by excess signaling.

Cisco's Use of the Patented Technology

34. On information and belief, Cisco makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States various networking equipment including routers and switches. For example, Cisco makes, uses, and sells Cisco 500 Series WPAN Industrial Routers that support Mapping of Address and Port capabilities for Customer Equipment (MAP-CE). The MAP-CE capabilities include software on the routers that implement methods of the claimed '844 Patent and/or '845 Patent. These capabilities include performing stateless address translation as described in RFC 7597 and RFC 7599. Further, the Cisco 500 Series WPAN Industrial Routers are home gateways because they support connecting a private network of user terminals with a service provider network.

35. Additionally, Cisco makes, uses, and sells ASR 1000 Series Aggregation Services Routers (e.g., ASR 1001-X, ASR 1002-X, ASR 1001-HX, ASR 1002-HX, ASR 1004, ASR 1006, ASR 1006-X, ASR 1009-X, ASR 1013), ASR 9000 Series Aggregation Services Routers (*e.g.*, ASR 9006, ASR 9010, ASR 9904, ASR 9906, ASR 9910, ASR 9912, ASR 9922), 1000 Series Integrated Services Routers (ISRs) (e.g., ISR 1111X-8P, ISR 1100-8P, ISR 1100-4P, ISR 1101-4P, ISR 1109-4P, ISR 1109-2P), 4000 Series ISRs (e.g., ISR 4331, ISR 4221, ISR 4321, ISR 4351, ISR 4431, ISR 4451, ISR 4461), and their corresponding line cards, interface modules, enhanced service modules, network interface modules, integrated services modules (ISMs), and virtual services modules (VSMs). These routers are made, used, and sold with software that implements MAP-E (RFC 7597) and/or MAP-T (RFC 7599) border relay capabilities, including those claimed by the '844 Patent and '965 Patent.

36. The ASR Series 9000 routers also support a feature called Virtual Private LAN Service (VPLS) Label Switched Multicast (LSM), which includes support for pseudo-wire configurations as claimed by the '775 Patent. The VPLS LSM solution employs point-to-multipoint (P2MP) label-switched paths (LSPs) in the MPLS core to carry broadcast, multicast, and unknown unicast traffic for a VPLS domain. The pseudo-wire configurations described by Cisco's documentation mirror those claimed by the '775 Patent.

37. The Cisco Accused Products include Cisco 500 Series WPAN Industrial Routers, ASR 1000 Series Aggregation Services Routers (e.g., ASR 1001-X, ASR 1002-X, ASR 1001-HX, ASR 1002-HX, ASR 1004, ASR 1006, ASR 1006-X, ASR 1009-X, ASR 1013), ASR 9000 Series Aggregation Services Routers (*e.g.*, ASR 9006, ASR 9010, ASR 9904, ASR 9906, ASR 9910, ASR 9912, ASR 9922), 1000 Series Integrated Services Routers (ISRs) (e.g., ISR 1111X-8P, ISR 1100-8P, ISR 1100-4P, ISR 1101-4P, ISR 1109-4P, ISR 1109-2P), 4000 Series ISRs (e.g., ISR 4331, ISR 4221, ISR 4321, ISR 4351, ISR 4431, ISR 4451, ISR 4461), other router/gateway products that support MAP-E and/or MAP-T as detailed below, and any corresponding line cards, interface modules, enhanced service modules, network interface modules, integrated services modules (ISMs), and virtual services modules (VSMs) for the accused routers and/or gateways.

Charter's Use of the Patented Technology

38. On information and belief, Charter uses, sells, and/or offers to sell in the United States, and/or imports into the United States various networking equipment including routers, switches, and home gateways. For example and on information and belief, Charter uses Cisco ASR 9000 Series routers and their corresponding line cards, integrated service modules (ISMs), and virtual service modules (VSMs) within its provider network, which implements MAP-T. These ASR Series routers are made, used, and sold with software that implements both MAP-E (RFC 7597) and MAP-T (RFC 7599) border relay capabilities, including those claimed by the '844 Patent and '965 Patent.

39. Additionally, Charter uses and induces its customers to use cable modems and/or home gateways within its network to support connecting a private network of user terminals with Charter's service provider network. Because Charter implements MAP-T within its network, at least some of the cable modems or home gateways supported and/or provisioned by Charter support Mapping of Address and Port capabilities for Customer Equipment (MAP-CE). The MAP-CE capabilities include software on the cable modems and/or home gateways that implement methods of the claimed '844 Patent and/or '845 Patent. These capabilities include performing stateless address translation as described in RFC 7597 and/or RFC 7599.

40. Charter provides customers with a list of modems supported on its network at the following address: https://www.spectrum.net/support/internet/compliant-modems-charter-network/. On information and belief, one or more of the following cable modems supported on the Charter network implements the infringing MAP-CE capabilities: Arris SB6190, Arris SBG7580, Arris SBG7580-AC, ASUS CM-32, ASUS CM-32_AC2600, Linksys CG7500, Linksys CM3016, Linksys CM3024, Motorola MB7621, Motorola MG7700, Motorola MB8600, Netgear C6900, Netgear C7000, Netgear CM600, Netgear CM700, Netgear CM1000v2, Arris SB6183, Arris SBG6900-AC, ASUS CM-16, Motorola MB7420, Motorola MG7540, Motorola MG7550, Netgear C6250, Netgear CM500, SMC Networks D3CM1604, TP-Link CR500, TP-Link CR700, TP-Link TC-7620, Arris SB6141, Arris , BG6400, Arris SBG6580, Arris SBG6580-2, Arris SBG6700-AC, D-Link DCM301, Linksys CM3008, Motorola MB7220, Motorola MG7310, Motorola MG7315, Netgear C3000, Netgear CG3000D, Netgear C3700, Netgear CM400, TP-Link TC-7610, TP-Link TC-W7960, Zoom 5341J, Zoom 5345, Zoom 5350, Zoom 5352, Zoom 5354, Zoom 5360, Zoom 5363, Zyxel CDA30360, Arris SB6120, Arris SB6121, and/or Netgear CMD31T.

41. Finally, Charter requires its business customers to use Charter-issued modems. *See* https://www.spectrumbusiness.net/support/internet/authorized-modems-spectrum-business-network ("Spectrum Business Internet customers are required to use Spectrum Business-issued modems."). On information and belief, one or more of the Spectrum Business-issued modems support the infringing MAP-CE capabilities.

42. The Charter Accused Products include Arris SB6190, Arris SBG7580, Arris SBG7580-AC, ASUS CM-32, ASUS CM-32_AC2600, Linksys CG7500, Linksys CM3016, Linksys CM3024, Motorola MB7621, Motorola MG7700, Motorola MB8600, Netgear C6900, Netgear C7000, Netgear CM600, Netgear CM700, Netgear CM1000v2, Arris SB6183, Arris SBG6900-AC, ASUS CM-16, Motorola MB7420, Motorola MG7540, Motorola MG7550, Netgear C6250, Netgear CM500, SMC Networks D3CM1604, TP-Link CR500, TP-Link CR700, TP-Link TC-7620, Arris SB6141, Arris , BG6400, Arris SBG6580, Arris SBG6580-2, Arris SBG6700-AC, D-

Link DCM301, Linksys CM3008, Motorola MB7220, Motorola MG7310, Motorola MG7315, Netgear C3000, Netgear CG3000D, Netgear C3700, Netgear CM400, TP-Link TC-7610, TP-Link TC-W7960, Zoom 5341J, Zoom 5345, Zoom 5350, Zoom 5352, Zoom 5354, Zoom 5360, Zoom 5363, Zyxel CDA30360, Arris SB6120, Arris SB6121, Netgear CMD31T, and Spectrum Business-issued modems. Charter Accused Products also include Cisco Accused Products that are used by Charter in its IPv4-to-IPv6 networks.

FIRST COUNT

(Infringement of U.S. Patent No. 8,451,844)

43. Monarch incorporates by reference the allegations set forth in Paragraphs 1-42 of this Complaint as though fully set forth herein.

44. Cisco makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that directly infringe the ’844 Patent, including the above identified Cisco Accused Products. Cisco Accused Products infringe at least claim 1 of the ’844 Patent.

45. Cisco Accused Products support and implement a method of receiving a data packet from an IPv4 domain in an IPv6 domain, said data packet comprising an IPv4 destination address and a destination port number. The Cisco Accused Products are configured to use the incoming IPv4 data packet to generate an IPv6 data packet that includes a newly constructed IPv6 destination address formed from an operator prefix, the IPv4 destination address and destination port information. The Cisco Accused Products are designed to route the generated IPv6 data packet within an IPv6 domain using the constructed IPv6 destination address. The ability to generate an IPv6 data packet while retaining the necessary IPv4 address and port information allows stateless mapping of IPv4-to-IPv6 communications. Specifically, the Cisco Accused Products are configured to support Mapping of Address and Port using both translation and encapsulation techniques, conventionally known as MAP-T and MAP-E.

46. The Cisco Accused Products, for example, include the ASR 1000 Series routers that run the IOS XE operating system:

> The Cisco ASR 1000 Series supports Cisco IOS® XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The Cisco ASR 1000 Series Embedded Services Processors (ESPs), which are

Cisco ASR 1000 Series Aggregation Services Routers Data Sheet at 3. Cisco included support for Mapping of Address and Port using translation (MAP-T) in IOS XE Release 3.8S, which was released in approximately November 2012. *See* Cisco ASR 1000 Series Aggregation Routers Release Notes, Cisco IOS XE Release 3S, Release 3.8S Features and Important Notes (listing "Mapping of Address and Port Using Translation (MAP-T)" as a new feature of 3.8S). Cisco added support for Mapping of Address and Port using encapsulation (MAP-E) in Release 16.11 of IOS XE (Gibraltar), published in approximately March 2019.

> • MAP-E—The MAP-E feature in this release complements the existing MAP-T capability by providing connectivity to IPv4 hosts across IPv6 domains on CE devices while encapsulating the original IPv4 packet. MAP-E also enables mapping of address between IPv6 and IPv4 addresses, and across transport layer ports. Additionally, the CE device performs NAPT44 translation between a customer private IPv4 address and the MAP-E NAT64 translation to ensure that different CE devices share a common public IPv4 address.

Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Gibraltar 16.11.x at 2.

47. The Cisco Accused Products also include the ASR 9000 Series routers that run the IOS XR operating system:

> design, incredible flexibility, and an attractive price-to-performance benchmark. The Cisco ASR 9000 Series has a wide product portfolio (Figure 1), ranging from the Cisco ASR 9001 (2 Rack Units [2RU]) to the Cisco ASR 9922 (44RU), with each system designed to provide true carrier-class reliability using the Cisco IOS® XR operating system, comprehensive system redundancy, and a full complement of network resiliency schemes. The Cisco ASR

Cisco ASR 9000 Series Aggregation Services Routers Data Sheet at 1. Cisco included support for MAP-E (without requiring ISMs or VSMs) in Release 5.3.2 of IOS XR, which was released in 2015.

> MAP-E without service modules feature allows to configure Mapping of Address and Portal-Encapsulation Mode (MAP-E) CGN solution without service modules (ISM or VSM cards). The CGN application directly interacts with the line cards to configure MAP-E.

Release Notes for Cisco ASR 9000 Series Aggregation Services Routers for Cisco IOS XR Software Release 5.3.2 at 61 (copyright date of 2015). Cisco included support for MAP-E that initially required a VSM (Virtualized Service Module) in Release 5.2.2 of IOS XR, which was released in 2014.

> **Mapping of Address and Port-Encapsulation Mode on VSM**
>
> Mapping of Address and Port-Encapsulation Mode (MAP-E) is a CGN solution that enables a service provider to enable IPv4 services to IPv6 (customer) sites to which it provides customer premise equipment (CPE). This approach utilizes stateless IPv4-in-IPv6 encapsulation to transit IPv6-enabled network infrastructure.

Release Notes for Cisco ASR 9000 Series Aggregation Services Routers for Cisco IOS XR Software Release 5.2.2 at 59 (copyright date of 2014). Cisco included support for MAP-E that initially required an ISM in Release 4.3.1 of IOS XR.

Feature	Description	Introduced/Changed in Release	Where Documented
Mapping of Address and Port-Encapsulation Mode (MAP-E)	This feature was introduced.	Release 4.3.1	*Implementing the Carrier Grade IPv6 on Cisco IOS XR Software* chapter • Mapping of Address and Port-Encapsulation Mode • Configuring MAP-E on ISM Refer *Carrier Grade NAT Commands on Cisco IOS XR Software* chapter in *Cisco ASR 9000 Series Aggregation Services Router CGv6 Command Reference* for information on the commands used to configure MAP-E on ISM.

Cisco ASR 9000 Series Aggregation Services Router Carrier Grade IPv6 (CGv6) Configuration Guide (version 4.3.x) at 8. Cisco included support for MAP-T that initially required an ISM since at least 2012:

> Cisco® ASR 9000 Series Integrated Service Module (ISM) is a universal service foundation for Cisco ASR 9000 Aggregation Services Routers. The module provides a highly scalable modular services delivery platform for delivering multiple types of services. Currently the Integrated Services Module (Figure 1) supports the following services:
>
> - Carrier Grade Network Address Translation (NAT): CGN
> - Dual-Stack Lite
> - Stateful NAT64
> - Mapping of Address and Port Translation (MAP-T)

Cisco ASR 9000 Series Integrated Service Module Data Sheet at 1. Subsequently, Cisco supported MAP-T in the ASR 9000 Series Routers without requiring ISM or VSM cards. This integrated support for MAP-T in the ASR Series 9000 Routers has existed since at least Release 5.3.2 of IOS XR:

> • From Cisco IOS XR Release 5.3.2, MAP-T is supported only on Cisco ASR 9000 High Density 100GE Ethernet line cards.

Release Notes for Cisco ASR 9000 Series Aggregation Services Routers for Cisco IOS XR Software Release 5.3.2 at 64 (copyright date of 2015). Thus, on information and belief, since at least 2015 the Cisco ASR 9000 Series Aggregation Services Routers are capable of implementing MAP-T and/or MAP-E stateless translations as sold, without requiring any additional ISM or VSM cards.

48. The manner in which MAP-E was implemented has been described in RFC 7597 (dated July 2015), and on information and belief, that implementation has been adopted and incorporated by Cisco in the Cisco Accused Products.

> MAP-E
> RFC 7597
>
> MAP-Encapsulation
> - Defines Stateless IPv4 in IPv6 Encapsulation based transport using MAP algorithm
> - Based on IPinIP, 6rd

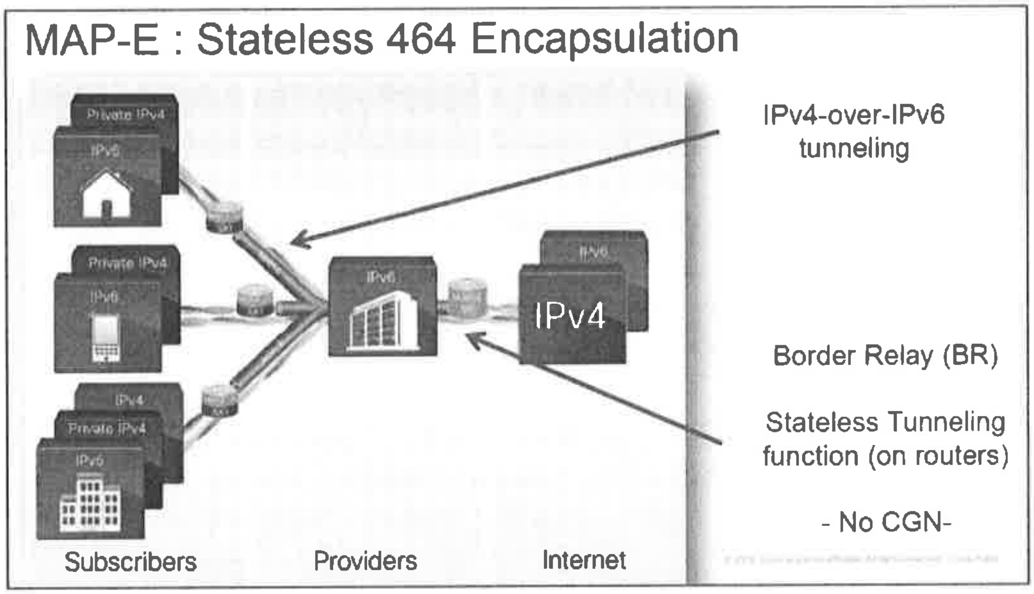
Cisco Live! 2016 Presentation, BRKSPG-2300 at 41.

49. Similarly, the manner in which MAP-T was implemented has been described in RFC 7599 (dated July 2015), and on information and belief, that implementation has been adopted and incorporated by Cisco in the Cisco Accused Products.

> MAP-T
> RFC 7599
>
> MAP-Translation
> - Defines Stateless NAT64 based transport using MAP algorithm
> - Based on NAT64 divi

Cisco Live! 2016 Presentation, BRKSPG-2300 at 41.

50. The Cisco Accused Products, when operating with either the MAP-E or MAP-T functionality, are capable of being used as MAP Border Relays (BR), in which they provide an interface between an IPv4 domain and an IPv6 domain, as illustrated in the figures below.



Cisco Live! 2016 Presentation, BRKSPG-2300 at 38.

51. This same network topology is generally depicted and described in the MAP-E/MAP-T descriptions in RFCs 7597 and 7599.

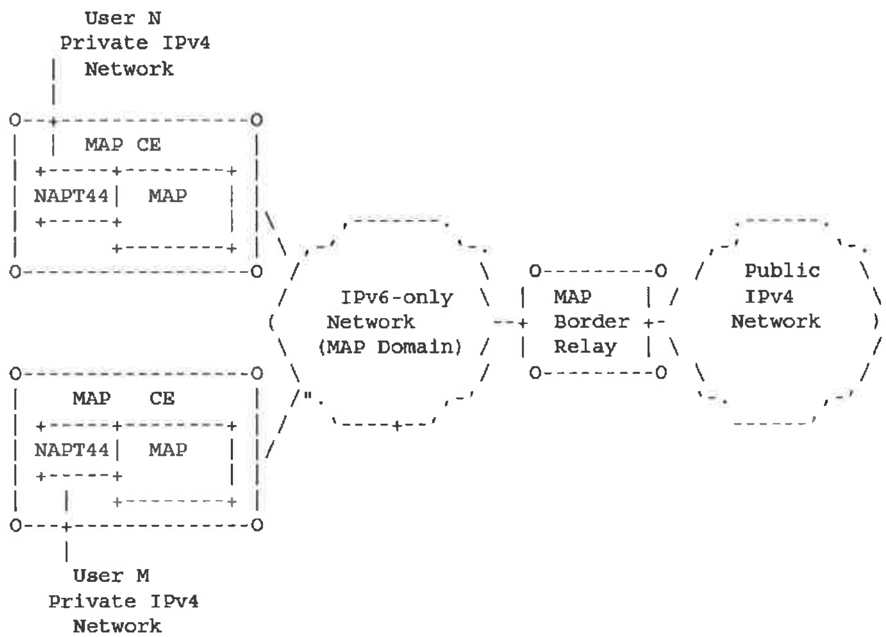


Figure 1: Network Topology

IETF RFC 7597 at 8; *see also* IETF RFC 7599 at 7. Accordingly, the Cisco Accused Products, operating as a Border Relay and/or Customer Edge device in an IPv6 domain, receive data packets from an IPv4 network that include an IPv4 destination address and a destination port number.

52. IPv4 packets (or Internet Protocol v4 packets), by definition, include IPv4 source and destination addresses. These addresses can be interpreted as network addresses or host addresses (or both). Additionally, certain IP packets encapsulate higher layer protocols, such as TCP and UDP, which rely on port numbers for addressing at that layer of the protocol stack.

53. To facilitate traffic across MAP domains, the edge devices (Border Relay and Customer Edge devices) use mapping rules, referred to in the applicable RFCs as Basic Mapping Rule and Forwarding Mapping Rule. In each case, the Mapping Rule requires identification of the following: (1) Rule IPv6 prefix; (2) Rule IPv4 prefix; and (3) EA bit length.

```
Both mapping rules share the same parameters:

o  Rule IPv6 prefix (including prefix length)

o  Rule IPv4 prefix (including prefix length)

o  Rule EA-bit length (in bits)
```

IETF RFC 7597 at 9. MAP-T relies on this same rule structure.

```
5.  Mapping Rules

   The MAP-T algorithmic mapping rules are identical to those in
   Section 5 of the MAP-E specification [RFC7597], with the following
   exception: the forwarding of traffic to and from IPv4 destinations
   outside a MAP-T domain is to be performed as described in this
   document, instead of Section 5.4 of the MAP-E specification.
```

IETF RFC 7599 at 8.

54. Cisco describes in its product literature and in marketing presentations how mapping rules are used to map IPv4 destination addresses and ports into an IPv6 address for both the Basic Mapping Rule (BMR) and for the Forward Mapping Rule (FMR). As an example, the BMR mapping is described below.

> MAP-E refers to Mapping of Address and Port Encapsulation (MAP-E). The MAP-E feature enables you to configure mapping rules for translation between IPv4 and IPv6 addresses. Each mapping of address and port using MAP-E domain uses a different mapping rule. A MAP-E configuration comprises of one basic mapping rule (BMR), one default mapping rule (DMR), and one or more forwarding mapping rules (FMRs) for each MAP-E domain.
>
> **A BMR configures the MAP IPv6 address or prefix.** You can configure only one BMR per IPv6 prefix. The MAP-E CE uses the BMR to configure itself with an IPv4 address, an IPv4 prefix, or a shared IPv4 address from an IPv6 prefix. A BMR can also be used for forwarding packets in such scenarios where an IPv4 destination address and a destination port are mapped into an IPv6 address/prefix. Every MAP-E node (CE device is a MAP-E node) must be provisioned with a BMR. The BMR prefix along with the port parameter is used as tunnel destination address. You can use the port-parameters command to configure port parameters for the MAP-E BMR.

IP Addressing: NAT Configuration Guide, Cisco IOS XE Gibraltar 16.11.x at 154.

Configuring BR Endpoint Address without modules

Perform this task to configure the BR Endpoint Address without service modules.

SUMMARY STEPS

1. **configure**
2. **service cgv6** *instance-name*
3. **service-inline** *interface-name*
4. **service-type map-e** *instance-name*
5. **cpe-domain ipv4 prefix** *ipv4 adress/prefix* **cpe-domain ipv6 prefix** *ipv6 adress/prefix*
6. **sharing-ration 256**
7. **contiguous-port 16**
8. **br-endpoint-adress**
9. **endor commit**

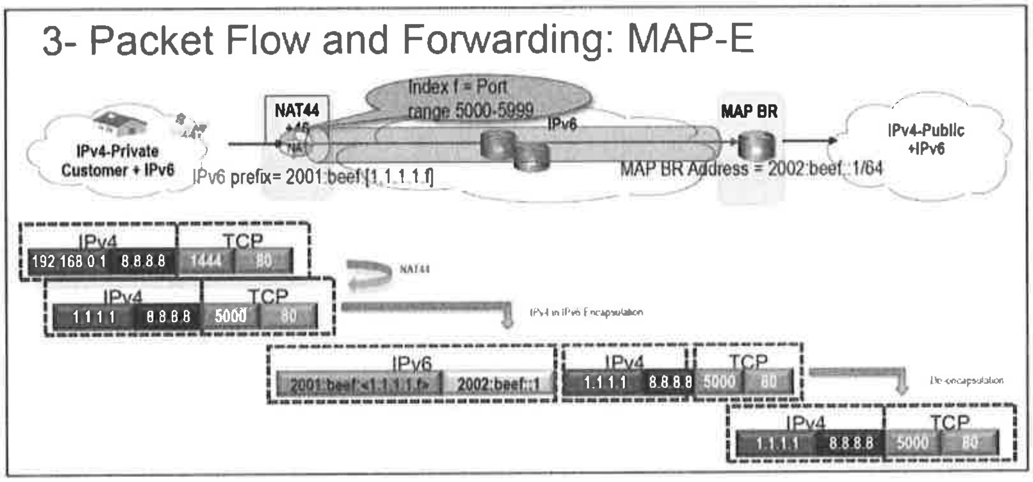
Cisco ASR 9000 Series Aggregation Services Router CGv6 Configuration Guide, Release 5.3.x at 311-12.

55. When a packet is received by a Cisco Accused Product with a destination IPv4 address that matches the IPv4 address prefix of a mapping rule, the Cisco Accused Product is programmed to construct an IPv6 address for transmitting the packet to a destination at the edge of the IPv6 domain, where the IPv4 address and port information are recovered and used to route the IPv4 packet to its intended destination in an IPv4 domain. On information and belief in the Cisco Accused Products, the destination IPv6 address is constructed for MAP-E by concatenating an IPv6 prefix and a sequence of Embedded Address (EA) bits, which represent the target IPv4 address and port number.

```
Figure 3 shows the structure of the complete MAP IPv6 address as
specified in this document.

|     n bits          |  o bits    | s bits  |   128-n-o-s bits      |
+---------------------+------------+---------+-----------------------+
|  Rule IPv6 prefix   |  EA bits   |subnet ID|     interface ID      |
+---------------------+------------+---------+-----------------------+
|<---  End-user IPv6 prefix  --->|

                 Figure 3: MAP IPv6 Address Format

The Rule IPv6 prefix is common among all CEs using the same Basic
Mapping Rule within the MAP domain.  The EA bit field encodes the
CE-specific IPv4 address and port information.  The EA bit field,
```

IETF RFC 7597 at 12. The Cisco Accused Products are programmed to use this same IPv6 address construction for MAP-T IPv6 addresses that are constructed from IPv4 addresses. *See* IETF RFC 7599 at Section 5.

56. The construction of an IPv6 address for MAP-E is depicted graphically below in this example from Cisco, which shows how the Cisco Accused Products are configured to support packets flowing from an IPv4 private customer through an IPv6 domain.



Cisco Live! 2016 Presentation, BRKSPG-2300 at 49; BRKSPG-2606 at 25-27. This same operation occurs in reverse at the Cisco Accused Products operating as a Border Relay when data packets are travelling from the Border Relay to the IPv6 domain. As this example illustrates, the IPv4 address and port information are encapsulated in the IPv6 address for transmission by the Cisco Accused Products across the IPv6 domain from both the customer edge and the border relay map nodes.

57. The EA bits identified in the RFC are used in the Cisco Accused Products to encode the destination IPv4 address and destination port.

```
Embedded Address (EA) bits:
                      The IPv4 EA-bits in the IPv6 address identify
                      an IPv4 prefix/address (or part thereof) or a
                      shared IPv4 address (or part thereof) and a
                      Port Set Identifier.
```

IETF RFC 7597 at 7. Pursuant to RFC 7597, the EA bit encoding can take three different forms: (1) an IPv4 prefix address; (2) an IPv4 address; or (3) a shared IPv4 address and a Port Set Identifier (PSID). In the third form, which the Cisco Accused Products are programmed to support, the EA bits represent an encoding of both an IPv4 address and a destination port, as claimed. This scenario is depicted below:

```
|   r bits     |        p bits         |          |   q bits    |
+--------------+-----------------------+          +-------------+
| Rule IPv4    | IPv4 address suffix   |          |Port Set ID  |
+--------------+-----------------------+          +-------------+
|              32 bits                 |

                 Figure 6: Shared IPv4 Address
```

IETF RFC 7597 at 13. The combined Rule IPv4 network address and IPv4 address suffix form the IPv4 destination address. The PSID forms the destination port for the packet. The p bits and q bits form the EA bits that are included in the destination IPv6 address, and represent an encoding of the target IPv4 address and target IPv4 destination port in the Cisco Accused Products.

58. Additionally, in the Cisco Accused Products, the IPv4 destination address is appended to the IPv6 operator prefix as part of the interface ID that forms the MAP IPv6 destination address. As illustrated above, the IPv6 address constructed in the Cisco Accused Products is comprised of a Rule IPv6 prefix, EA bits, a subnet ID, and an interface ID. The format of the interface ID, which includes the destination IPv4 address, is illustrated below:

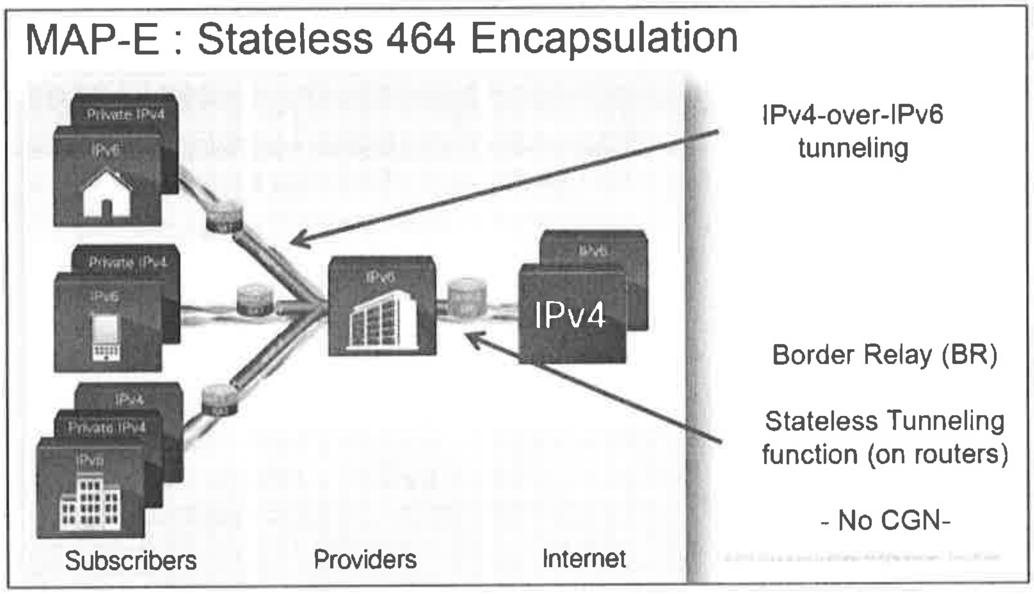
```
6.  The IPv6 Interface Identifier

   The interface identifier format of a MAP node is described below.

                  |              128-n-o-s bits            |
                  | 16 bits|    32 bits     | 16 bits|
                  +--------+----------------+--------+
                  |   0    |  IPv4 address  |  PSID  |
                  +--------+----------------+--------+

                  Figure 8: IPv6 Interface Identifier
```

IETF RFC 7597 at 15; IETF RFC 7599 at 9.

59. As its name indicates, MAP-E is an IPv4 to IPv6 solution based on encapsulation.

```
          Mapping of Address and Port with Encapsulation (MAP-E)

Abstract

   This document describes a mechanism for transporting IPv4 packets
   across an IPv6 network using IP encapsulation.  It also describes a
   generic mechanism for mapping between IPv6 addresses and IPv4
   addresses as well as transport-layer ports.
```

IETF RFC 7597 at 1. Cisco refers to this encapsulation as stateless tunneling, which Cisco promotes to its customers as being advantageous relative to other stateful routing techniques.



Cisco Live! 2016 Presentation, BRKSPG-2300 at 38; BRKSPG-2606 at 38. Thus, for MAP-E support in the Cisco Accused Products, the received IPv4 packet is encapsulated into an IPv6 packet that uses the constructed IPv6 destination address. The resulting IPv6 packet is the claimed generated IPv6 packet.

60. MAP-T translates (rather than encapsulates) the incoming IPv4 address information into an IPv6 address and then constructs an IPv6 packet using the newly translated addresses.

```
in the Mapping of Address and Port with Encapsulation (MAP-E)
specification [RFC7597].  The MAP-T solution differs from MAP-E in
that MAP-T uses IPv4-IPv6 translation, rather than encapsulation, as
the form of IPv6 domain transport.  The translation mode is
```

IETF RFC 7599 at 4.

61. Cisco Accused Products configured as MAP-T Border Relays are programmed to accept incoming IPv4 packets, construct destination IPv6 addresses, and forward the resulting packet as an IPv6 packet.

```
8.4.  IPv4 to IPv6 at the BR

   A MAP-T BR receiving IPv4 packets uses a longest match IPv4 +
   transport-layer port lookup to identify the target MAP-T domain and
   select the FMR and DMR rules.  The MAP-T BR MUST then compute and
   apply the IPv6 destination addresses from the IPv4 destination
   address and port as per the selected FMR.  The MAP-T BR MUST also
   compute and apply the IPv6 source addresses from the IPv4 source
   address as per Section 5.1 (i.e., using the IPv4 source and the BR's
   IPv6 prefix, it forms an IPv6-embedded IPv4 address).  The generic
   IPv4-to-IPv6 header translation procedures outlined in [RFC6145]
   apply throughout.  The resulting IPv6 packets are then passed to
   regular IPv6 forwarding.
```

IETF RFC 7599 at 13. Once the IPv6 packet is generated, it is routed through the IPv6 MAP domain per standard IPv6 routing mechanisms based on the IPv6 constructed destination address that is generated by the Cisco Accused Product.

62. On information and belief, Charter is a customer of Cisco's that has purchased the Cisco Accused Products for use in its network, and to "aid[] Charter's efforts to support IPv6 traffic . . . ."

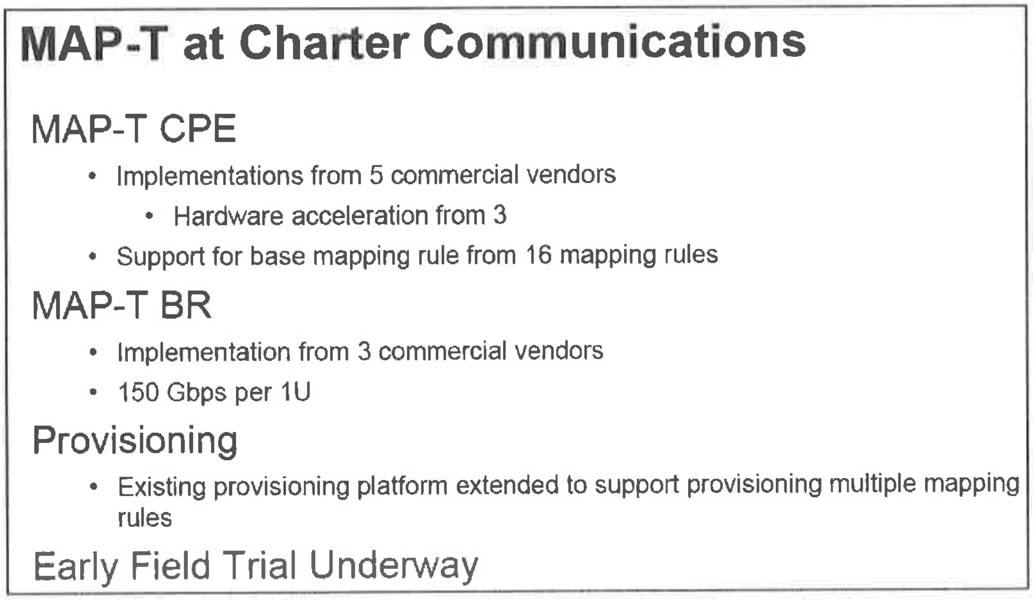
> **SAN JOSE, Calif., August 15, 2011 –** Cisco today announced that Charter Communications, a leading communications and entertainment services provider and the fourth-largest cable operator in the United States,is deploying the Cisco® CRS-3 Carrier Routing System and Cisco ASR 9000 Series Aggregation Services Routers to deliver enhanced video, data, voice and mobile backhaul services to residential and commercial customers.

https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=452731 (last visited 1/8/2020).

> - Use of the Cisco IP NGN architecture aids Charter's efforts to support IPv6 traffic, necessary to support the huge boost in IP-connected devices used in consumer, business, mobile and machine-to-machine environments.

https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=452731 (last visited 1/8/2020).

63. Charter engineer, E. Jordan Gottlieb, presented "Mapping of Address and Port using Translation (MAP-T)" at a North American Network Operators' Group (NANOG) meeting/conference. *See* https://www.youtube.com/watch?v=ZmfYHCpfr_w. In that presentation, he explained that Charter has implemented MAP-T within its network.



Gottlieb, Mapping of Address and Port using Translation (MAP-T) at 14. Additional details of Charter's implementation can be found in that presentation.

64. Mr. Gottlieb (and John Berg), both associated with Charter, assisted in drafting a Mapping of Address and Port (MAP) Technical Report for CableLabs, which "is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers." CL-TR-MAP-V01-160630 at 1 (2016). The report provides extensive details on MAP implementations, as well as highlighting issues of which service providers should be aware when designing and implementing MAP within their network.

65. Charter also highlighted that its network uses customer premises equipment (CPE) from five commercial vendors and include support for base mapping rule from 16 mapping rules. Charter lists the modems it supports for its network at the following addresses: https://www.spectrumbusiness.net/support/internet/authorized-modems-spectrum-business-network; https://www.spectrum.net/support/internet/compliant-modems-charter-network/. The eRouter specification that was defined by CableLabs for the cable industry (and to which Cisco contributed), requires that current cable modems must comply and support MAP-E and MAP-T as defined in RFC 7597 and RFC 7599.

The eRouter MUST support MAP-E as defined in [RFC 7597]. The eRouter MUST support MAP-T as defined in [RFC 7599].

Data-Over-Cable Service Interface Specifications: IPv4 and IPv6 eRouter Specification, CM-SP-eRouter-I20-190515 at 57. On information and belief, one or more of the Charter Accused Products comply with RFC 7597 and/or RFC 7599, and thus infringe claims of the '844 Patent, as outlined by the evidence above.

66. On information and belief and as one example of Charter's direct infringement, Charter uses Cisco Accused Products as Border Relays in one or more MAP-T network domains in a manner that directly infringes claims of the '844 Patent.

67. By making, using, offering for sale, and/or selling products in the United States, and/or importing products into the United States, including but not limited to the Cisco Accused Products and Charter Accused Products, Cisco and Charter have injured Monarch and are liable to Monarch for directly infringing one or more claims of the '844 Patent, including without limitation claim 1 pursuant to 35 U.S.C. § 271(a).

68. In addition to direct infringement, Cisco also indirectly infringes the '844 Patent under 35 U.S.C. § 271(b). Through its sales and marketing program for the Cisco Accused Products, including those identified above, Cisco has induced Charter and others to implement a network that directly infringes the '844 patented inventions.

69. Cisco knowingly encourages and intends to induce infringement of the '844 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the Cisco Accused Products, with knowledge and specific intention that such products will be used by its customers to support MAP-T and MAP-E functionality. For example, Cisco specifically instructs its customers (such as Charter) on how to use and implement the technology claimed in the '844 patent. *See, e.g.*, Carrier-Grade IPv6: Mapping Address and Port-Translation Technical Brief; IP Addressing: NAT Configuration Guide, Cisco IOS XE Gibraltar 16.11.x; Cisco ASR 9000 Series Aggregation Services Router CGv6 Configuration Guide, Release 5.3.x.

70. Charter also indirectly infringes the '844 Patent under 35 U.S.C. § 271(b).

71. Charter knowingly encourages and intends to induce infringement of the '844 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the Charter Accused Products, with knowledge and specific intention that such products will be used by its customers. For example, Charter instructs its customers on how to use and implement the technology claimed in the '844 patent. *See, e.g.*, : https://www.spectrumbusiness.net/support/internet/authorized-modems-spectrum-business-network; https://www.spectrum.net/support/internet/compliant-modems-charter-network/.

72. On information and belief, Cisco and Charter were aware of the '844 Patent and related Monarch patents that had been developed by France Telecom, had knowledge of the infringing nature of their activities, and nevertheless elected to perform and to continue to perform their infringing activities. At a minimum, Cisco and Charter are aware of the '844 Patent at least as of the filing of this complaint, and their continued support for the Cisco Accused Products and the Charter Accused Products constitutes indirect infringement of the '844 Patent.

73. Cisco's and Charter's infringement of the '844 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

74. As a result of Cisco's and Charter's infringement of the '844 Patent, Monarch has suffered monetary damages and seeks recovery in an amount adequate to compensate for Cisco's and Charter's infringement, but in no event less than a reasonable royalty with interest and costs.

SECOND COUNT

(Infringement of U.S. Patent No. 8,451,845)

75. Monarch incorporates by reference the allegations set forth in Paragraphs 1-74 of this Complaint as though fully set forth herein.

76. Cisco makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that directly infringe the '845 Patent, including the above identified Cisco

Accused Products that implement Mapping of Address and Port capabilities for Customer Equipment, such as Cisco 500 Series WPAN Industrial Routers. The Cisco Accused Products infringe at least claim 1 of the '845 Patent.

77. The Cisco Accused Products are programmed to implement a method for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, with the packet comprising an IPv6 destination address and an IPv6 source address. This method is executed, for example, in a home gateway adapted to connect a user terminal to the IPv6 domain.

78. The Cisco Accused Products, using Cisco 500 Series WPAN Industrial Routers as an example, support the MAP-T CE functionality, as defined in IETF RFC 7599.

> **Mapping of Address and Port using Translation (MAP-T)–The gateway provides shared or uniquely addressed IPv4 host connectivity to and across an IPv6 domain using MAP-T. The gateway implements the MAP Customer Edge (CE) functionality, as described in draft-ietf-software-map-t.** Each MAP domain must also include a device that implements the MAP-T Border Relay (BR) functionality (for example, the ASR 1000). The gateway configuration and management of MAP-T is done via CSMP and the CG-NMS.

Cisco IR500 Series WPAN Gateway and WPAN Range Extender Installation and Configuration Guide at 4 [hereinafter IR500 Guide].

79. As such, the Cisco Accused Products are designed with the capability to connect to an IPv6 domain (the MAP-T domain) and also connect to an IPv4 domain. This IPv4 domain may include, by way of example and not by way of limitation, Connected Grid Endpoint (CGE) devices and Distribution Automation (DA) devices.

> **WPAN Gateway and WPAN Range Extender and the Cisco Field Area Network**
>
> The WPAN gateway and WPAN range extender operate in the Cisco Connected Grid (CG) Field Area Network (FAN).
>
> The FAN solution provides an IPv6-based networking solution for connecting and managing a multitude of devices in a smartgrid architecture. The Cisco CG FAN consists of three components:
>
> - Connected Grid Endpoint (CGE) devices
> - Connected Grid Router (CGR) devices
> - Cisco Connected Grid Network Management System (CG-NMS)

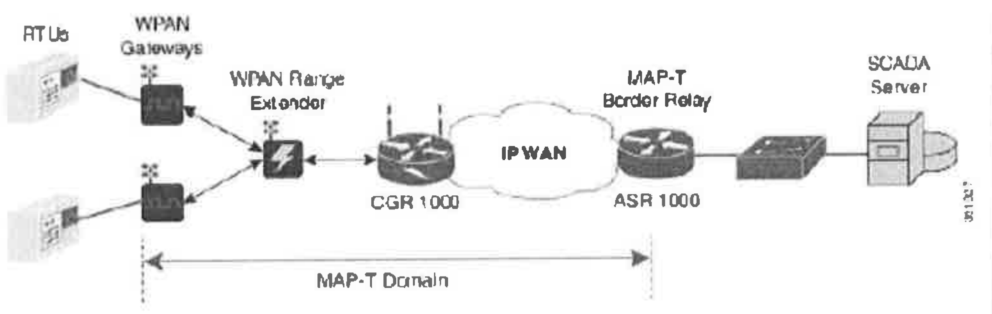
IR500 Guide at 2.

> The devices supply radio frequency (RF) mesh connectivity to IPv4/Ethernet and serial IoT devices, including recloser control, cap bank control, voltage regulator controls, and other endpoint controllers.
>
> The devices provide an open standards RF mesh solution based on the following standards:
>
> - IEEE 802.15.4 g/e
> - RFC6775–Neighbor Discovery Optimization for Low Power and Lossy Networks (6LoWPAN)
> - RFC6550–RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks
> - IETF MAP-T–Mapping of Address and Port using Translation (MAP-T)
> - RFC7252–The Constrained Application Protocol (CoAP)

IR500 Guide at 3.

80. The MAP-T domain is illustrated in the figure below from the Cisco documentation, showing a Cisco ASR 1000 operating as the MAP-T Border Relay on one edge of the domain and the Cisco Accused Products operating as MAP-T CE devices on the other edge of the domain.

Figure 5-5 MAP-T in a FAN and WPAN Gateway Scenario



IR500 Guide at 8. Thus, Cisco specifically instructs its customers how to implement an infringing system, and it designs and programs the Cisco Accused Products with the capability to support those infringing implementations.

81. When packets flow from the Border Relay to the Cisco Accused Products, those packets are traversing an IPv6-only domain and are received by the Cisco Accused Products as an IPv6 packet.

> **MAP-T**
>
> 6LoWPAN is an IPv6-only adaptation layer for the physical (PHY) and media access control (MAC) layer technologies implementing it. No IPv4 adaptation layer is defined for these PHY and MAC layers, so the Mapping of Address and Port using Translation (MAP-T) architecture is used as an IPv4-IPv6 translation mechanism. The "mapping of address and port" mechanism defines how IPv4 nodes can communicate over an IPv6-only infrastructure.

IR500 Guide at 8.

82. Accordingly, the IPv6 packets that are received by the Cisco Accused Product are comprised of a source and destination IPv6 address. The Accused Products comprise a home gateway by virtue of their connection to a private network of user terminals and a service provider network. *See* '845 Patent at 1:45-48 ("Below, the express 'home gateway' refers to any equipment for interconnecting a private network and a network operated by a service provider, the private network being either a home network or a business network.").

83. The IPv6 destination address of packets received by the Cisco Accused Products for delivery to Connected Grid Endpoints are constructed by concatenating an IPv6 Prefix, an IPv4 destination address, and a destination port number, per the Basic Mapping Rule and IETF RFC 7599. To facilitate traffic across MAP domains, the Cisco edge devices (Border Relay and Customer Edge devices) use mapping rules, referred to in the RFC as Basic Mapping Rule and Forwarding Mapping Rule. In each case, the Mapping Rule requires identification of the following: (1) Rule IPv6 prefix; (2) Rule IPv4 prefix; and (3) EA bit length.

```
Both mapping rules share the same parameters:

o  Rule IPv6 prefix (including prefix length)

o  Rule IPv4 prefix (including prefix length)

o  Rule EA-bit length (in bits)
```

IETF RFC 7597 at 9. MAP-T relies on this same rule structure.

```
5.  Mapping Rules

   The MAP-T algorithmic mapping rules are identical to those in
   Section 5 of the MAP-E specification [RFC7597], with the following
   exception: the forwarding of traffic to and from IPv4 destinations
   outside a MAP-T domain is to be performed as described in this
   document, instead of Section 5.4 of the MAP-E specification.
```

IETF RFC 7599 at 8.

84. The format of IPv6 packets received by the Cisco Accused Products is illustrated below. The address is constructed from an IPv6 prefix, a set of EA bits indicating the target IPv4 address and port, a subnet ID, and an interface ID that also includes the target IPv4 address.

```
Figure 3 shows the structure of the complete MAP IPv6 address as
specified in this document.

|     n bits          |  o bits    | s bits  |   128-n-o-s bits      |
+--------------------+-----------+---------+------------------------+
|  Rule IPv6 prefix  |  EA bits  |subnet ID|     interface ID       |
+--------------------+-----------+---------+------------------------+
|<---  End-user IPv6 prefix  --->|

                 Figure 3: MAP IPv6 Address Format

The Rule IPv6 prefix is common among all CEs using the same Basic
Mapping Rule within the MAP domain.  The EA bit field encodes the
CE-specific IPv4 address and port information.  The EA bit field,
```

IETF RFC 7597 at 12. This same address construction is relied in for MAP-T IPv6 address construction in the Cisco Accused Devices as well. *See* IETF RFC 7599 at Section 5.

85. The EA bits encode the destination IPv4 address and destination port.

```
Embedded Address (EA) bits:
                      The IPv4 EA-bits in the IPv6 address identify
                      an IPv4 prefix/address (or part thereof) or a
                      shared IPv4 address (or part thereof) and a
                      Port Set Identifier.
```

IETF RFC 7599 at 6. The EA bit encoding can take three different forms: (1) an IPv4 prefix address; (2) an IPv4 address; or (3) a shared IPv4 address and a Port Set Identifier (PSID). In the third form, the EA bits represent an encoding of both an IPv4 address and a destination port. This scenario is depicted below:

```
|    r bits    |        p bits         |         |  q bits   |
+-------------+---------------------+         +------------+
|  Rule IPv4  | IPv4 address suffix |         |Port Set ID |
+-------------+---------------------+         +------------+
|            32 bits                |

            Figure 6: Shared IPv4 Address
```

IETF RFC 7597 at 13. The combined Rule IPv4 network address and IPv4 address suffix form the IPv4 destination address in the Cisco Accused Products. The PSID identifies the destination port for the packet. The p bits and q bits form the EA bits that are included in the destination IPv6 address, and represent an encoding of the target IPv4 address and target IPv4 destination port.

86. Additionally, the IPv4 destination address is appended to the IPv6 operator prefix as part of the interface ID that forms the MAP IPv6 destination address. As illustrated above, the IPv6

address is comprised of a Rule IPv6 prefix, EA bits, a subnet ID, and an interface ID. The format of the interface ID, which includes the destination IPv4 address, is illustrated below:

```
6.  The IPv6 Interface Identifier

   The interface identifier format of a MAP-T node is the same as the
   format described in Section 6 of [RFC7597].  The format diagram is
   provided here for convenience:

                 |          128-n-o-s bits             |
                 | 16 bits|    32 bits     | 16 bits|
                 +--------+----------------+--------+
                 |   0    |  IPv4 address  |  PSID  |
                 +--------+----------------+--------+

                   Figure 2: IPv6 Interface Identifier
```

IETF RFC 7599 at 9.

87. The above-described address format components are discussed in the Cisco 500 Series documents as well.

MAP-T Basic Mapping Rule (BMR): the IPv6 and IPv4 prefixes used to address MAP-T nodes inside the MAP-T domain

- **BMR IPv4 prefix and prefix length are the IPv4 subnet selected to address all IPv4 nodes in a MAP-T domain.** For example, a MAP-T domain set-up with 153.10.10.0/24 as IPv4 subnet has all IPv4 nodes configured with IPv4 address from this subnet, BMR IPv4 prefix = 153.10.10.0 and prefix length = 24
- **BMR IPv6 prefix and prefix length are used to embed the IPv4 address of nodes inside the MAP-T domain.** For example, a MAP-T domain is configured with a MAP-T IPv6 BMR = 2031:6f8:147e:10::/56. Packets sent or received from IPv4 nodes inside the MAP-T domain have a translated IPv6 address based on this prefix, i.e. 2031:6f8:147e:10fe:99:a0a:fe00:0 for a MAP-T IPv4 node set-up with IPv4 153.10.10.254.
- BMR Share ratio: MAP-T being designed for various deployment scenarios, it could be feasible to allocate to a MAP-T node either an IPv4 prefix (smaller than the MAP-T BMR IPv4 prefix), or a single IPv4 address (/32) or share a single IPv4 address (/32) between several nodes. In the later case, it requires indicating how many bits for port numbers are assigned, which is called "BMR share ratio". In case of IR 500 deployment, it is recommended to use a single IPv4 address (/32) per IR 500 with a share ratio = 1 to keep the addressing simple.
- **BMR Embedded Address (EA) bits indicate** - in the case of share ration = 1 - the length of the IPv4 suffix embedded in the MAP-T IPv6 End-user IPv6 prefix. For example, in case of an IPv4 /24 prefix allocated to a MAP-T domain, the BMR EA value derived from it is 8.

IR500 Guide at 9

88. On receiving an IPv6 packet constructed in the manner described above, the Cisco Accused Products translate the IPv6 destination address to the IPv4 destination address embedded in the IPv6 destination address, per the Basic Mapping Rule.

> NAT44–The gateway uses NAT44 to translate private IPv4 addresses used by DA devices connected to the Ethernet port to public IPv4 addresses used with MAP-T.
>
> - Dynamic NAT44 performs translation for outgoing communications (Device to Server).
> - Static NAT44 performs translation for incoming communications (Server to Device).

IR500 Guide at 4. Once the constructed IPv6 address is replaced with the native IPv4 address and port, the packet can be delivered to the proper Connected Grid Endpoint, for example.

89. Once the IPv6 address is replaced with the native IPv4 destination address, it may be routed to its final destination in an IPv4 domain. The MAP-T RFC 7599 illustrates the Private IPv4 network through which received packets are routed.

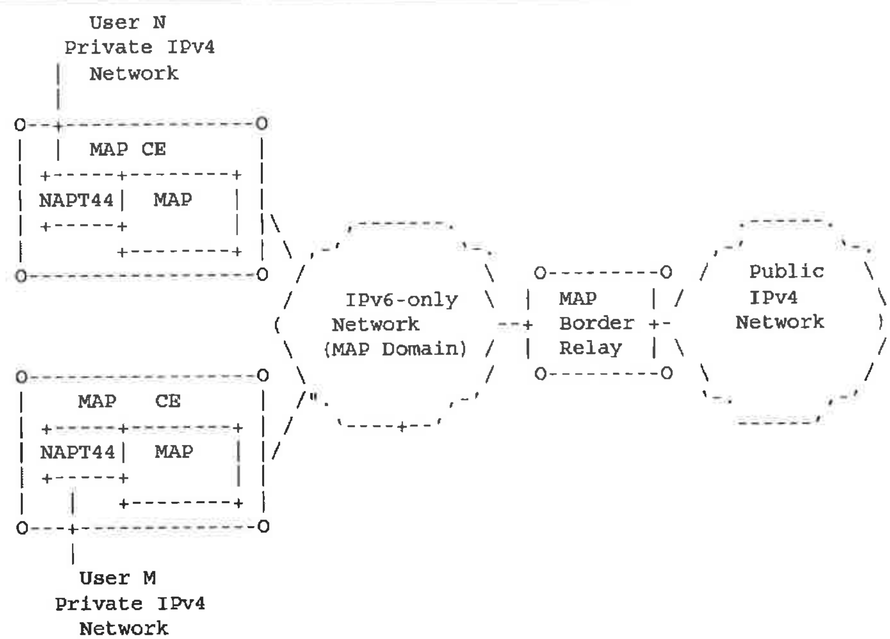
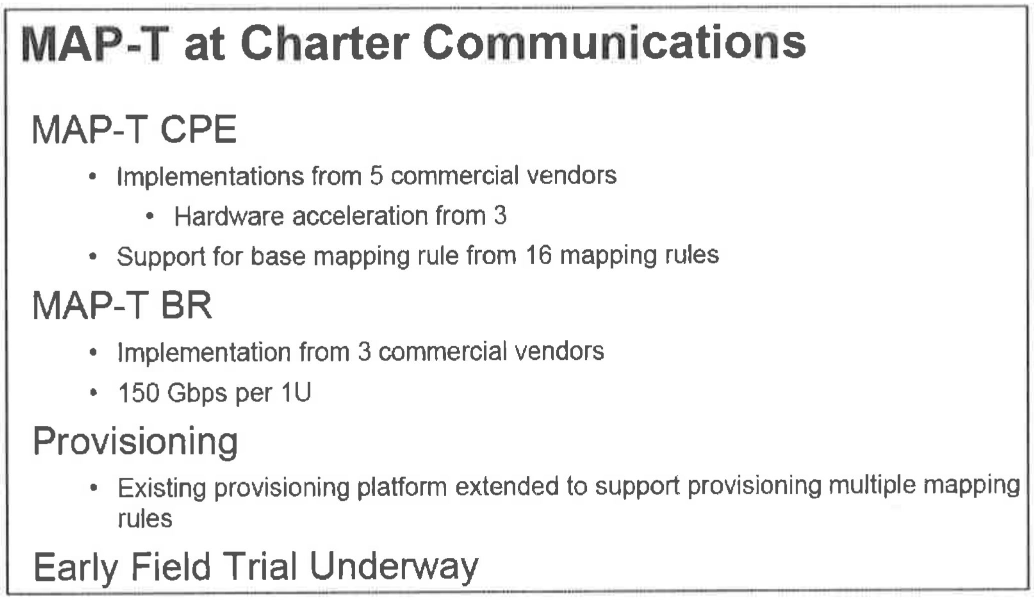


Figure 1: Network Topology

IETF RFC 7599 at 7.

90. As detailed above, Charter is a Cisco customer that has implemented MAP-T within its network. Accordingly, Charter's network uses equipment to implement the Border Relays (e.g., the ASR routers detailed earlier) as well as customer premises equipment to implement the MAP-CE capabilities. Charter engineer, E. Jordan Gottlieb, presented "Mapping of Address and Port using Translation (MAP-T)" at a North American Network Operators' Group (NANOG)

meeting/conference. See https://www.youtube.com/watch?v=ZmfYHCpfr_w . In that presentation, Charter indicated that it had implemented MAP-T in its network.



Gottlieb, Mapping of Address and Port using Translation (MAP-T) at 14.

91. Charter highlighted that its network uses customer premises equipment (CPE) from five commercial vendors and include support for base mapping rule from 16 mapping rules. Charter lists the modems it supports for its network at the following addresses: https://www.spectrumbusiness.net/support/internet/authorized-modems-spectrum-business-network; https://www.spectrum.net/support/internet/compliant-modems-charter-network/.

92. One or more of the Charter Accused Products provides the CPE support required for Charter's MAP-T implementation, which includes the support for RFC 7599 (MAP-T) as detailed above regarding the Cisco Accused Products.

93. By making, using, offering for sale, and/or selling products in the United States, and/or importing products into the United States, including but not limited to the Cisco Accused Products and Charter Accused Products, Cisco and Charter have injured Monarch and are liable to Monarch for directly infringing one or more claims of the '845 Patent, including without limitation claim 1 pursuant to 35 U.S.C. § 271(a).

94. Cisco also indirectly infringes the '845 Patent under 35 U.S.C. § 271(b).

95. Cisco knowingly encourages and intends to induce infringement of the '845 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the Cisco Accused Products, with knowledge and specific intention that such products will be used by its customers. For example, Cisco specifically instructs its customers how to use and implement the technology claimed in the '845 Patent and it designs and programs the Cisco Accused Products with that specific functionality. *See, e.g.*, IR500 Guide; Carrier-Grade IPv6: Mapping Address and Port-Translation Technical Brief.

96. Charter also indirectly infringes the '845 Patent under 35 U.S.C. § 271(b).

97. Charter knowingly encourages and intends to induce infringement of the '845 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the Charter Accused Products, with knowledge and specific intention that such products will be used by its customers. For example, Charter instructs its customers on how to use and implement the technology claimed in the '845 Patent. *See, e.g.*, : https://www.spectrumbusiness.net/support/internet/authorized-modems-spectrum-business-network; https://www.spectrum.net/support/internet/compliant-modems-charter-network/.

98. On information and belief, Cisco and Charter were aware of the '845 Patent and related Monarch patents, had knowledge of the infringing nature of their activities, and nevertheless continue their infringing activities. Cisco and Charter are aware of the '845 Patent at least as of the filing of this complaint.

99. Cisco's and Charter's infringement of the '845 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

100. As a result of Cisco's and Charter's infringement of the '845 Patent, Monarch has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty with interest and costs.

THIRD COUNT

(Infringement of U.S. Patent No. 9,019,965)

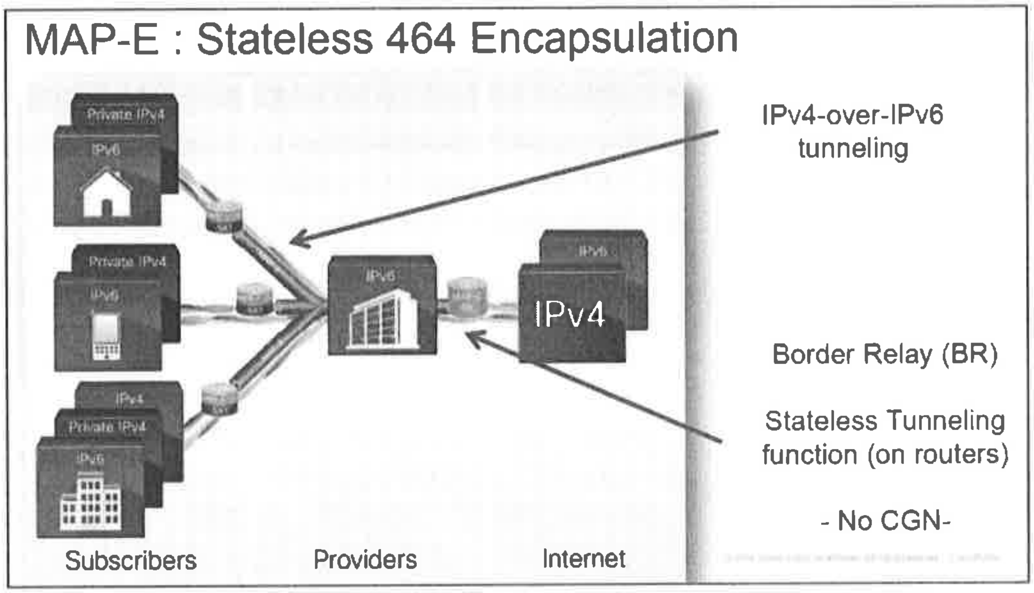
101. Monarch incorporates by reference the allegations set forth in Paragraphs 1-100 of this Complaint as though fully set forth herein.

102. Cisco makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that directly infringe the '965 Patent, including the above identified Cisco Accused Products. The Cisco Accused Products infringe at least claim 3 of the '965 Patent.

103. The Cisco Accused Products comprise devices that are capable of routing an IPv4 data packet sent by a source terminal belonging to a first IPv4 domain, via an IPv6 domain, to a destination terminal belonging to a second private IPv4 domain. As sold, the Cisco Accused Products include a processor and memory programmed to route packets as described below, and thus directly infringe the '965 Patent.

104. As noted supra regarding the '844 Patent, the Cisco Accused Products support MAP-E functionality.

105. The Cisco Accused Products, which are programmed with the MAP-E functionality, are capable of being used as MAP Border Relays, in which they connect to a first IPv4 network and communicate with a second private IPv4 network via an IPv6 network. This configuration is specifically noted in Cisco documentation:



Cisco Live! 2016 Presentation, BRKSPG-2300 at 38.

106. To facilitate traffic across MAP-E domains for example, the edge devices (Border Relay and Customer Edge devices) use mapping rules, referred to in the RFCs as Basic Mapping Rule and Forwarding Mapping Rule. In each case, the Mapping Rule requires identification of the following: (1) Rule IPv6 prefix; (2) Rule IPv4 prefix; and (3) EA bit length.

```
Both mapping rules share the same parameters:

o  Rule IPv6 prefix (including prefix length)

o  Rule IPv4 prefix (including prefix length)

o  Rule EA-bit length (in bits)
```

IETF RFC 7597 at 9. For example, Cisco describes the manner in which it implements the Basic Mapping Rule in its product documentation:

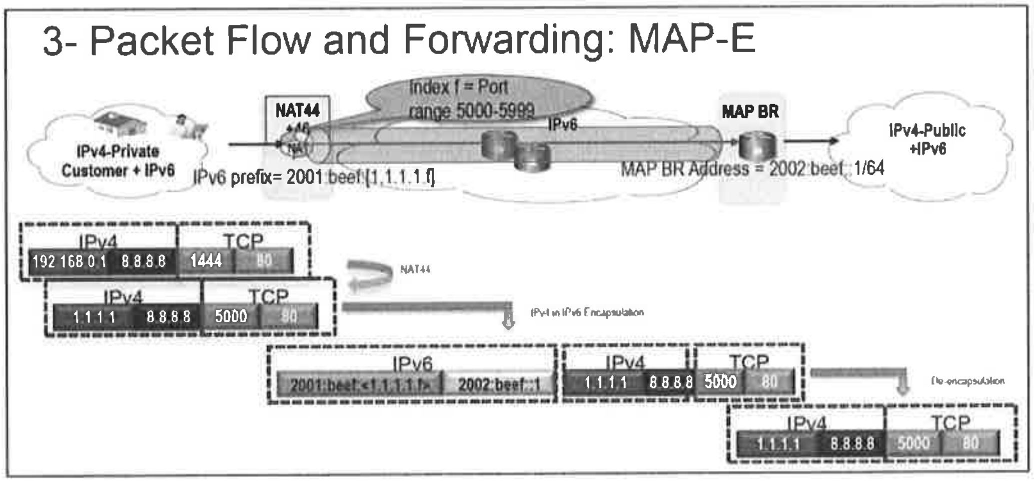
> MAP-E refers to Mapping of Address and Port Encapsulation (MAP-E). The MAP-E feature enables you to configure mapping rules for translation between IPv4 and IPv6 addresses. Each mapping of address and port using MAP-E domain uses a different mapping rule. A MAP-E configuration comprises of one basic mapping rule (BMR), one default mapping rule (DMR), and one or more forwarding mapping rules (FMRs) for each MAP-E domain.
>
> **A BMR configures the MAP IPv6 address or prefix.** You can configure only one BMR per IPv6 prefix. The MAP-E CE uses the BMR to configure itself with an IPv4 address, an IPv4 prefix, or a shared IPv4 address from an IPv6 prefix. **A BMR can also be used for forwarding packets in such scenarios where an IPv4 destination address and a destination port are mapped into an IPv6 address/prefix.** Every MAP-E node (CE device is a MAP-E node) must be provisioned with a BMR. The BMR prefix along with the port parameter is used as tunnel destination address. You can use the **port-parameters** command to configure port parameters for the MAP-E BMR.

IP Addressing: NAT Configuration Guide, Cisco IOS XE Gibraltar 16.11.x at 154.

107. When a packet is received by a Cisco Accused Product with a destination IPv4 address that matches the IPv4 address prefix of a mapping rule, the Cisco Accused Product constructs an IPv6 address for transmitting the packet to the destination of the IPv4 packet. The destination IPv6 address is constructed as described below in the MAP-E RFC 7597. It involves concatenating an IPv6 prefix and a sequence of EA bits (representing the target IPv4 address and port number).

```
Figure 3 shows the structure of the complete MAP IPv6 address as
specified in this document.

|     n bits         |  o bits   | s bits  |   128-n-o-s bits      |
+--------------------+-----------+---------+-----------------------+
|  Rule IPv6 prefix  |  EA bits  |subnet ID|     interface ID      |
+--------------------+-----------+---------+-----------------------+
|<---  End-user IPv6 prefix  --->|

                 Figure 3: MAP IPv6 Address Format

The Rule IPv6 prefix is common among all CEs using the same Basic
Mapping Rule within the MAP domain.  The EA bit field encodes the
CE-specific IPv4 address and port information.  The EA bit field,
```

IETF RFC 7597 at 12. The construction of an IPv6 address for MAP-E is depicted graphically below.

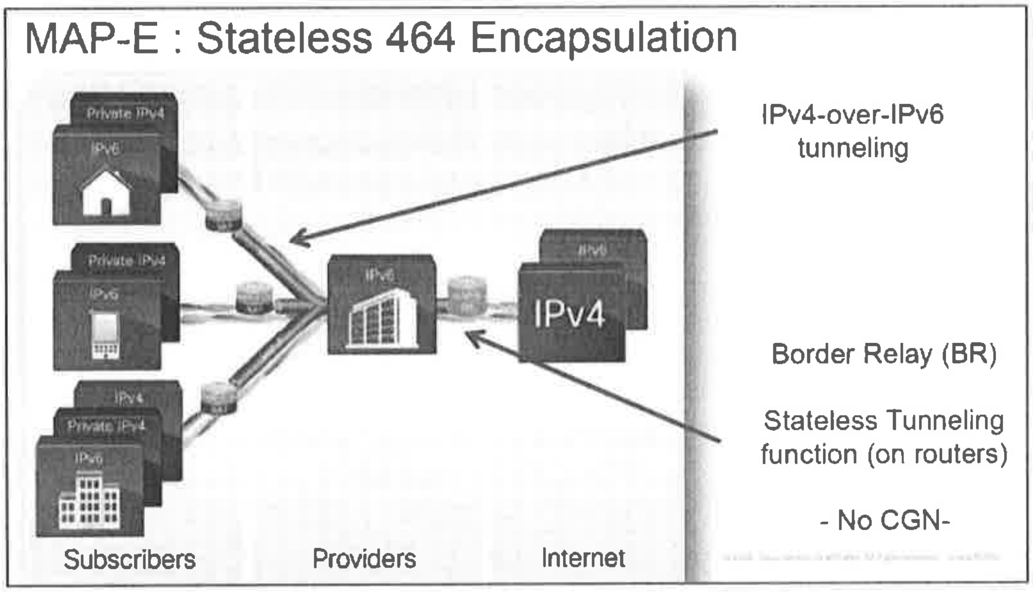


Cisco Live! 2016 Presentation, BRKSPG-2300 at 49.

108. The Cisco Accused Products encapsulate the IPv4 data packet in an IPv6 data packet carrying said IPv6 destination address. As its name indicates, MAP-E is an IPv4 to IPv6 solution based on encapsulation.

> Mapping of Address and Port with Encapsulation (MAP-E)
>
> Abstract
>
> This document describes a mechanism for transporting IPv4 packets across an IPv6 network using IP encapsulation. It also describes a generic mechanism for mapping between IPv6 addresses and IPv4 addresses as well as transport-layer ports.

IETF RFC 7597 at 1. Cisco refers to this encapsulation as stateless.



Cisco Live! 2016 Presentation, BRKSPG-2300 at 38.

109. The address constructed as described above is the destination address for the IPv6 packet that encapsulates the received IPv4 packet. Once the IPv6 packet is constructed, it is routed through the IPv6 MAP domain per standard IPv6 routing mechanisms using the newly constructed IPv6 destination address.

110. The Cisco Accused Products include the capability to construct the IPv6 destination address by combining an IPv6 prefix and the private IPv4 address of said destination terminal in the MAP Border Relay that interfaces an IPv4 domain and an IPv6 network. Based on the Basic Mapping Rule that is provisioned to all CEs and BRs in the MAP domain, the EA bits (which describe the CE's IPv4 address and allowable port set) that are combined with the IPv6 prefix to construct the IPv6 destination address comprise the IPv4 destination address of the destination terminal. To the extent that the destination terminal uses an external facing private IPv4 address, the IPv4 address used to construct the IPv6 address is a private IPv4 address. The MAP-E RFC does not prohibit the use of external-facing private IP addresses on CE devices.

111. The MAP-E RFC graphically depicts how the IPv4 address and port numbers are encoded into the EA bits, which are then concatenated with the IPv6 address prefix to form an IPv6 destination address for the packet.

```
|        32 bits           |         |      16 bits        |
+--------------------------+         +-------------------+
| IPv4 destination address |         |  IPv4 dest port   |
+--------------------------+         +-------------------+
                :          :           ___/       :
                |  p bits  |          /  q bits   :
                +----------+         +------------+
                |IPv4 suffix|        |Port Set ID |
                +----------+         +------------+
                \          /    ____/    ________/
                  \       :  __/    _____/
                    \     : /      /
|     n bits         |  o bits   | s bits  |   128-n-o-s bits     |
+--------------------+-----------+---------+------------+----------+
|  Rule IPv6 prefix  |  EA bits  |subnet ID|     interface ID      |
+--------------------+-----------+---------+-----------------------+
|<---  End-user IPv6 prefix  --->|

            Figure 7: Derivation of MAP IPv6 Address
```

IETF RFC 7597 at 14. The EA bits permit the IPv4 destination address to be determined.

112. Additionally, the Cisco Accused Products include the capability to append the IPv4 destination address to the IPv6 operator prefix as part of the interface ID that forms the MAP IPv6 destination address. As illustrated above, the IPv6 address is comprised of a Rule IPv6 prefix, EA bits, a subnet ID, and an interface ID. The format of the interface ID, which includes the destination IPv4 address, is illustrated below:

```
6.  The IPv6 Interface Identifier

   The interface identifier format of a MAP node is described below.

                |              128-n-o-s bits              |
                | 16 bits|    32 bits     | 16 bits|
                +--------+----------------+--------+
                |   0    |  IPv4 address  |  PSID  |
                +--------+----------------+--------+

                  Figure 8: IPv6 Interface Identifier
```

IETF RFC 7597 at 15.

113. By making, using, offering for sale, and/or selling products in the United States, and/or importing products into the United States, including but not limited to the Cisco Accused Products, Cisco has injured Monarch and is liable to Monarch for directly infringing one or more claims of the '965 Patent, including without limitation claim 3 pursuant to 35 U.S.C. § 271(a).

114. Cisco also indirectly infringes the '965 Patent under 35 U.S.C. § 271(b).

115. Cisco knowingly encourages and intends to induce infringement of the ’965 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing them into the United States, including but not limited to the Cisco Accused Products, with knowledge and specific intention that such products will be used by its customers. For example, Cisco instructs its customers on how to use and implement the technology claimed in the ’965 Patent. *See, e.g.*, Carrier-Grade IPv6: Mapping Address and Port-Translation Technical Brief; IP Addressing: NAT Configuration Guide, Cisco IOS XE Gibraltar 16.11.x; Cisco ASR 9000 Series Aggregation Services Router CGv6 Configuration Guide, Release 5.3.x.

116. On information and belief, Cisco was aware of the ’965 Patent and related Monarch patents invented by France Telecom, had knowledge of the infringing nature of its activities, and nevertheless continues its infringing activities. At a minimum, Cisco is aware of the ’965 Patent since at least the filing date of this complaint.

117. Cisco’s infringement of the ’965 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys’ fees pursuant to 35 U.S.C. §§ 284-285.

118. As a result of Cisco’s infringement of the ’965 Patent, Monarch has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco’s infringement, but in no event less than a reasonable royalty with interest and costs.

FOURTH COUNT

(Infringement of U.S. Patent No. 8,130,775)

119. Monarch incorporates by reference the allegations set forth in Paragraphs 1-118 of this Complaint as though fully set forth herein.

120. Cisco makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that directly infringe the ’775 Patent, including the above identified Cisco Accused Products that use VPLS LSM such as ASR 9000 Series routers and any other products with similarly functionality.

121. For example, Cisco Accused Products infringe at least claim 6 of the '775 Patent in at least the manner described below.

122. The Cisco ASR 9000 Series Routers include and execute computer code in the form of Cisco IOS XR software (Version 5.1 or later) that is stored on a non-transitory computer-readable medium associated with the ASR 9000 Routers.

> **Introduction**
>
> This document describes Virtual Private LAN Service (VPLS) Label Switched Multicast (LSM) for the Aggregation Services Router (ASR) 9000 Series that run Cisco IOS® XR software.

ASR 9000 Overview[1] at 1.

123. The computer code comprises instructions for implementing a method of automatically configuring at least two pseudo-wires able to broadcast a data stream when said program is executed by a computer. Starting at least with IOS XR Release 5.1, the ASR 9000 Router implements Label Switched Multicast with point-to-multipoint traffic engineering (P2MP-TE) for delivering broadcast, multicast and certain unicast streams to a VPLS domain using pseudo-wires.

> **VPLS LSM Configuration**
>
> P2MP Auto Tunnel Configuration
>
> MPLS TE Fast Reroute (FRR) Configuration
>
> L2VPN Configuration

ASR 9000 Overview at 1.

[1] *ASR 9000 VPLS Label Switched Multicast (LSM) Overview and Configuration Example*, updated April 1, 2014, Document ID 117570, *available at* https://www.cisco.com/c/en/us/support/docs/routers/asr-9000-series-aggregation-services-routers/117570-configure-vpls-00.pdf ("ASR 9000 Overview").

> **VPLS LSM Features**
>
> VPLS is a widely-deployed service provider L2VPN technology that is also used for multicast transport. Although L2 technology allows snooping to be used in order to optimize replication of multicast traffic into L2 pseudowires, the core remains agnostic to multicast traffic. As a result, multiple copies of the same flow traverse core networks. In order to mitigate this inefficiency, pair LSM with VPLS in order to introduce LSM multicast trees over the core. In Cisco IOS-XR Software Release 5.1.0, Cisco ASR 9000 Series implement VPLS LSM with point-to-multipoint traffic engineering (P2MP-TE) inclusive trees. VPLS end points are automatically discovered and P2MP-TE trees are set up with the use of Resource Reservation Protocol Traffic Engineering (RSVP-TE) without operational intervention.

ASR 9000 Overview at 2.

> - The VPLS LSM solution employs P2MP LSPs in the MPLS core in order to carry broadcast, multicast, and unknown unicast traffic for a VPLS domain.
> - P2MP LSPs allow replication in the MPLS network at the most optimal node and minimize the amount of packet replication in the network.

ASR 9000 Overview at 3.

124. The Cisco VPLS LSM solution involves automatically creating P2MP unidirectional pseudo-wires using computer code provided on the Cisco ASR 9000 Series Routers.

> - P2MP PWs are unidirectional as opposed to P2P PWs, which are bidirectional.
> - The VPLS LSM solution involves the creation of a P2MP PW per VPLS domain in order to emulate a VPLS P2MP service for core PWs in the VPLS domain.
> - VPLS LSM is supported in Cisco IOS XR Release 5.1.0 and later.
>
> **VPLS LSM Restrictions**
>
> - Cisco IOS-XR Release 5.1.0 VPLS LSM functionality supports only MPLS Traffic Engineering P2MP-TE trees set up with RSVP-TE.
> - A P2MP PW can be signaled with the BGP protocol only in Cisco IOS-XR Release 5.1.0. In this first phase, the remote PEs that participate in the VPLS domain are auto-discovered with BGP Auto-Discovery (BGP-AD).

ASR 9000 Overview at 3.

> - VPLS LSM overcomes the drawbacks of ingress replication.
> - The VPLS LSM solution employs P2MP LSPs in the MPLS core in order to carry broadcast, multicast, and unknown unicast traffic for a VPLS domain.
> - P2MP LSPs allow replication in the MPLS network at the most optimal node and minimize the amount of packet replication in the network.
> - The VPLS LSM solution only sends flooded VPLS traffic over P2MP LSPs.

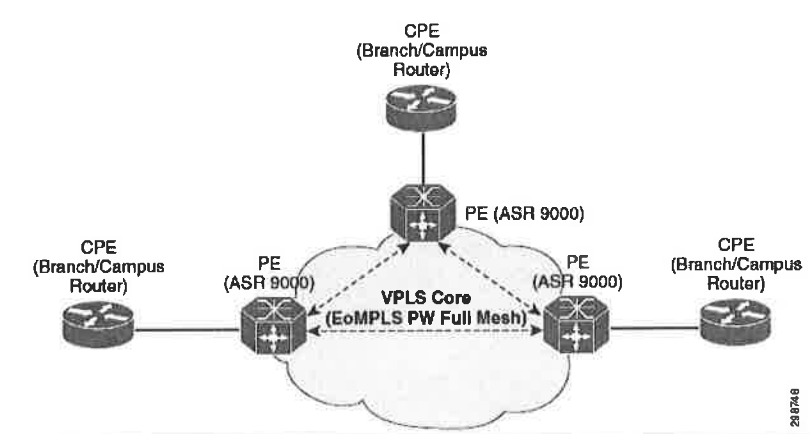
ASR 9000 Overview at 2–3.

125. Cisco describes VPLS as a multipoint L2VPN technology allowing connection between two or more enterprise locations in a single LAN-like bridge domain over the MPLS transport infrastructure.

> **Virtual Private LAN Service (VPLS)**
>
> VPLS is a multipoint L2VPN technology that connects two or more enterprise locations in a single LAN like bridge domain over the MPLS transport infrastructure. Multiple enterprise locations in a VPLS domain can communicate with each other over VPLS core. This is achieved by using VFI, attaching local ACs and full mesh of pseudo-wires between provider edges to the VFI as described below (Figure 3-2).

ASR9000 Implementation Guide[2] at 32.

Figure 3-2 VPLS



ASR9000 Implementation Guide at 32.

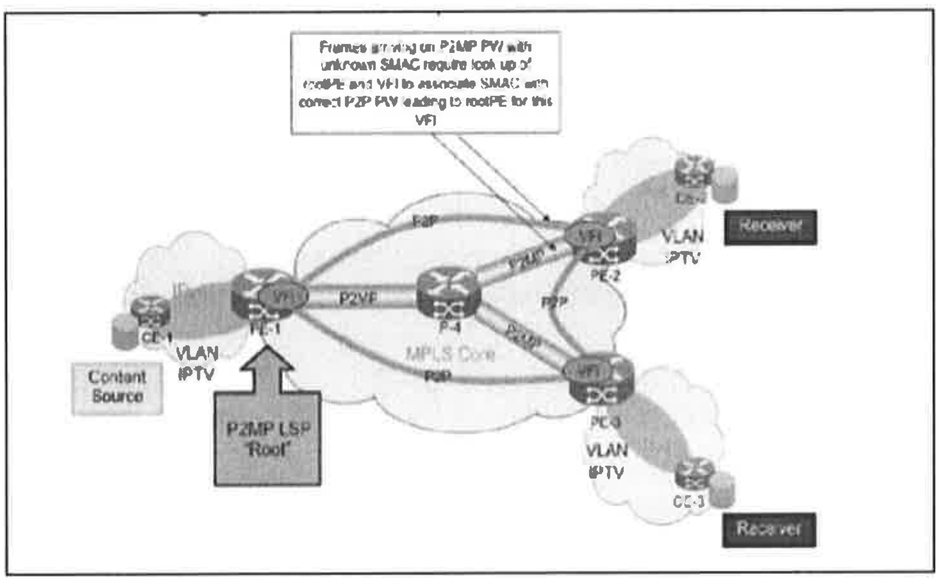
[2] Cisco ASR9000 Enterprise L2VPN for Metro-Ethernet, DC-WAN, WAN Core, and Government and Public Networks Implementation Guide *available at* https://studylib.net/doc/14395431/cisco-asr9000-enterprise-l2vpn-for-metro-ethernet--dc-wan ("ASR9000 Implementation Guide").

126. Cisco describes VPLS LSM as advantageous for eliminating unnecessary ingress replication, and thus is especially advantageous in multicasting/broadcasting streams to a large group of customers.

> VPLS Label-Switched Multicast (LSM) overcomes these drawbacks. The VPLS LSM solution employs point-to-multipoint (P2MP) label-switched paths (LSPs) in the MPLS core to carry broadcast, multicast, and unknown unicast traffic for a VPLS domain. P2MP LSP allows replication in the MPLS core at most optimal node in the MPLS network and minimizes the number of packet replications in the network. VPLS LSM solution sends only VPLS traffic that requires flooding over P2MP LSPs. Unicast VPLS traffic is still sent over P2P pseudo-wires. Traffic sent over access pseudo-wires in the case of MPLS access, continues to be sent using normal replication. P2MP pseudo-wires are unidirectional as opposed to P2P pseudo-wires that are bidirectional.
>
> The VPLS LSM solution involves creating a P2MP pseudo-wire-per-VPLS domain to emulate VPLS P2MP service for core pseudo-wires in the VPLS domain. The P2MP pseudo-wire is supported over the P2MP LSP called P-tree. This P-tree-based P2MP LSP is created by using RSVP signaling.

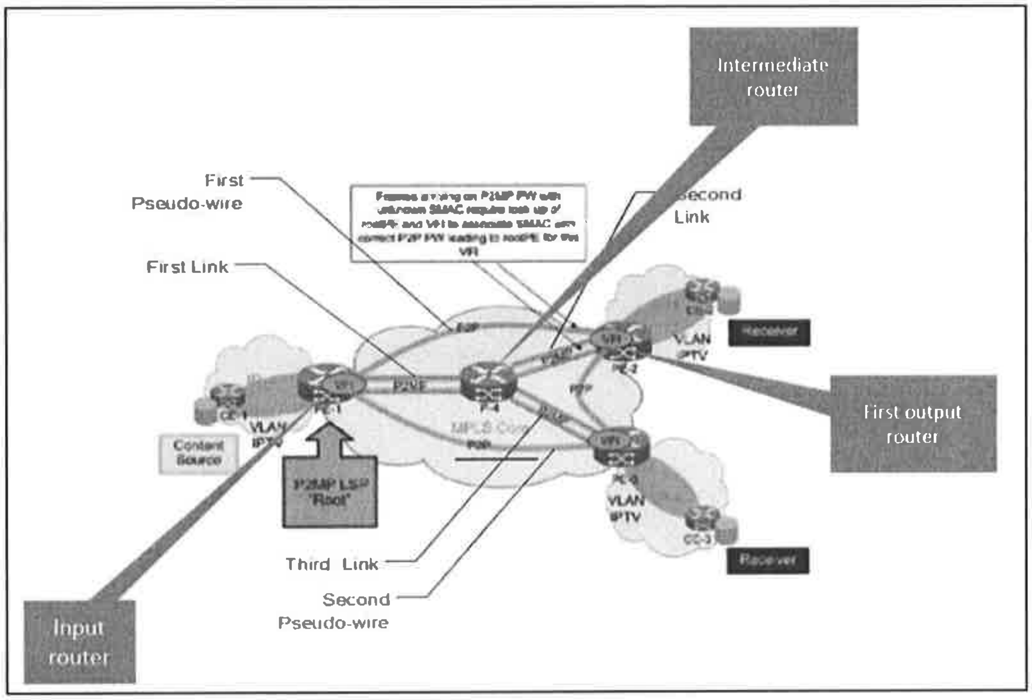
ASR9000 Implementation Guide at 81.

127. Virtual Private LAN Service (VPLS) in the ASR 9000 Routers provides point to multipoint (P2MP) communication over IP or MPLS networks, allowing geographically dispersed sites to share a multicast/broadcast domain by connecting nodes through P2MP Pseudo-wires.



ASR 9000 Overview at 4.

128. In the Cisco Configuration example for constructing a VPLS LSM network, an MPLS Core enables packet switching in the network based on labels. The first output router is designated as PE-2 in the Cisco example, the second output router is designated as PE-3, the bud node PE is the intermediate router (P-4), and the input router is PE-1.



ASR 9000 Overview at 4 (annotations added). As the Cisco documentation describes, a Cisco ASR 9000 Series Router is capable of automatically setting up P2MP-TE trees "without operational intervention":

> the core. In Cisco IOS-XR Software Release 5.1.0, Cisco ASR 9000 Series implement VPLS LSM with point-to-multipoint traffic engineering (P2MP-TE) inclusive trees. VPLS end points are automatically discovered and P2MP-TE trees are set up with the use of Resource Reservation Protocol Traffic Engineering (RSVP-TE) without operational intervention.

ASR 9000 Overview at 2.

129. The Cisco Overview and Configuration Example indicates that a frame arriving on the P2MP pseudo-wire at PE-2 from PE-1 via P-4 is treated as if the frame arrived on a P2P pseudo-wire between PE-1 and PE-2.

> MAC learning on the Leaf PE for a frame that arrives on P2MP PW is done as if the frame is received on the P2P PW leading to the Root PE for that P2MP PW. In this image, MAC Learning on PE-2 for frames that arrive on the P2MP PW LSP rooted at PE-1 is done as if the frame arrived on the P2P PW between PE-1 and PE-2. The L2VPN control plane is responsible for programming the VPLS disposition information with P2P PW information for MAC learning on the P2MP LSP disposition.

ASR 9000 Overview at 3.

130. According to the Cisco Configuration guidance, P2MP pseudo-wires are automatically created by the Cisco 9000 Series Router between PE-1, PE-2, and PE-3 with a P router (P-4) configured as an intermediate (or bud) node. Because P2MP pseudo-wires are unidirectional, a separate P2MP pseudo-wire may be created in each direction if traffic is two-way.

> The P2MP tunnels are auto-discovered tunnels. Static P2MP tunnels are **not** supported.
>
> Static tunnel configurations are not used. The auto P2MP tunnel configuration must be enabled on all of the PE routers and also on a P router if it acts as a bud node. A bud node is a midpoint and tailend router at the same time.
>
> A sample topology with configuration is shown here. In this topology, P2MP PWs are created between the three PEs and a P router which acts as a bud node. All three PE routers act as Head (for ingress traffic) and Tail (for egress traffic).

ASR 9000 Overview at 5-6. During auto-configuration, the PE1 router is connected to the P router.

PE1 Configuration

```
RP/0/RSP0/CPU0:PE1#show run
hostname PE1

interface GigabitEthernet0/1/1/0
 description connected P router
 ipv4 address 209.165.201.1 255.255.255.224
```

P Configuration

```
RP/0/RSP0/CPU0:P#show run
hostname P

interface GigabitEthernet0/1/1/0
 description connected to PE1 router
 ipv4 address 209.165.201.2 255.255.255.224
 transceiver permit pid all
```

ASR 9000 Overview at 6–8. During auto-configuration, the PE bud node router is connected to the PE2 router as a second link.

PE2 Configuration

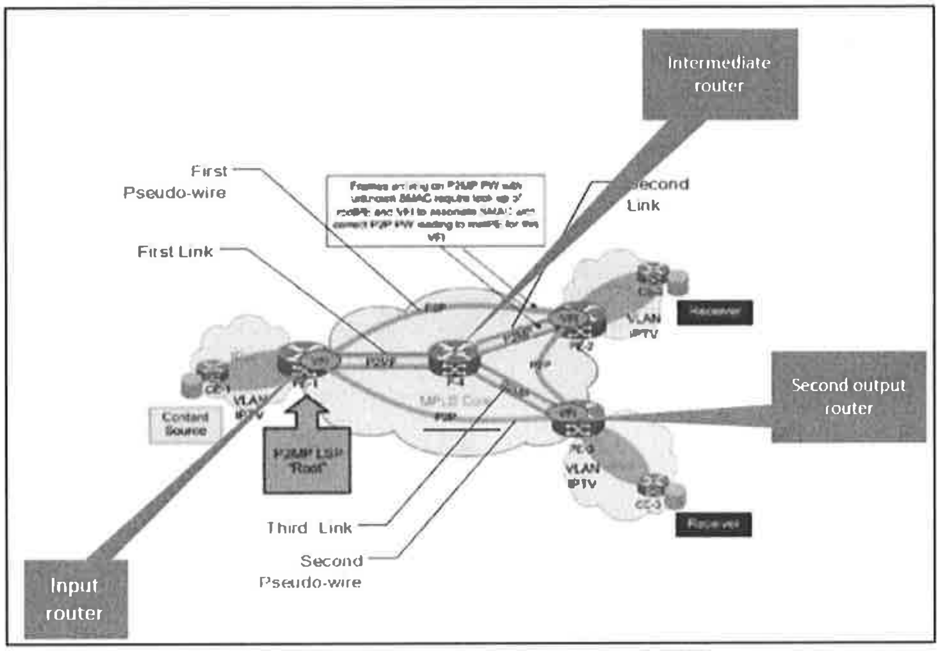
```
RP/0/RSP0/CPU0:PE2#show run
hostname PE2

interface GigabitEthernet0/[illegible]
 description connected to P router
 ipv4 address 209.165.201.62 255.255.255.224
 transceiver permit pid all
```

P Configuration

```
RP/0/RSP0/CPU0:P#show run
hostname P

interface GigabitEthernet0/1/1/3
 description connected to PE2 router
 ipv4 address 209.165.201.61 255.255.255.224
```

ASR 9000 Overview 8–10.

131. As described above, the first output router is PE-2, the second output router is PE-3, the bud PE is the intermediate router (P-4), and the input router is PE-1.



ASR 9000 Overview at 4 (annotations added).

132. During auto-configuration, the PE1 router is connected to the P router (see evidence cited above). During auto-configuration, the P router is also connected to the PE3 router as a third link.

PE3 Configuration	**P Configuration**
RP/0/RSP0/CPU0:PE3#**show run**	RP/0/RSP0/CPU0:P#**show run**
hostname PE3	hostname P
interface GigabitEthernet0/2/1/8	interface GigabitEthernet0/1/1/8
description connected to P router	description connected to PE3 router
ipv4 address 209.165.201.102 255.255.255.224	ipv4 address 209.165.201.101 255.255.255.224
transceiver permit pid all	

ASR 9000 Overview at 8, 12.

133. The Cisco Configuration Guide shows the configuration of the underlying P2MP sub-LSP and pseudo-wires (Bridge Domain – L2VPN) confirming the link between the input router and Intermediate router is used for both the pseudo-wires terminating at the PE2 and PE3 and traversing the intermediate, a.k.a. bud, router. The Loopback addresses are (identifying only the last octate):

PE1: - .225

P: -.226

PE2: -.227

PE3: -.228

```
RP/0/RSP0/CPU0:PE1#show l2vpn bridge-domain

  List of VFIs:
    VFI bg1_bd1_vfi (up)
      P2MP: RSVP-TE, BGP, 1, Tunnel Up
      Neighbor 209.165.200.226 pw-id 1, state: up, Static MAC addresse
      Neighbor 209.165.200.227 pw-id 1, state: up, Static MAC addresse
      Neighbor 209.165.200.228 pw-id 1, state: up, Static MAC addresse
 RP/0/RSP0/CPU0:PE1#
```

ASR 9000 Overview at 14.

134. The PE1 pseudo-wire paths are to the P router destination (209.165.200.226), the PE2 router destination (209.165.200.227) and to the PE3 router destination (209.165.200.228).

```
RP/0/RSP0/CPU0:PE1#show mpls traffic-eng tunnels p2mp

Name: tunnel-mte100 (auto-tunnel for VPLS (l2vpn))
   Signalled-Name: auto_PE1_mt100

Destination summary: (3 up, 0 down, 0 disabled) Affinity: 0x0/0xffff
Auto-bw: disabled
Destination: 209.165.200.226
  State: Up for 00:32:35
  Path options:
    path-option 10 dynamic      [active]
Destination: 209.165.200.227
  State: Up for 00:25:41
  Path options:
    path-option 10 dynamic      [active]
Destination: 209.165.200.228
  State: Up for 00:22:55
  Path options:
    path-option 10 dynamic      [active]
```

ASR 9000 Overview at 17-18.

135. The Path for the underlying S2L Sub-LSP confirms that the link 209.165.201.2 is used for both S2L LSPs to PE2 and PE3 confirming that this link is common to first and second P2MP pseudo-wires.

```
S2L Sub LSP: Destination 209.165.200.227 Signaling Status: connected
  S2L up for: 00:25:41 (since Tue Feb 18 04:05:25 UTC 2014)
  Sub Group ID: 2 Sub Group Originator ID: 209.165.200.225
  Path option path-option 10 dynamic    (path weight 2)
  Path info (OSPF 100 area 0)
    209.165.201.2
    209.165.201.61
    209.165.201.62
    209.165.200.227
```

```
S2L Sub LSP: Destination 209.165.200.228 Signaling Status: connected
  S2L up for: 00:22:55 (since Tue Feb 18 04:08:11 UTC 2014)
  Sub Group ID: 4 Sub Group Originator ID: 209.165.200.225
  Path option path-option 10 dynamic    (path weight 2)
  Path info (OSPF 100 area 0)
    209.165.201.2
    209.165.201.101
    209.165.201.102
    209.165.200.228
```

ASR 9000 Overview at 18.

```
RP/0/RSP0/CPU0:PE1#show mpls traffic-eng tunnels p2mp tabular

           Tunnel   LSP     Destination          Source               FRR   LSP  Path
             Name    ID         Address         Address  State  State Role  Prot
----------------- ----- --------------- --------------- ------ ------ ---- -----
   ^tunnel-mte100 10004 209.165.200.226 209.165.200.225     up  Ready Head
   ^tunnel-mte100 10004 209.165.200.227 209.165.200.225     up  Ready Head
   ^tunnel-mte100 10004 209.165.200.228 209.165.200.225     up  Ready Head
     auto_P_mt100 10005 209.165.200.225 209.165.200.226     up  Inact Tail
   auto_PE2_mt100 10003 209.165.200.225 209.165.200.227     up  Inact Tail
   auto_PE3_mt100 10004 209.165.200.225 209.165.200.228     up  Inact Tail
* = automatically created backup tunnel
^ = automatically created P2MP tunnel
RP/0/RSP0/CPU0:PE1#
```

ASR 9000 Overview at 20.

136. By making, using, offering for sale, and/or selling products in the United States, and/or importing products into the United States, including but not limited to the Cisco Accused Products, Cisco has injured Monarch and is liable to Monarch for directly infringing one or more claims of the ’775 Patent, including without limitation claim 6 pursuant to 35 U.S.C. § 271(a).

137. Cisco also indirectly infringes the ’775 Patent under 35 U.S.C. § 271(b).

138. Cisco knowingly encourages and intends to induce infringement of the ’775 Patent by making, using, offering for sale, and/or selling products in the United States, and/or importing

them into the United States, including but not limited to the Cisco Accused Products, with knowledge and specific intention that such products will be used by its customers. For example, Cisco instructs its customers on how to use and implement the technology claimed in the '775 Patent. *See, e.g.*, ASR 9000 Overview; ASR9000 Implementation Guide.

139. On information and belief, Cisco was aware of the '775 Patent and related Monarch patents invented by France Telecom, had knowledge of the infringing nature of its activities, and nevertheless continues its infringing activities. At least by the filing date of this Complaint, Cisco was aware of the infringement allegations regarding the '775 patent contained herein.

140. Cisco's infringement of the '775 Patent has been and continues to be deliberate and willful, and, this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

141. As a result of Cisco's infringement of the '775 Patent, Monarch has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty with interest and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment and seeks relief against Cisco and Charter as follows:

(a) For judgment that U.S. Patent Nos. 8,451,844; 8,451,845; 9,019,965; and 8,130,775 have been and continue to be infringed by Cisco;

(b) For judgment that U.S. Patent Nos. 8,451,844 and 8,451,845 have been and continue to be infringed by Charter;

(c) For an accounting of all damages sustained by Plaintiff as the result of Cisco's and Charter's acts of infringement;

(d) For finding that Cisco's and Charter's infringement is willful and enhancing damages pursuant to 35 U.S.C. § 284;

(e) For a mandatory future royalty payable on each and every future sale by Cisco and/or Charter of a product that is found to infringe one or more of the Asserted Patents and on all future products that are not colorably different from products found to infringe;

(f) For an award of attorneys' fees pursuant to 35 U.S.C. § 285 or otherwise permitted by law;

(g) For all costs of suit; and

(h) For such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure and Local Rule CV-38, Plaintiff demands a trial by jury of this action.

Dated: January 21, 2020

Respectfully submitted,
/s/ Max L. Tribble

Max L. Tribble Jr.
Texas Bar No. 20213950
mtribble@susmangodfrey.com
Joseph S. Grinstein
Texas Bar No. 24002188
jgrinstein@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, Texas 77002
Telephone: (713) 651-9366
Facsimile: (713) 654-6666

Steven M. Shepard
New York Bar No. 5291232
sshepard@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas 32nd Floor
New York, NY 10019
Telephone: (212) 336-8330
Facsimile: (212) 336-8340

Michael F. Heim
Texas Bar No. 09380923
mheim@hpcllp.com
R. Allan Bullwinkel
Texas Bar No. 24064327
abullwinkel@hpcllp.com

Alden G. Harris
Texas Bar No. 24083138
aharris@hpcllp.com
HEIM, PAYNE & CHORUSH, LLP
1111 Bagby St. Ste. 2100
Houston, Texas 77002
Telephone: (713) 221-2000
Facsimile: (713) 221-2021

T. John Ward, Jr.
Texas Bar No. 00794818
E-mail: jw@wsfirm.com
Claire Abernathy Henry
Texas Bar No. 24053063
E-mail: Claire@wsfirm.com
WARD, SMITH & HILL, PLLC
1507 Bill Owens Pkwy.
Longview, Texas 75604
Telephone: (903) 757-6400
Facsimile: (903) 757-2323

S. Calvin Capshaw, III
Texas Bar No. 03783900
Capshaw DeRieux LLP
114 E. Commerce Avenue
Gladewater, TX 75647
Phone: (903) 845-5770
Email: ccapshaw@capshawlaw.com

ATTORNEYS FOR MONARCH NETWORKING SOLUTIONS LLC