IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

MONARCH NETWORKING SOLUTIONS LLC, Plaintiff, v. JUNIPER NETWORKS, INC.; Defendant.	Case No. 1:23-cv-670 **COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

COMPLAINT FOR PATENT INFRINGEMENT

1. Plaintiff, Monarch Networking Solutions LLC ("Monarch"), for its Complaint against Defendant Juniper Networks, Inc. ("Juniper"), 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

2. This is an action for patent infringement. Monarch alleges that Juniper infringes U.S. Patent Nos. 8,451,844 ("the '844 Patent"), 8,451,845 ("the '845 Patent"), 8,130,775 ("the '775 Patent"), and 8,693,369 ("the '369 Patent"), (collectively, the "Asserted Patents"), copies of which are attached hereto as Exhibits A-D.

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

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,'775 Patent, and '369 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 information and belief, Defendant Juniper is a corporation organized under the laws of Delaware with its principal place of business at 1133 Innovation Way, Sunnyvale, CA 94089. Juniper is registered to do business in the state of Virginia. Juniper has appointed C T Corporation System at 4701 Cox Road, Suite 285, Glen Allen, VA, 23060 as its agent for service of process.

7. On information and belief, Juniper maintains a regular and established place of business and does business in Virginia and in the Eastern District of Virginia, *inter alia*, at its facility at 2251 Corporate Park Dr, Herndon, VA 20171.

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

JURISDICTION

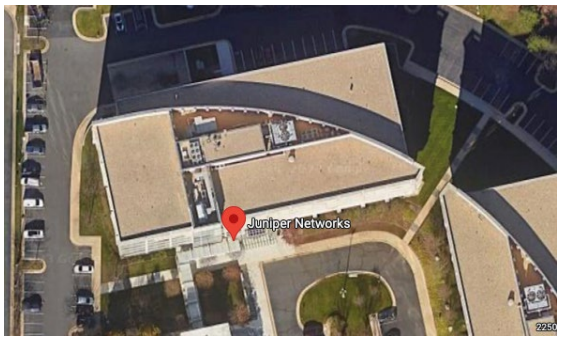
9. This is an action arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. Accordingly, this Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

10. This Court has personal jurisdiction over Juniper due, *inter alia*, to its continuous presence in, and systematic contact with, this judicial district and its registration in Virginia and domicile in this judicial district. Juniper 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

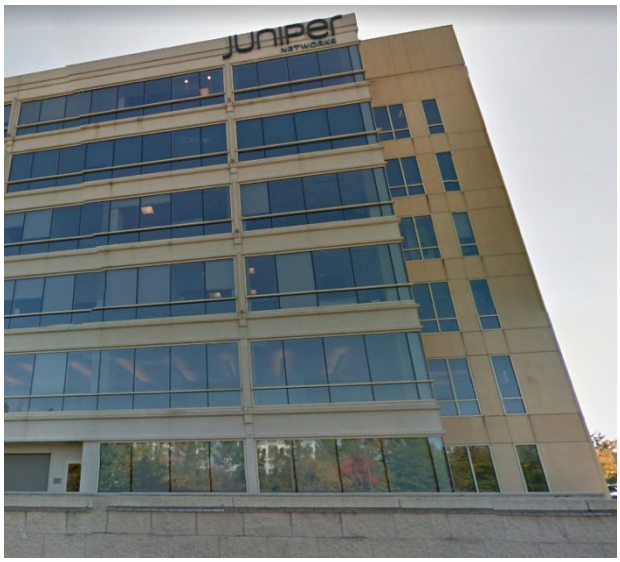
11. Venue is proper in this District pursuant to 28 U.S.C. §§1391(b), (c), (d), and 1400(b) because Juniper has a regular and established physical place of business in this District and has committed acts of patent infringement in the District, including at the Juniper Networks Offices located at 2251 Corporate Park Dr, Herndon, VA 20171.

FIGURE 1



Juniper Networks Offices at 2251 Corporate Park Dr., Herndon, VA 20171

FIGURES 2 & 3



Juniper Networks Offices at 2251 Corporate Park Dr., Herndon, VA 20171

12. The Juniper Network Office is a regular, physical, continuous, and established place of business of Juniper, which Juniper has established, ratified, and controlled; has listed on its website as a place of business of Juniper; has employed numerous Juniper employees to conduct Juniper's business in and from this District; and from which Juniper has infringed and willfully infringed the Asserted Patents in order to benefit Juniper in this District. Moreover, the regular and established place of business of Juniper, at which Juniper employees conduct Juniper business, is not limited to the Juniper Networks Offices at 2251 Corporate Park Dr, Herndon, VA 20171, but also include the place of business of customer on-site employees in this District who conduct Juniper business, as well as home office employees who conduct Juniper business in this District. Juniper commits acts of infringement in this District, including as explained further below by selling, making or using the infringing systems in and performing at least one step of the accused methods of the Asserted Patents at or from Juniper's regular and established place of business in this District.

13. Juniper has previously filed a complaint for patent infringement in this District and stated that "[v]enue is proper in the Eastern District of Virginia" for that case. *See Juniper Networks, Inc. v. Graphon Corp. et al.*, No. 1:09-cv-00287 (E.D. Va. Mar. 16, 2009).

FACTUAL ALLEGATIONS
Monarch Patents

14. The '844 Patent, '845 Patent,'775 Patent, and '369 Patent were all invented and developed by engineers at France Telecom in Paris. France Telecom was a leader and pioneer in the areas of networking specific to these patents.

15. 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 owns 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.

16. 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 industry that the limited supply of IPv4 public addresses was going to run out. In anticipation of this problem, IPv6 was developed which supported IPv6 addresses comprising 128 bits, considerably more than the IPv4 addresses comprising 32-bits that were then available. 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 remained slow.

17. The ’844 Patent discloses and claims improved systems, methods, and apparatuses to facilitate the migration and transformation from IPv4 networks to IPv6 networks. The inventions claimed by the ’844 Patent, described below, address many of the drawbacks regarding the stateful techniques that were previously available. *See, e.g.*, ’844 Patent at 2:11-55. 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 permitting 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.

18. 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.

19. 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 owns 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.

20. The ’845 Patent, like the ’844 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 systems, methods, and apparatuses 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.

21. The '845 Patent solution constitutes an improvement over prior solutions at least 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. With the '845 Patent 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 these state or translation tables improves the network's operation, providing a more efficient and elegant solution for interconnecting IPv4 domains with IPv6 domains. It also provides an efficient migration and transformation solution, allowing network operators to effectively address the problem of an exhausted IPv4 address space.

22. The '775 Patent, entitled "Method for Protecting a Pseudo-Wire," was duly and lawfully issued on March 6, 2012. Monarch owns 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 C.

23. 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, such as 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.

24. 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. If a fault occurs that affects 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. One disadvantage to this redundancy, however, is that the use of multiple pseudo-wires consumes

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. Such resource consumption increases the initial time required to set up the two pseudo-wires, and increases the restore time in the event of a fault affecting an output router, with a negative impact on quality of service.

25. The ’775 Patent discloses and claims improved systems and methods for setting up at least two pseudo-wires in a manner that mitigates or avoids 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. As one 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 novel configuration technique is noteworthy in that a link is shared by the two pseudo-wires between the intermediate router and the input router.

26. The ’775 Patent solution improves upon prior approaches because it alleviates and 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.

27. The '369 Patent, entitled "Method of Routing a Data Packet in a Network and an Associated Device," was duly and lawfully issued on April 8, 2014. Monarch is the owner of all right, title, and interest in the '369 Patent. The '369 Patent was filed on March 31, 2009 as Application No. 12/935,040 and is the U.S. national phase of the International Patent Application No. PCT/FR2009/050548, filed on March 31, 2009, which claims the benefit of French Application No. 08 52108, filed on March 31, 2008. A true and correct copy of the '369 Patent is attached hereto as Exhibit D.

28. The '369 Patent relates to "IP telecommunications networks in which packets of data are transported from source equipment to destination equipment identified by a destination address." '369 Patent at 1:15-18. 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.

29. The '369 Patent discloses and claims improved systems, methods, and apparatuses to facilitate the migration and transformation from IPv4 networks to IPv6 networks. In particular,

the "invention relates to a mechanism for allocating addresses and port numbers enabling the same primary address to be assigned to a plurality of pieces of terminal equipment of the telecommunications network." '369 Patent at 1:37-40. In this manner, the invention relates to any type of network addressing, including public and private IPv4 addressing schemes as well as IPv6 addressing schemes.

30. The '369 Patent improves on prior solutions to the IPv4 address exhaustion problem in a way that avoids degraded service to the client terminals being served. '369 Patent at 2:47-50. The '369 Patent solution describes a method for routing packets in an IP network that operates by using port masks to multiplex a single IP address across multiple terminals. In particular, a port mask is assigned to each destination equipment that defines a range of port numbers allocated for that destination equipment. Using this port mask, an identifier of the destination equipment associated with that port mask is selected and used for routing the packet to the destination equipment.

Juniper's Use of the Patented Technology

31. On information and belief, Juniper makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States networking equipment products including routers and switches that practice one or more claims of one of more of the Asserted Patents (the "Accused Products"). For example, Juniper makes, uses, and sells the Juniper MX Series Universal Routing Platform that supports Mapping of Address and Port capabilities for Border Relay (MAP-BR). The MAP-BR capabilities include software on the routers that implement the solutions claimed by the '844 Patent and '369 Patent. Similarly, Juniper makes, uses, and sells the Juniper NFX Series Network Services Platform that supports Mapping of Address and Port capabilities for Customer Edge (MAP-CE). The Juniper products with MAP-CE capabilities implement the solutions claimed by the '844 Patent, '845 Patent, and/or '369 Patent. These capabilities include

performing stateless address translation as described in Internet Engineering Task Force Request for Comments 7597. https://tools.ietf.org/html/rfc7597 ("IETF RFC 7597" or "RFC 7597"). Further, the Juniper NFX Series Network Services Platform are home gateways because they support connecting a private network of user terminals with a service provider network.

32. Additionally, Juniper makes, uses, and sells products installed with the Junos operating system ("Junos OS"), including the MX Series Universal Routing Platform (e.g., Virtual MX, MX5, MX10, MX40, MX80, MX104, MX150, MX204, MX240, MX480, MX960, MX2000, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016), NFX Series Network Services Platform (e.g., NFX150, NFX250, NFX350), and their corresponding line cards, interface modules, port concentrators, physical interface cards, and modular interface cards. These routers are made, used, and sold with software, including Junos OS, which together implement MAP-E (RFC 7597) capabilities, including those claimed by the '844 Patent, '845 Patent, and/or '369 Patent.

33. Juniper's Junos OS products, including the MX Series Universal Routing Platform, EX Series Ethernet Switches, ACX Series Universal Metro Routers, QFX Series Switches, T Series Core Routers, and TX Matrix Routers also support features called Virtual Private LAN Service ("VPLS") and Ethernet VPN ("EVPN"), which includes support for pseudo-wire configurations as claimed by the '775 Patent. The pseudo-wire configurations described by Juniper's documentation mirror those claimed by the '775 Patent.

34. The Accused Products include Juniper products using Junos OS, including the MX Series Universal Routing Platform (e.g., Virtual MX, MX5, MX10, MX40, MX80, MX104, MX150, MX204, MX240, MX480, MX960, MX2000, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016), NFX Series Network Services Platform (e.g., NFX150, NFX250,

NFX350), EX Series Ethernet Switches, ACX Series Universal Metro Routers, QFX Series Switches, T Series Core Routers, and TX Matrix Routers and other router/gateway products that support MAP-E, VPLS and/or EVPN as detailed below, and any corresponding line cards, interface modules, port concentrators, physical interface cards, modular interface cards, and Junos OS operating system for the accused routers and/or gateways.

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

35. Monarch incorporates by reference the allegations set forth in Paragraphs 1-34 of this Complaint as though fully set forth herein.

36. Juniper 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 Accused Products. The Accused Products infringe at least claims 1, 4, and 5 of the '844 Patent.

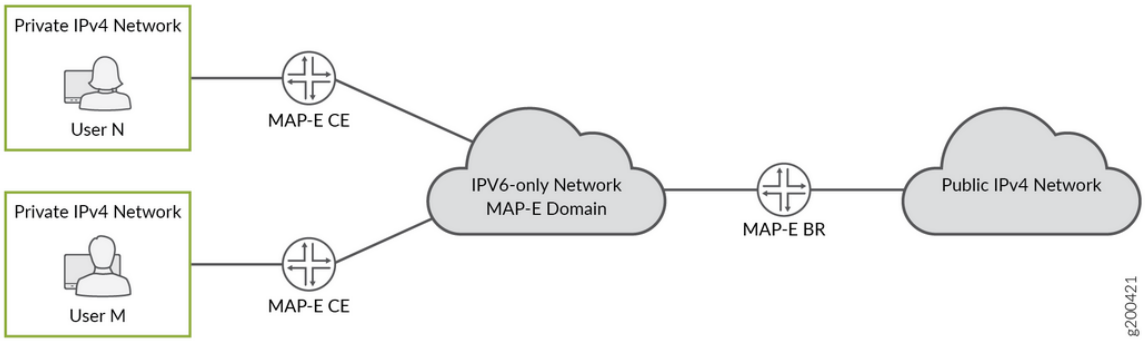
37. The Accused Products support and implement a method of receiving a data packet from an IPv4 domain in an IPv6 domain, said data packet comprising an IPv4 destination address and a destination port number. The Accused Products are configured to use the incoming IPv4 data packet to generate an IPv6 data packet that includes a newly constructed IPv6 destination address formed from an operator prefix, the IPv4 destination address and destination port information. The 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 Accused Products are configured to support Mapping of Address and Port using encapsulation techniques, conventionally known as MAP-E.

38. As one example, the Accused Products include the MX and NFX Series routers that run Junos OS:

> This topic provides an overview of Mapping of Address and Port with Encapsulation (MAP-E) feature and its benefit to service providers when used as an inline service on MX Series routers with MPC and MIC interfaces. Starting in Junos OS release 20.2R1, MAP-E softwires are supported under Next Gen Services on either an MPC or MIC by specifying the inline services `si-1/1/0` naming convention.

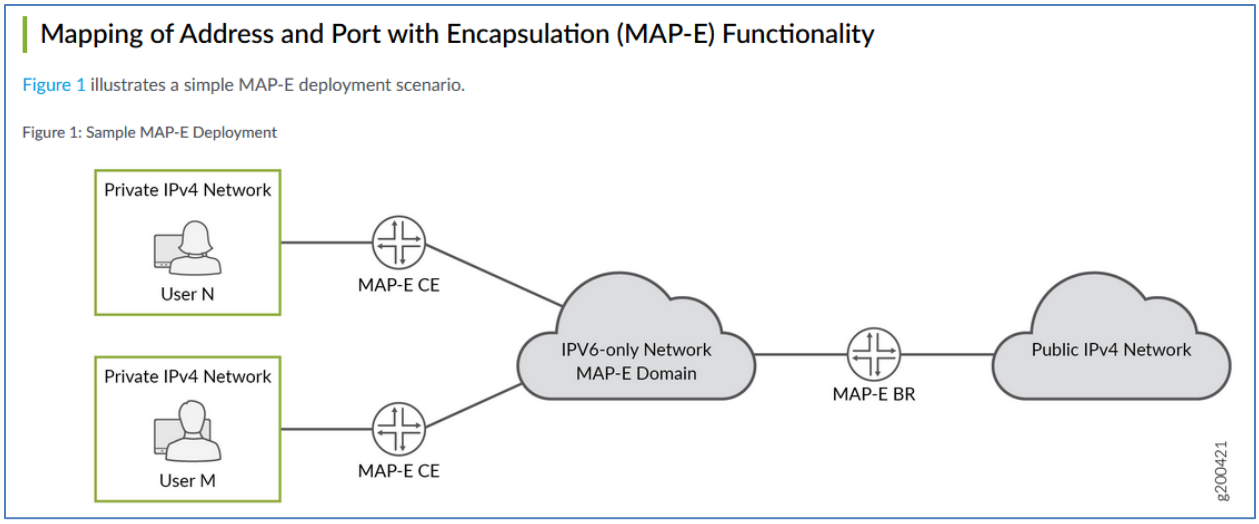
https://www.juniper.net/documentation/en_US/junos20.2/topics/concept/map-e-overview.html.

Juniper included support for Mapping of Address and Port using encapsulation (MAP-E) in Junos OS Release 18.2R1, which was released in approximately June 2018. *See* https://www.juniper.net/documentation/us/en/software/junos/interfaces-adaptive-services/topics/ref/statement/map-e-edit-services-softwire-softwire-concentrator.html; Junos OS 18.2R1 Release Notes at 272. 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 Juniper in the Accused Products.

> **Mapping of Address and Port with Encapsulation (MAP-E) Functionality**
>
> Figure 1 illustrates a simple MAP-E deployment scenario.
>
> Figure 1: Sample MAP-E Deployment
>
> 
>

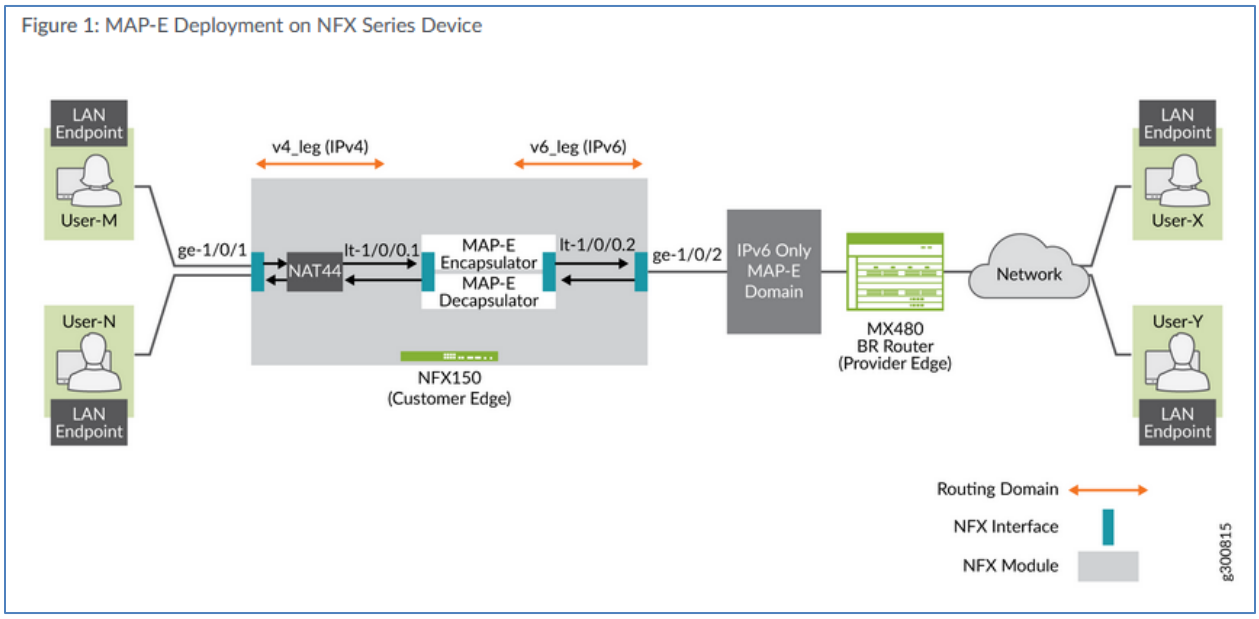
https://www.juniper.net/documentation/en_US/junos20.2/topics/concept/map-e-overview.html.

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



https://www.juniper.net/documentation/en_US/junos20.2/topics/concept/map-e-overview.html

40. An exemplary MAP-E domain is illustrated in the figure below from the Juniper documentation, showing an accused NFX150 operating as a MAP-E Customer Edge on one edge of the domain and an accused MX480 operating as a MAP-E Border Rely on the other edge of the domain.



https://www.juniper.net/documentation/us/en/software/junos/nfx150-getting-started/topics/topic-map/nfx-series-map-e-configuring.html.

41. This same network topology is generally depicted and described in the MAP-E descriptions in RFCs 7597.

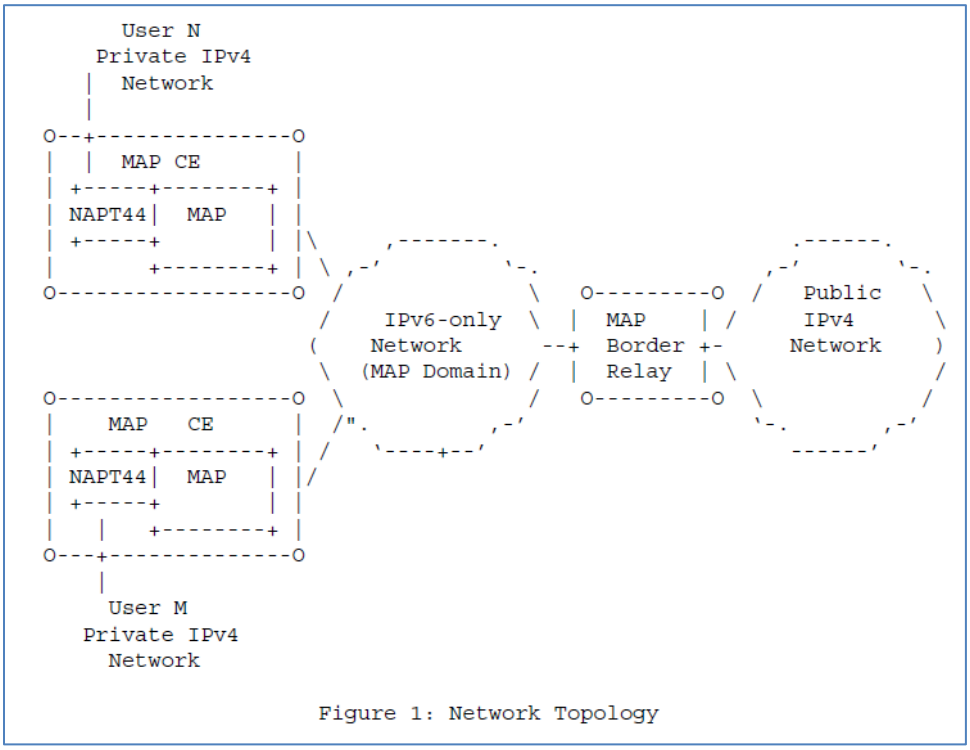


Figure 1: Network Topology

IETF RFC 7597 at 8. Accordingly, the 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.

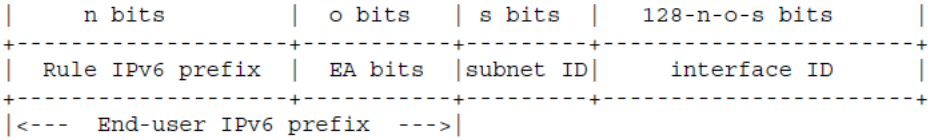
42. IPv4 packets (or Internet Protocol v4 packets), by definition, include IPv4 source and destination addresses. These addresses can be interpreted as network addresses or host addresses (or both). Additionally, certain IP packets encapsulate higher layer protocols, such as TCP and UDP, which rely on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

43. 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.

44. When a packet is received by an Accused Product with a destination IPv4 address that matches the IPv4 address prefix of a mapping rule, the Accused Product constructs 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 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.
>
> 
>
>
> 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.

45. The Accused Products use the EA bits identified in the RFC 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. As described in 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 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:

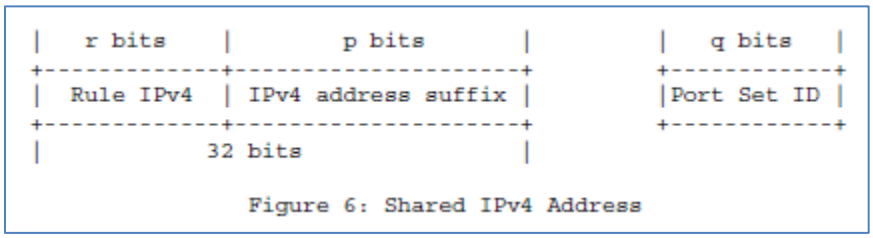
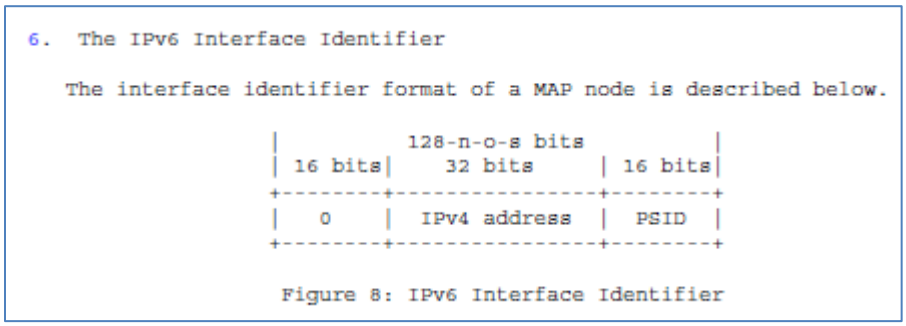


Figure 6: Shared IPv4 Address

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 Accused Products.

46. Additionally, in the 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 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

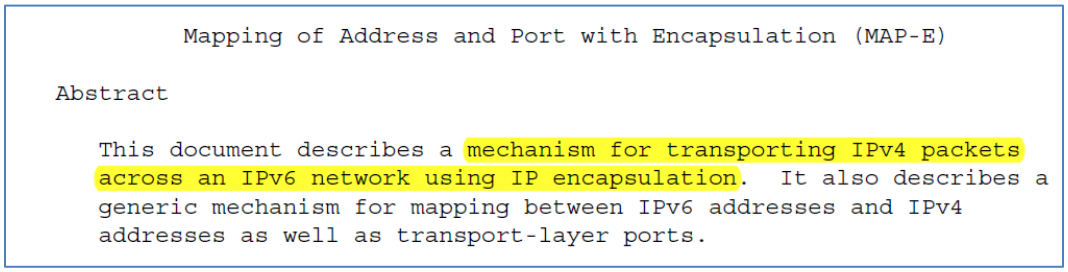
The interface identifier format of a MAP node is described below.

```
|          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.

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

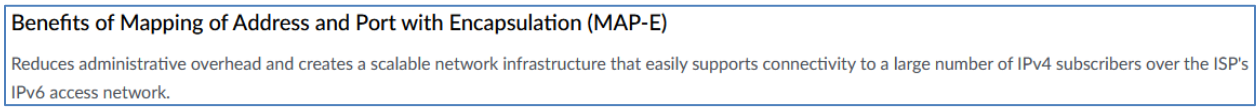


Mapping of Address and Port with Encapsulation (MAP-E)

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. Juniper promotes MAP-E to its customers as being advantageous relative to other routing techniques.



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

Reduces administrative overhead and creates a scalable network infrastructure that easily supports connectivity to a large number of IPv4 subscribers over the ISP's IPv6 access network.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html.

Thus, for MAP-E support in the 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.

48. 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 Accused Products, Juniper has injured Monarch and is liable to Monarch for directly infringing one or more claims of the ’844 Patent, including without limitation claims 1, 2, and 5 pursuant to 35 U.S.C. § 271(a).

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

50. Juniper 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 Accused Products, with knowledge and specific intention that such products will be used by its customers to support MAP-E functionality. For example, Juniper specifically instructs its customers on how to use and implement the technology claimed in the ’844 patent. *See, e.g.*, Configuring Mapping of Address and Port with Encapsulation (MAP-E) *available at* https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html.

51. On information and belief, Juniper was 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. For example, Juniper was aware of the ’844 Patent at least as of September 17, 2019 when the application leading to the ’844 Patent was cited during the examination of U.S. Patent No. 10,887,231 assigned to Juniper. By further example, Juniper was aware of the ’844 Patent at least as of March 20, 2013, when the France Telecom disclosed the application publication leading to the ’844 patent to the IETF, in which Juniper participates, through and Intellectual Property Right disclosure (“IPR disclosures”). *See* https://datatracker.ietf.org/ipr/2049/.

52. Additionally, Juniper is a member of RPX Corporation, which includes as part of its membership the distribution of patent litigation alerts via RPX Insight, which provides news and analysis to RPX members such as US Litigation and Alerts, Monthly NPE Reports, Entity Dossiers, PTAB analytics, District Court Analytics, and other Advanced Alerts. Multiple news alerts, analyses, dossiers, and/or other information about the '844 Patent have been distributed to RPX members, including on information and belief Juniper, since at least early 2020, when Monarch filed suit against Juniper's competitor (on January 21, 2020), Cisco Systems, Inc., for infringing the '844 Patent. The infringement allegations in that case mirror those here.

53. At a minimum, Juniper was aware of the '844 Patent at least as of the filing of this complaint, and their continued support for the Accused Products constitutes indirect infringement of the '844 Patent.

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

55. As a result of Juniper's infringement of the '844 Patent, Monarch has suffered monetary damages and seeks recovery in an amount adequate to compensate for Juniper'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)

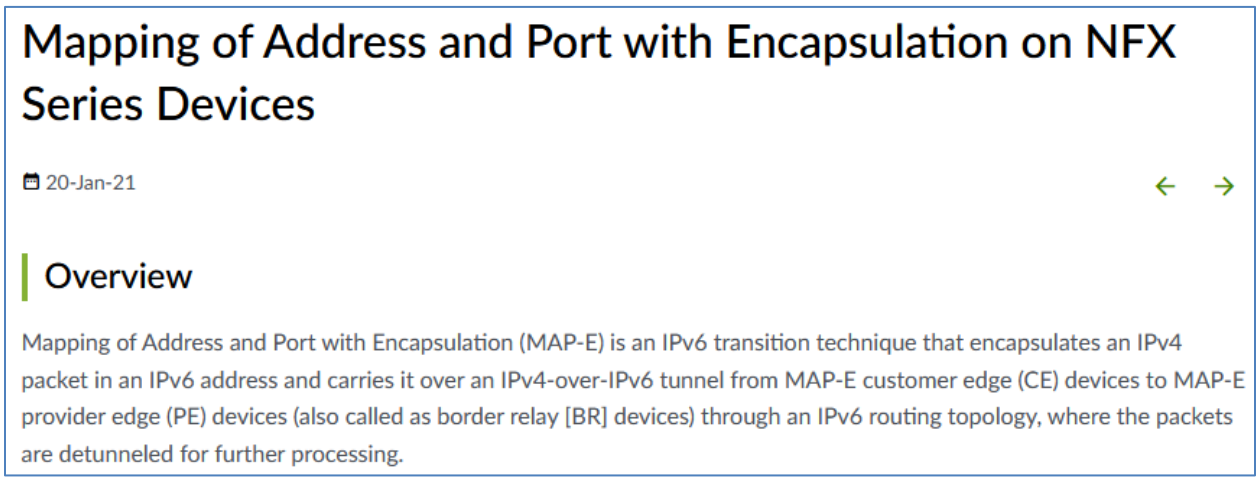
56. Monarch incorporates by reference the allegations set forth in Paragraphs 1-55 of this Complaint as though fully set forth herein.

57. Juniper 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 Accused Products that implement Mapping of Address and Port capabilities for Customer

Equipment, such as Juniper NFX series routers. The Accused Products infringe at least claims 1, 7, and 8 of the '845 Patent.

58. The 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. The Accused Products identify an IPv6 destination address constructed by concatenating an IPv6 prefix, an IPv4 destination address, and a destination port number. If necessary, the Accused Products regularize at least one of the IPv6 source or destination addresses of a data packet by replacing one of the IPv6 addresses. The Accused Products perform such address replacement using either a native address or a constructed address. After performing any necessary replacements, the Accused Products modify the data packet with the replacement addresses (as needed) and then route the packet to its destination.

59. The Accused Products support MAP-E CE functionality, as defined in IETF RFC 7597.

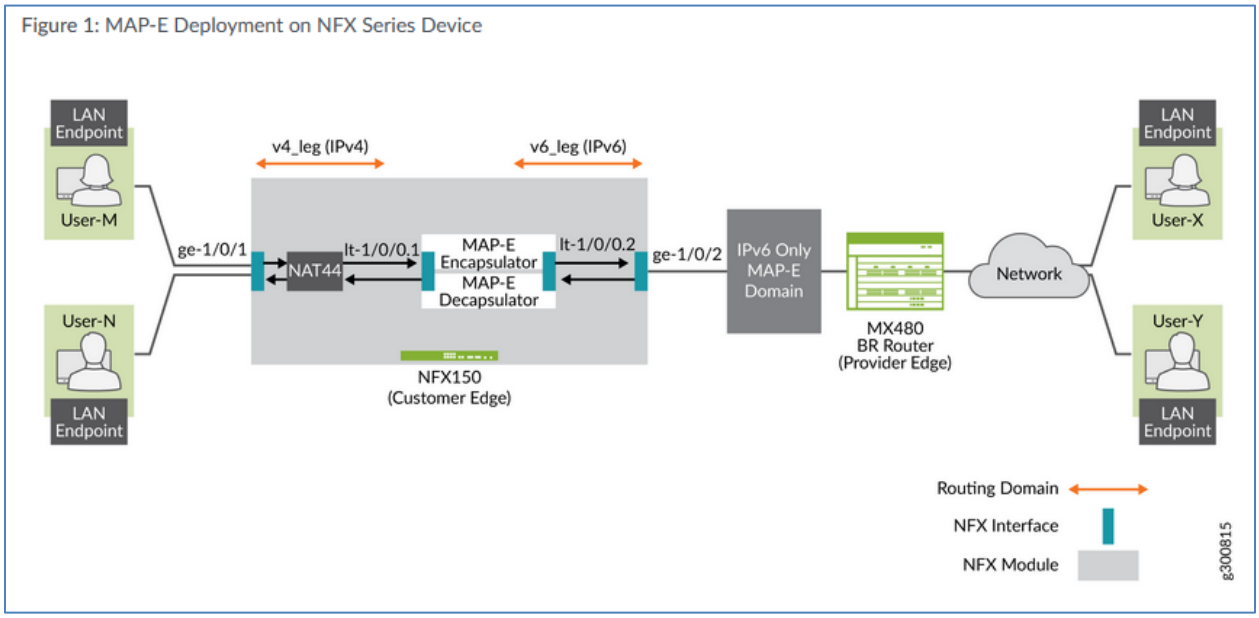


https://www.juniper.net/documentation/us/en/software/junos/nfx150-getting-started/topics/topic-map/nfx-map-e-overview.html.

60. As such, the Accused Products are designed with the capability to connect to an IPv6 domain (the MAP-E domain) and also connect to an IPv4 domain.

61. An exemplary MAP-E domain is illustrated in the figure below from Juniper documentation, showing an accused NFX150 operating as a MAP-E Customer Edge on one edge of the domain and an accused MX480 operating as a MAP-E Border Rely on the other edge of the domain.

Figure 1: MAP-E Deployment on NFX Series Device



https://www.juniper.net/documentation/us/en/software/junos/nfx150-getting-started/topics/topic-map/nfx-series-map-e-configuring.html. Juniper specifically instructs its customers how to implement an infringing system, and it designs and configures the Accused Products with the capability to support those infringing implementations.

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

63. Accordingly, the IPv6 packets that are received by the Accused Product comprise 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.").

64. The IPv6 destination address of packets received by the Accused Products for delivery to an IPv4 domain are constructed by concatenating an IPv6 Prefix, an IPv4 destination address, and a destination port number, per the Basic Mapping Rule and IETF RFC 7597. To facilitate traffic across MAP domains, the Juniper 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.

65. The format of IPv6 packets received by the 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.

66. The Accused Products use the EA bits identified in the RFC 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 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:

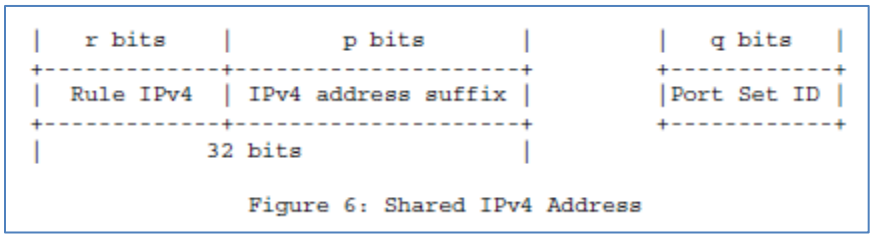


Figure 6: Shared IPv4 Address

IETF RFC 7597 at 13. The combined Rule IPv4 network address and IPv4 address suffix form the IPv4 destination address in the 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.

67. 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 node is described below.

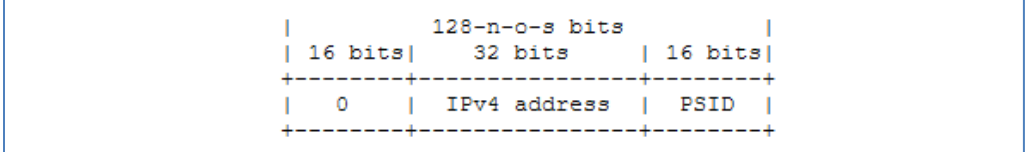


Figure 8: IPv6 Interface Identifier

In the case of an IPv4 prefix, the IPv4 address field is right-padded with zeros up to 32 bits. The PSID field is left-padded with zeros to create a 16-bit field. For an IPv4 prefix or a complete IPv4 address, the PSID field is zero.

If the End-user IPv6 prefix length is larger than 64, the most significant parts of the interface identifier are overwritten by the prefix.

IETF RFC 7597 at 14.

68. On receiving an IPv6 packet constructed in the manner described above, the Accused Products translate the IPv6 destination address to the IPv4 destination address embedded in the IPv6 destination address, per the Basic Mapping Rule. Once the constructed IPv6 address is replaced with the native IPv4 address and port, the packet can be delivered to the destination.

69. 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-E RFC 7597 illustrates the Private IPv4 network through which received packets are routed.

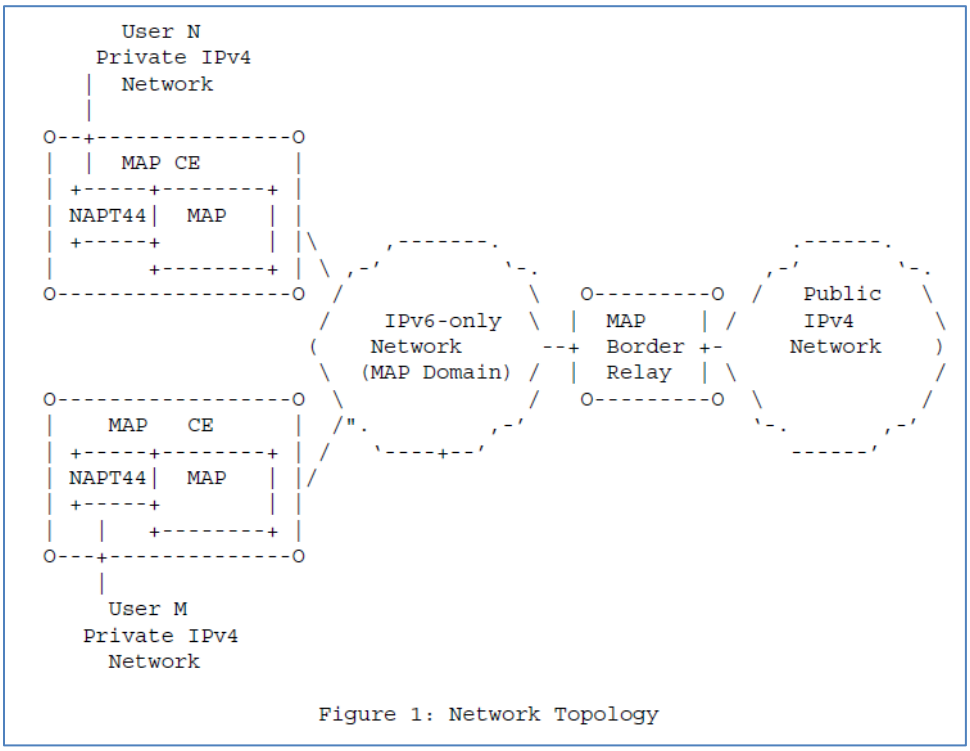


Figure 1: Network Topology

IETF RFC 7597 at 7.

70. 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 Accused Products, Juniper has injured Monarch and is liable to Monarch for directly infringing one or more claims of the ’845 Patent, including without limitation claims 1, 7, and 8 pursuant to 35 U.S.C. § 271(a).

71. Juniper also indirectly infringes the ’845 Patent under 35 U.S.C. § 271(b).

72. Juniper 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 Accused Products, with knowledge and specific intention that such products will be used by its customers. For example, Juniper specifically instructs its customers how to use and implement the technology claimed in the ’845 Patent and it designs and programs the Accused Products with that specific functionality.

See, e.g., Configuring MAP-E on NFX Series Devices *available at* https://www.juniper.net/documentation/us/en/software/junos/nfx150-getting-started/topics/topic-map/nfx-series-map-e-configuring.html.

73. Additionally, Juniper is a member of RPX Corporation, which includes as part of its membership the distribution of patent litigation alerts via RPX Insight, which provides news and analysis to RPX members such as US Litigation and Alerts, Monthly NPE Reports, Entity Dossiers, PTAB analytics, District Court Analytics, and other Advanced Alerts. Multiple news alerts, analyses, dossiers, and/or other information about the '845 Patent have been distributed to RPX members, including on information and belief Juniper, since at least early 2020, when Monarch filed suit against Juniper's competitor (on January 21, 2020), Cisco Systems, Inc., for infringing the '845 Patent. The infringement allegations in that case mirror those here.

74. At a minimum, Juniper was aware of the '845 Patent and related Monarch patents, had knowledge of the infringing nature of their activities, and nevertheless continue their infringing activities. Juniper was aware of the '845 Patent at least as of the filing of this complaint.

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

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

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

77. Monarch incorporates by reference the allegations set forth in Paragraphs 1-76 of this Complaint as though fully set forth herein.

78. Juniper 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 Accused Products that use VPLS and/or EVPN such as the MX, NFX, ACX, QFX, T and TX Series routers, EX and QFX Series switches, and any other products with similarly functionality, including those using Juniper's Junos OS.

79. For example, the Accused Products infringe at least claims 1 and 6 of the '775 Patent in at least the manner described below.

80. The Juniper routers include and execute computer code in the form of Juniper Junos OS software that is stored on a non-transitory computer-readable medium associated with the Accused Products.

> **VPLS on PE Routers**
>
> Within a VPLS configuration, a device running Junos OS can act as a PE router. Junos OS passes the VPLS traffic through the following ports and PIMs on the Juniper Networks device to CE routers in the VPLS network:
>
> - Built-in Ethernet ports on front panel
> - Gigabit Ethernet uPIMs
> - Gigabit Ethernet ePIMs
> - Fast Ethernet PIMs
> - Fast Ethernet ePIMs

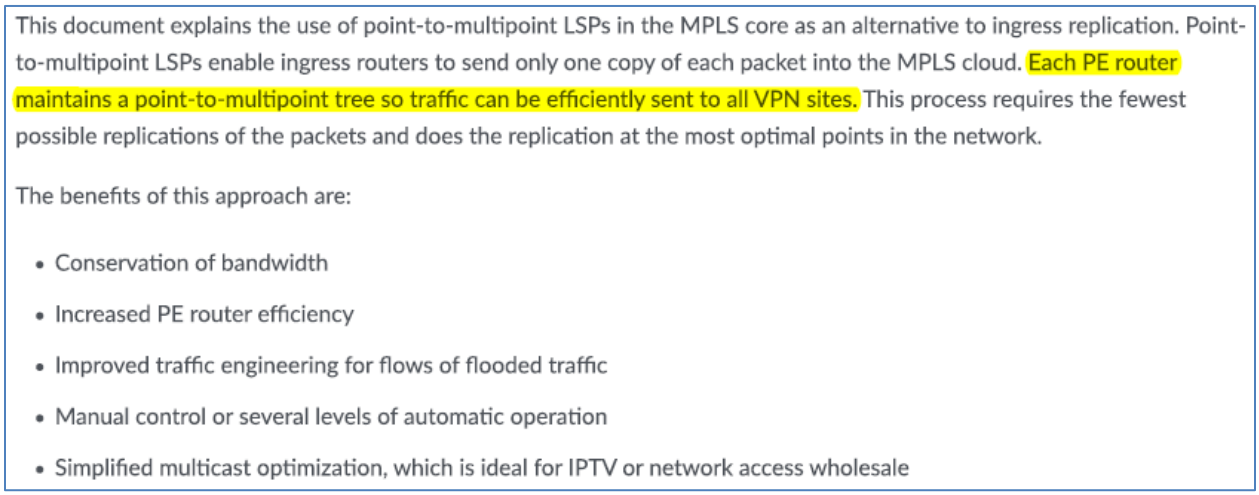
https://www.juniper.net/documentation/en_US/junos/topics/concept/vpls-security-overview.html.

81. The computer code comprises instructions for implementing a method of setting up least two pseudo-wires able to broadcast a data stream. The Junos OS implements point-to-multipoint (P2MP) label-switched paths (LSP) for delivering broadcast, multicast, and certain unicast streams to a VPLS domain using pseudo-wires.

> Juniper Networks has several important VPLS enhancements that provide a solution for the replication overhead issue:
>
> - Point-to-multipoint LSP support provides efficient distribution of multicast traffic such as IP-based television (IPTV).
> - Multihoming support integrates the path selection capability of BGP with VPLS to allow a customer edge (CE) Ethernet switch to have a backup path across the network.

Next-Generation VPLS Point-to-Multipoint Forwarding Overview *available at* https://www.juniper.net/documentation/us/en/software/junos/vpn-l2/topics/concept/ng-vpls-p2mp-lsp-forwarding-overview.html.

82. The Juniper VPLS solution involves automatically maintaining a point to multipoint tree so that network traffic can be efficiently sent to all VPN sites.



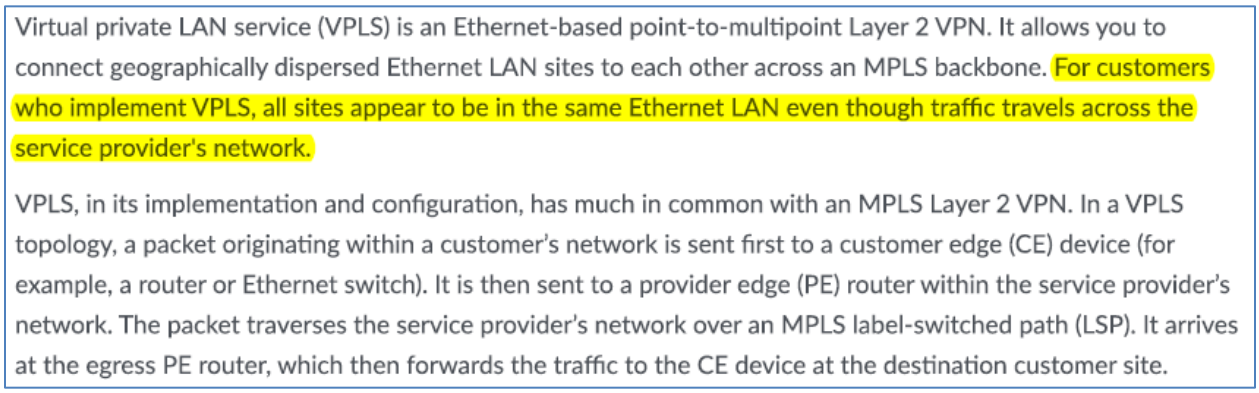
This document explains the use of point-to-multipoint LSPs in the MPLS core as an alternative to ingress replication. Point-to-multipoint LSPs enable ingress routers to send only one copy of each packet into the MPLS cloud. Each PE router maintains a point-to-multipoint tree so traffic can be efficiently sent to all VPN sites. This process requires the fewest possible replications of the packets and does the replication at the most optimal points in the network.

The benefits of this approach are:

- Conservation of bandwidth
- Increased PE router efficiency
- Improved traffic engineering for flows of flooded traffic
- Manual control or several levels of automatic operation
- Simplified multicast optimization, which is ideal for IPTV or network access wholesale

Id.

83. Juniper explains that VPLS has much in common with an MPLS Layer 2 VPN technology allowing connection between two or more locations in a single LAN-like bridge domain over the MPLS transport infrastructure.



Virtual private LAN service (VPLS) is an Ethernet-based point-to-multipoint Layer 2 VPN. It allows you to connect geographically dispersed Ethernet LAN sites to each other across an MPLS backbone. For customers who implement VPLS, all sites appear to be in the same Ethernet LAN even though traffic travels across the service provider's network.

VPLS, in its implementation and configuration, has much in common with an MPLS Layer 2 VPN. In a VPLS topology, a packet originating within a customer's network is sent first to a customer edge (CE) device (for example, a router or Ethernet switch). It is then sent to a provider edge (PE) router within the service provider's network. The packet traverses the service provider's network over an MPLS label-switched path (LSP). It arrives at the egress PE router, which then forwards the traffic to the CE device at the destination customer site.

VPLS Overview *available at* https://www.juniper.net/documentation/en_US/junos/topics/concept/vpls-security-overview.html.

84. Juniper describes VPLS as advantageous for requiring the fewest possible replications of packets as well as performing the replication at the most optimal points in the network, thus providing several benefits for customers.

> This document explains the use of point-to-multipoint LSPs in the MPLS core as an alternative to ingress replication. Point-to-multipoint LSPs enable ingress routers to send only one copy of each packet into the MPLS cloud. Each PE router maintains a point-to-multipoint tree so traffic can be efficiently sent to all VPN sites. This process requires the fewest possible replications of the packets and does the replication at the most optimal points in the network.
>
> The benefits of this approach are:
>
> - Conservation of bandwidth
> - Increased PE router efficiency
> - Improved traffic engineering for flows of flooded traffic
> - Manual control or several levels of automatic operation
> - Simplified multicast optimization, which is ideal for IPTV or network access wholesale

Next-Generation VPLS Point-to-Multipoint Forwarding Overview *available at* https://www.juniper.net/documentation/us/en/software/junos/vpn-l2/topics/concept/ng-vpls-p2mp-lsp-forwarding-overview.html.

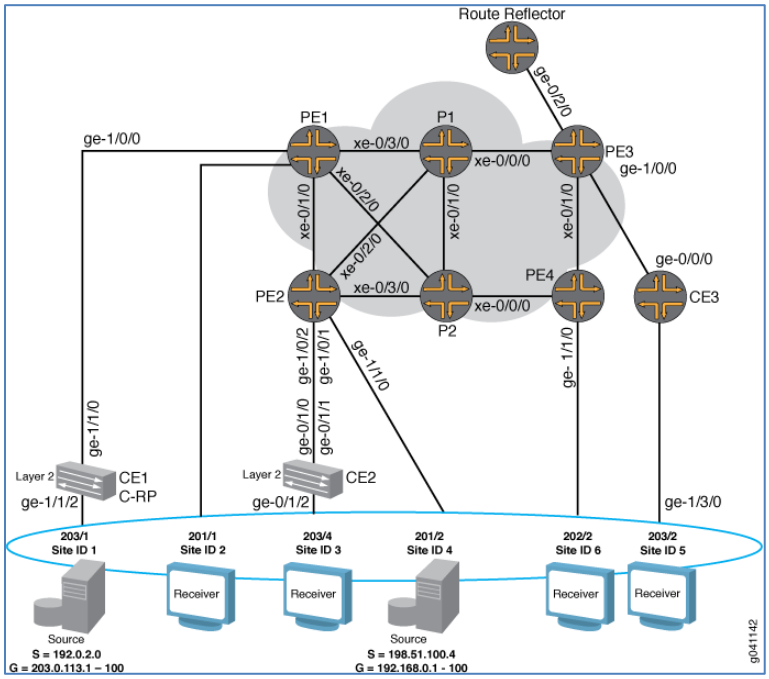
85. Juniper's VPLS solution includes setting up at least two pseudo-wires able to broadcast a data stream. For example, Juniper's VPLS solution is able to broadcast a data stream, for example, by emulating the broadcast domain of a LAN across and MPLS network cloud:

> VPLS emulates the broadcast domain of a LAN across an MPLS network cloud. Traditional MPLS implementations of VPLS require that all participating ingress provider edge (PE) routers make separate copies of each broadcast or multicast packet to send to all other PE routers that are part of the VPLS site for the same extended LAN. In a large virtual private network (VPN), replication overhead can be significant for each ingress router and its attached core-facing links.

Id.

86. Juniper's VPLS solution implements the method by setting up a first pseudo-wire comprising a first link set up between an input router of a packet-switched network and an intermediate router of the packet-switched network and a second link set up between said intermediate router and a first output router of the packet-switched network. In an exemplary

topology created by Juniper, a first link is setup between input router PE1 and router P2, both of which are MX series routers:



Note the following topology details:

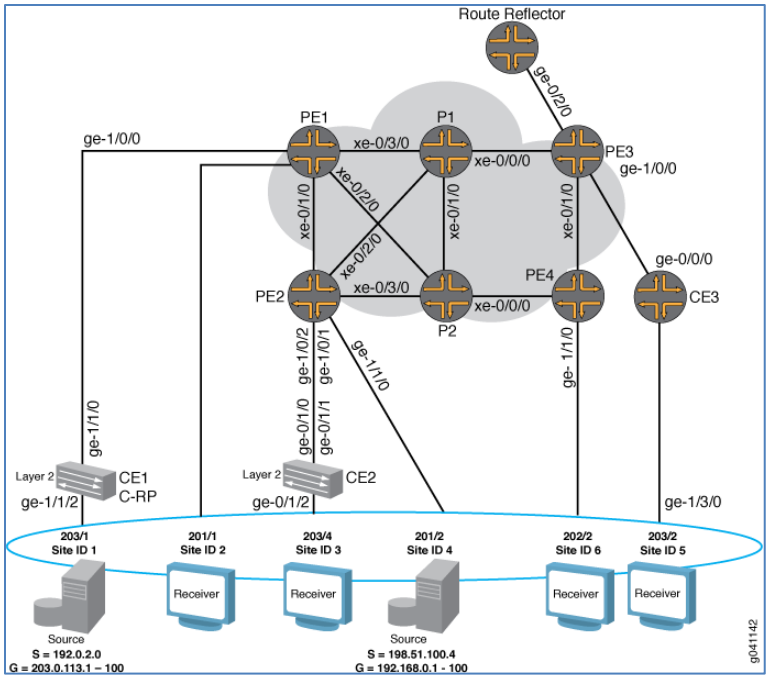
- A route reflector is configured in the topology to reflect the family `l2-vpn` routes to all the PE routers for BPG-VPLS.

Example: NG-VPLS Using Point-to-Multipoint LSPs *available at* https://www.juniper.net/documentation/us/en/software/junos/vpn-l2/topics/example/ng-vpls-p2mp-lsp-forwarding-configuration.html#overview-and-topology1114__physical-topology. A second link is set up between router P2 and output router PE2. This process is described by Juniper:

> For each VPLS instance, a PE router with dynamic point-to-multipoint LSPs enabled creates a dedicated point-to-multipoint LSP based on the point-to-multipoint template. Whenever VPLS discovers a new neighbor through BGP, a sub-LSP for this neighbor is added to the point-to-multipoint LSP.
>
> If there are *n* PE routers in the VPLS instance then the router creates *n* point-to-multipoint LSPs in the network where each PE router is the root of the tree and includes the rest of the *n-1* PE routers as leaf nodes connected through a source-to-leaf sub-LSP.
>
> 1. In this step, you configure Router PE1 and Router PE2 to use a dynamic point-to-multipoint LSP template for LSP creation. When these routers receive a new BGP route advertised from the route reflector for a new neighbor, they create a point-to-multipoint sub-LSP to that neighbor. To create the dynamic point-to-multipoint LSP template, include the `label-switched-path` statement, give the LSP template a meaningful name, include the `template` statement and include the `p2mp` statement. Also enable link protection and configure the optimize timer to periodically reoptimize the LSP path.

Id.

87. Juniper's VPLS solution sets up a second pseudo-wire between said input router and a second output router of the packet-switched network, wherein the second pseudo-wire comprises said first link and a third link set up between said intermediate router and said second output router, said first link being shared by the first and second pseudo-wires. In the example above, a pseudo-wire is set up whenever Juniper's VPLS discovers a new Layer 2 VPN neighbor. In that example, Juniper's VPLS sets up a new pseudo-wire between input router PE1 and second output router PE4. The exemplary pseudo-wire comprises the first link between PE1 and P2, which is shared with the first pseudo-wire as explained above, and a third link between P2 and PE4:



Id.

88. Similarly, Juniper's EVPN solution implements a method of setting up at least two pseudo-wires able to broadcast a data stream. For example, an EVPN connects dispersed customer sites using a Layer 2 virtual bridge. The EVPN builds a topology of point-to-point connections that connect end customer sites in a VPN and supports a broadcast domain:

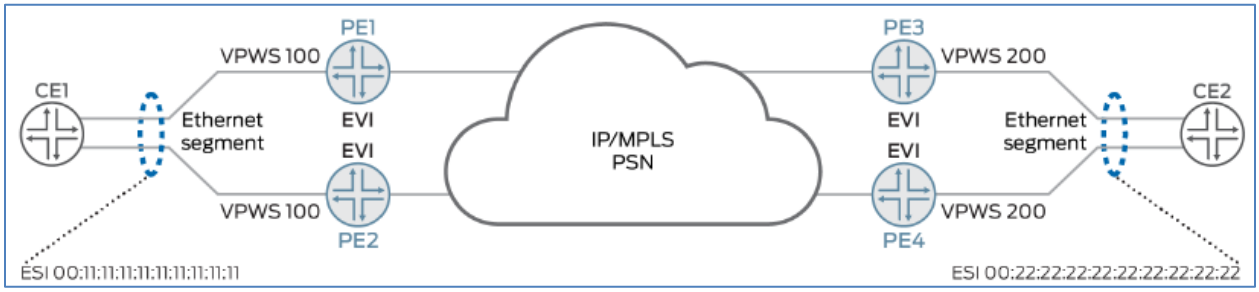
> An Ethernet VPN (EVPN) enables you to connect dispersed customer sites using a Layer 2 virtual bridge. As compared with other types of Layer 2 VPNs, an EVPN consists of customer edge (CE) devices (host, router, or switch) connected to provider edge (PE) routers. The PE routers can include an MPLS edge switch (MES) that acts at the edge of the MPLS infrastructure. Either an MX Series 5G Universal Routing Platform or a standalone switch can be configured to act as an MES. You can deploy multiple EVPNs within a service provider network, each providing network connectivity to a customer while ensuring that the traffic sharing on that network remains private.
>
> Virtual private wire service (VPWS) Layer 2 VPNs employ Layer 2 services over MPLS to build a topology of point-to-point connections that connect end customer sites in a VPN. The service provisioned with these Layer 2 VPNs is known as VPWS. You can configure a VPWS instance on each associated edge device for each VPWS Layer 2 VPN.

> An EVPN instance (EVI) is an EVPN routing and forwarding instance spanning across all the PE routers participating in that VPN. An EVI is configured on the PE routers on a per-customer basis. Each EVI has a unique route distinguisher and one or more route targets. An EVI is configured on PE1, PE2, PE3, and PE4. An Ethernet tag identifies a particular broadcast domain, such as a VLAN. An EVI consists of one or more broadcast domains. Ethernet tags are assigned to the broadcast domains of a given EVI by the provider of that EVPN. Each PE router in that EVI performs a mapping between broadcast domain identifiers understood by each of its attached CE devices and the corresponding Ethernet tag. Depending on the multihoming mode of redundancy, only one path or all paths can be active at any one time.

Overview of VPWS with EVPN Signaling Mechanisms *available at* https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/concept/evpn-vpws-signaling-mechanisms-overview.html.

89. Juniper's EVPN solution implements the method by setting up a first pseudo-wire comprising a first link set up between an input router of a packet-switched network and an intermediate router of the packet-switched network and a second link set up between said intermediate router and a first output router of the packet-switched network. In an example created by Juniper, a first link is setup between input router PE1 and an intermediate router in the cloud P:

> Figure 1 illustrates an EVPN-VPWS network. Device CE1 is multihomed to Routers PE1 and PE2 and Device CE2 is multihomed to Routers PE3 and PE4. Device CE2 has two potential paths to reach CE1, and depending on the multihoming mode of redundancy, only one path or all paths can be active at any one time. When a CE device is multihomed to two or more PE routers, the set of Ethernet links constitutes an Ethernet segment. An Ethernet segment appears as a link aggregation group (LAG) to the CE device. The links from PE1 and PE2 to CE1 and PE3 and PE4 to CE2 form an Ethernet segment.



Id. A second link is set up between P and output router PE3.

90. Juniper describes the advantages of the EVPN solution as supporting autonomous VPN capabilities:

> An EVPN-VPWS network provides a framework for delivering VPWS with EVPN signaling mechanisms. The advantages of VPWS with EVPN mechanisms are single-active or all-active multihoming capabilities and support for Inter-autonomous system (AS) options associated with BGP-signaled VPNs. Metro Ethernet Forum (MEF) describes the following two service models for VPWS:

Id.

91. Juniper's EVPN solution sets up a second pseudo-wire between said input router and a second output router of the packet-switched network, wherein the second pseudo-wire comprises said first link and a third link set up between said intermediate router and said second output router, said first link being shared by the first and second pseudo-wires. In the example above, a pseudo-wire is set between input router PE1 and second output router PE4. The exemplary pseudo-wire comprises the first link between PE1 and P, which is shared with the first pseudo-wire as explained above, and a third link between P and PE4. These connections are set up automatically when using Juniper's multihoming mode:

> The multihoming mode of operation along with VPWS service identifiers determine which PE router or routers forward and receive traffic in the EVPN-VPWS network. The VPWS service identifier identifies the endpoints of the EVPN-VPWS network. These endpoints are autodiscovered by BGP and are used to exchange the service labels(learned from the respective PE routers) that are used by autodiscovered routes per EVI route type. The service identifier is of two types:

Id.

92. 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 Accused Products, Juniper has injured Monarch and is liable to Monarch for directly infringing one or more claims of the '775 Patent, including without limitation claims 1 and 6 pursuant to 35 U.S.C. § 271(a).

93. Juniper also indirectly infringes the '775 Patent under 35 U.S.C. § 271(b).

94. Juniper 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 Accused Products, with knowledge and specific intention that such products will be used by its customers. For example, Juniper instructs its customers on how to use and implement the technology claimed in the '775 Patent. *See, e.g.*, Example: NG-VPLS Using Point-to-Multipoint LSPs (providing step-by-step instructions for configuring a PE router).

95. Additionally, Juniper is a member of RPX Corporation, which includes as part of its membership the distribution of patent litigation alerts via RPX Insight, which provides news and analysis to RPX members such as US Litigation and Alerts, Monthly NPE Reports, Entity Dossiers, PTAB analytics, District Court Analytics, and other Advanced Alerts. Multiple news alerts, analyses, dossiers, and/or other information about the '775 Patent have been distributed to RPX members, including on information and belief Juniper, since at least early 2020, when Monarch filed suit against Juniper's competitor (on January 21, 2020), Cisco Systems, Inc., for infringing the '775 Patent.

96. At a minimum, Juniper 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, Juniper was aware of the infringement allegations regarding the '775 patent contained herein.

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

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

FOURTH COUNT
(Infringement of U.S. Patent No. 8,693,369)

99. Monarch incorporates by reference the allegations set forth in Paragraphs 1-98 of this Complaint as though fully set forth herein.

100. Juniper makes, uses, sells, and/or offers to sell in the United States, and/or imports into the United States products that directly infringe the '369 Patent, including the above identified the Accused Products. The Accused Products infringe at least claim 1 of the '369 Patent.

101. The Accused Products support and implement a method of routing an IP data packet, which includes a destination address and a destination port number, in a telecommunications network to a destination equipment. The Accused Products are configured to determine a port mask assigned to a destination equipment, the port mask defining a range of port numbers for the destination equipment. The Accused Products are designed to select an identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask. The Accused Products are designed to then route the packet to the destination equipment based on the selected identifier. Specifically, the Accused Products are configured to support Mapping of Address and Port using encapsulation techniques, conventionally known as MAP-E.

102. The Accused Products include Juniper devices configured to support MAP-E and/or MAP-T, including those that run the Junos OS release 18.2R1 or later, such as MX Series routers with MPC and MIC interfaces (*e.g.*, MX240, MX480, MX960).

103. The Accused Products run the Junos OS. The "map-e" command has been supported since Junos OS Release 18.2R1.

Release Information

Statement introduced in Junos OS Release 18.2R1.

Support added in Junos OS release 20.2R1 at MAP-E for Next Gen Services on MX240, MX480, and MX960 routers.

Support added in Junos OS release 20.4R1 at MAP-E CE confidentiality on NFX150, NFX250, NFX350,and SRX1500 devices.

Junos OS: Adaptive Services Interfaces User Guide for Routing Devices (published 2022-09-12) [hereinafter "Adaptive Services Guide"] at 1433 (describing release information for the Junos OS map-e command); *see also* Next Gen Services Interfaces User Guide for Routing Devices (published 2022-09-11) at 706 [hereinafter "Next Gen Guide"].

104. Since at least Junos OS Release 20.2R1, some Accused Products have supported Mapping of Address and Port with Encapsulation.

This topic provides an overview of Mapping of Address and Port with Encapsulation (MAP-E) feature and its benefit to service providers when used as an inline service on MX Series routers with MPC and MIC interfaces. Starting in Junos OS release 20.2R1, MAP-E softwires are supported under Next Gen Services on either an MPC or MIC by specifying the inline services `si-1/1/0` naming convention. Starting in Junos OS release 20.3R1, MPC10E and MX2K-MPC11E support MAP-E.

Adaptive Services Guide at 370; Next Gen Guide at 245.

Release History Table

Release	Description
22.3R1	Starting in Junos OS Release 22.3R1, the line cards on MX series routers support partial reassembly of IPv4 fragments for MAP-E.
20.3R1	Starting in Junos OS release 20.3R1, MPC10E and MX2K-MPC11E support MAP-E.
20.2R1	Starting in Junos OS release 20.2R1, MAP-E softwires are supported under Next Gen Services on either an MPC or MIC by specifying the inline services `si-1/1/0` naming convention.

Adaptive Services Guide at 374; Next Gen Guide at 251.

105. Juniper implements MAP-E as described by IETF RFC 7597:

Internet Engineering Task Force (IETF) — O. Troan, Ed.
Request for Comments: 7597 — W. Dec
Category: Standards Track — Cisco Systems
ISSN: 2070-1721 — X. Li
C. Bao
Tsinghua University
S. Matsushima
SoftBank Telecom
T. Murakami
IP Infusion
T. Taylor, Ed.
Huawei Technologies
July 2015

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; *see also* Adaptive Services Guide at 373; Next Gen Guide at 249.

106. The Accused Products, when operating with the MAP-E functionality, are capable of being used as MAP Border Relays (BR) in which they route an IP data packet in a telecommunications network to a destination equipment, as illustrated below:

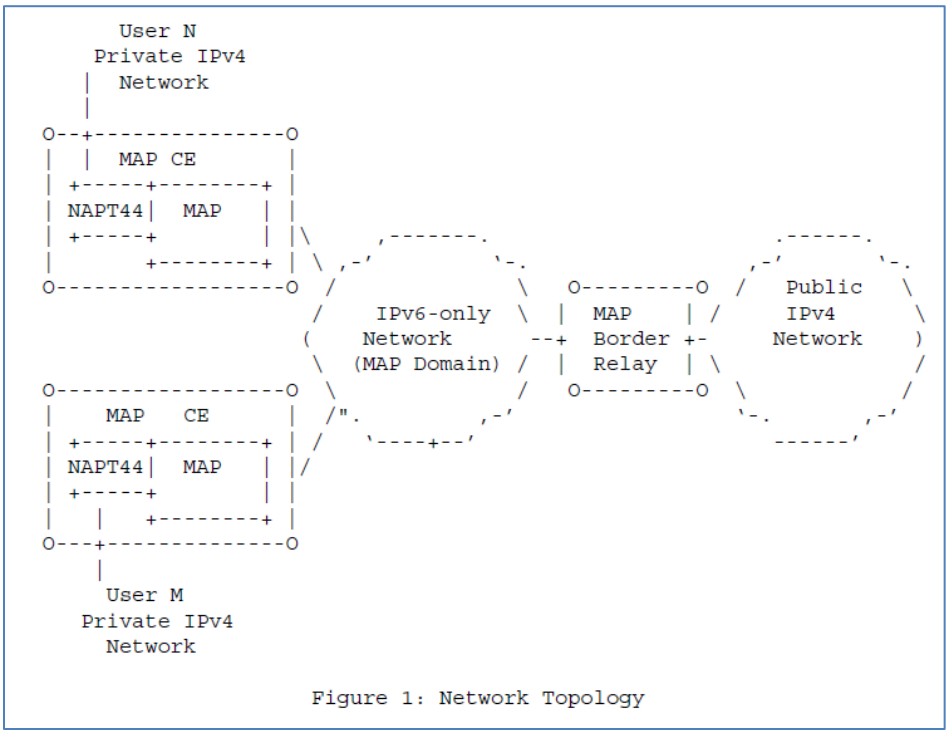
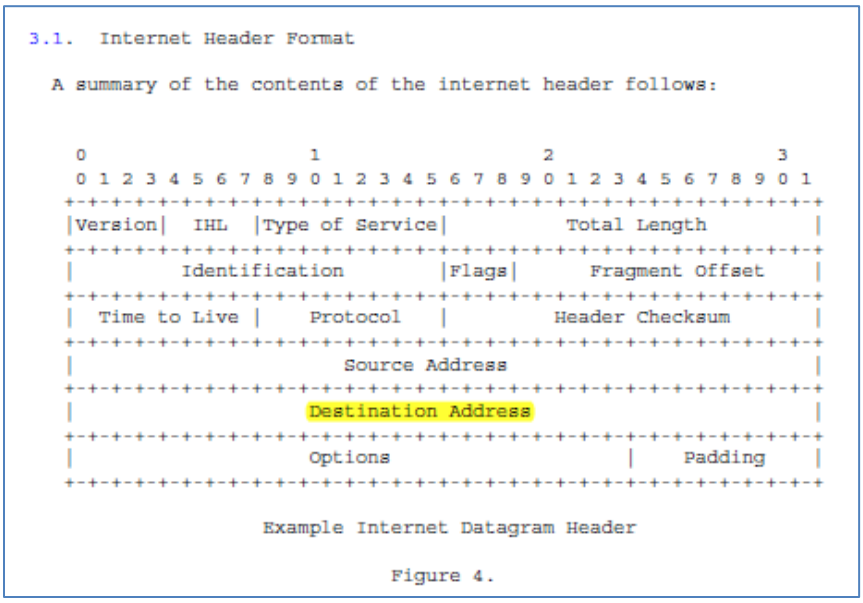


Figure 1: Network Topology

RFC 7597 at 8. Accordingly, the Accused Products, operating in an IPv6 domain, receive data packets from the IPv4 network in which those packets include an IPv4 destination address and a destination port number, corresponding to the primary destination address and a destination port number.

107. IPv4 packets (or Internet Protocol v4 packets), by definition, include IPv4 source and destination addresses. RFC 791 establishes the standard internet protocol. This RFC defines the IPv4 packet:



3.1. Internet Header Format

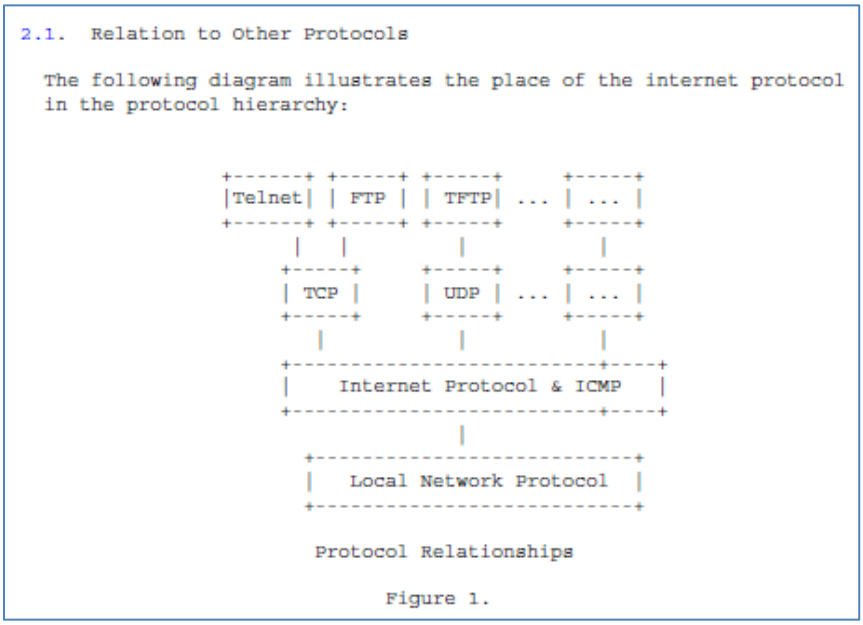
A summary of the contents of the internet header follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet Datagram Header

Figure 4.

https://tools.ietf.org/html/rfc791 ("RFC 791") at 11. Additionally, many 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.



2.1. Relation to Other Protocols

The following diagram illustrates the place of the internet protocol in the protocol hierarchy:

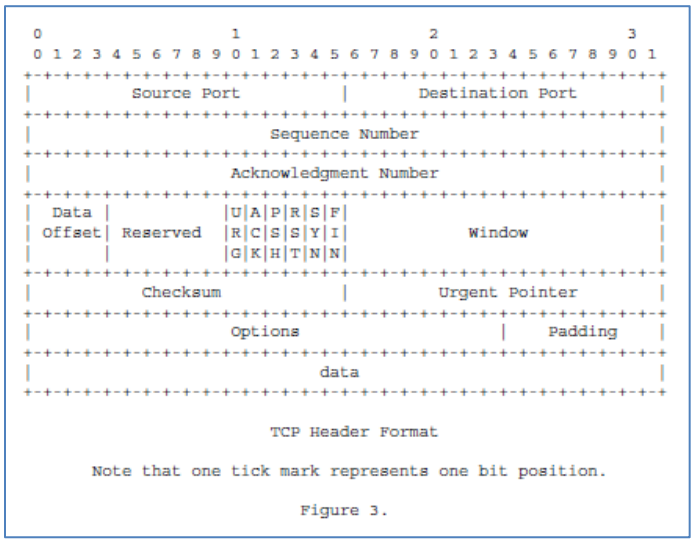
```
+------+ +-----+ +-----+     +-----+
|Telnet| | FTP | | TFTP| ... | ... |
+------+ +-----+ +-----+     +-----+
      |   |         |           |
    +-----+     +-----+     +-----+
    | TCP |     | UDP | ... | ... |
    +-----+     +-----+     +-----+
       |           |           |
    +---------------------------+----+
    |    Internet Protocol & ICMP    |
    +---------------------------+----+
                    |
      +-----------------------------+
      |   Local Network Protocol    |
      +-----------------------------+
```

Protocol Relationships

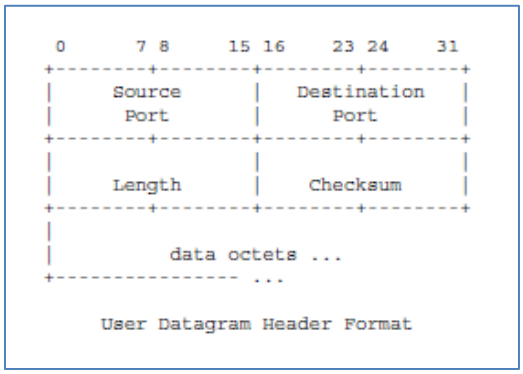
Figure 1.

RFC 791 at 5.

108. The port numbers are illustrated below in the header formats for the TCP protocol:



https://tools.ietf.org/html/rfc793 ("RFC 793") at 15 (illustrating the TCP header format). The port numbers are illustrated below in the header formats for the UDP protocol.



https://tools.ietf.org/html/rfc768 ("RFC 768") at 1.

109. To facilitate traffic across MAP domains, the Accused Products use mapping rules, referred to in the RFCs as Basic Mapping Rule and Forwarding Mapping Rule. The Mapping Rule requires identification of the following: (1) Rule IPv6 prefix; (2) Rule IPv4 prefix; and (3) EA bit length.

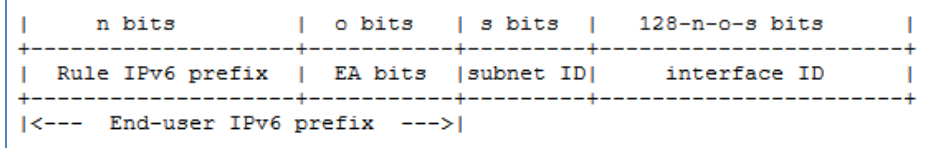
> **5. Mapping Algorithm**
>
> A MAP node is provisioned with one or more mapping rules.
>
> Mapping rules are used differently, depending on their function. Every MAP node must be provisioned with a Basic Mapping Rule. This is used by the node to configure its IPv4 address, IPv4 prefix, or shared IPv4 address. This same basic rule can also be used for forwarding, where an IPv4 destination address and, optionally, a destination port are mapped into an IPv6 address. Additional mapping rules are specified to allow for multiple different IPv4 subnets to exist within the domain and optimize forwarding between them.

> There are two types of mapping rules:
>
> 1. Basic Mapping Rule (BMR) - mandatory. A CE can be provisioned with multiple End-user IPv6 prefixes. There can only be one Basic Mapping Rule per End-user IPv6 prefix. However, all CEs having End-user IPv6 prefixes within (aggregated by) the same Rule IPv6 prefix may share the same Basic Mapping Rule. In combination with the End-user IPv6 prefix, the Basic Mapping Rule is used to derive the IPv4 prefix, address, or shared address and the PSID assigned to the CE.
>
> 2. Forwarding Mapping Rule (FMR) - optional; used for forwarding. The Basic Mapping Rule may also be a Forwarding Mapping Rule. Each Forwarding Mapping Rule will result in an entry in the rule table for the Rule IPv4 prefix. Given a destination IPv4 address and port within the MAP domain, a MAP node can use the matching FMR to derive the End-user IPv6 address of the interface through which that IPv4 destination address and port combination can be reached. In hub-and-spoke mode, there are no FMRs.
>
> 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)

RFC 7597 at 8-9.

110. When a packet is received by the Accused Product with a destination IPv4 address that matches the IPv4 address prefix of a mapping rule, the Accused Product constructs 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 on an IPv4 domain.

111. The destination IPv6 address is constructed as described below according to the MAP-E RFC. It involves concatenating (1) an IPv6 prefix, (2) a sequence of Embedded Address (EA) bits, which include a designated Port Set ID (PSID) for the destination equipment, and (3) an interface ID, which includes the complete IPv4 destination address and PSID port number.

> Figure 3 shows the structure of the complete MAP IPv6 address as specified in this document.
>
> 
>
>
> 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, which is unique for a given Rule IPv6 prefix, can contain a full or partial IPv4 address and, in the shared IPv4 address case, a PSID. An EA bit field length of 0 signifies that all relevant MAP IPv4 addressing information is passed directly in the BMR and is not derived from the EA bit field in the End-user IPv6 prefix.
>
> The MAP IPv6 address is created by concatenating the End-user IPv6 prefix with the MAP subnet identifier (if the End-user IPv6 prefix is shorter than 64 bits) and the interface identifier as specified in Section 6.

RFC 7597 at 12.

112. The EA bits identified in the RFC include a port set identifier (PSID) that represents a port mask defining a range of port numbers assigned to the destination equipment. The received destination port number is associated with the PSID used to construct the resulting IPv6 address.

> 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.

RFC 7597 at 7.

113. 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, supported by the accused Juniper devices, the EA bits represent an encoding of both an IPv4 address and a destination port, as claimed.

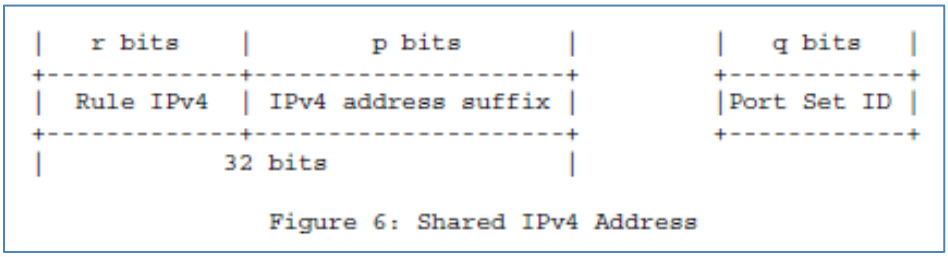


Figure 6: Shared IPv4 Address

RFC7597 at 13.

114. The combined Rule IPv4 and IPv4 address suffix form the destination address. The PSID corresponds to 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 the port mask.

115. By constructing the IPv6 address, the Accused Products select at least one identifier of the destination equipment of the packet (i.e., the constructed IPv6 address). When using EA bits according to the third form identified above, a shared IPv4 address and a Port Set Identifier (PSID), the Accused Products associate a multiple destination devices (i.e., MAP CE components) with a single shared IP destination address. Each such CE component has an associated equipment identifier, such as its corresponding MAP IPv6 address (which is constructed at the BR – as detailed above) or the interface ID component of that MAP IPv6 address, detailed below.

116. Additionally, the complete IPv4 destination address and PSID destination port number is appended to the IPv6 operator prefix as part of the interface ID. The format of the interface ID, which includes the destination IPv4 address and PSID, is illustrated below:

6. The IPv6 Interface Identifier

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

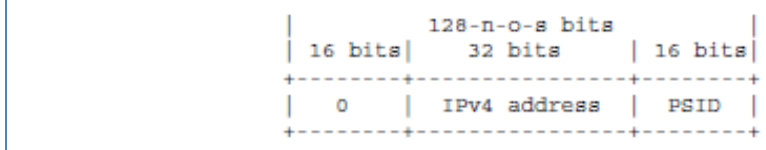


Figure 8: IPv6 Interface Identifier

RFC 7597 at 15.

117. Thus, both the constructed MAP IPv6 destination address and its interface ID component represent at least one identifier of the destination equipment that is selected from a plurality of equipment identifiers associated with said primary destination address. And this selection is based on the PSID, or port mask.

118. 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. The Accused Products are routers, and thus support the routing of constructed IPv6 packets in the MAP domain. A MAP Border Relay (BR) is defined to be a MAP-enabled router.

MAP Border Relay (BR): A MAP-enabled router managed by the service provider at the edge of a MAP domain. A BR has at least an IPv6-enabled interface and an IPv4 interface connected to the native IPv4 network. A MAP BR may also be referred to as simply a "BR" within the context of MAP.

RFC 7597 at 6.

119. The IPv6 packet is routed to its destination based on the at least one identifier of the destination equipment of the packet (*e.g.*, the MAP IPv6 destination address or the interface ID component of that address).

120. Juniper's infringement of the '369 Patent has been and continues to be deliberate and willful, and therefore, this is an exceptional case warranting an award of enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284-285.

121. As a result of Juniper's infringement of the '369 Patent, Monarch has suffered monetary damages and seeks recovery in an amount adequate to compensate for Juniper's infringement, but in no event less than a reasonable royalty with interest and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests entry of judgment in its favor and against Defendant Juniper as follows:

(a) Declaring that Defendant Juniper has infringed and continues to infringe U.S. Patent Nos. 8,451,844; 8,451,845; 8,130,775; and 8,693,369;

(b) Declaring that Defendant Juniper's infringement of each Asserted Patent has been willful and deliberate;

(c) Awarding all damages sustained by Plaintiff as the result of Juniper's acts of infringement in an amount no less than a reasonable royalty for Defendant's infringement of each Asserted Patent, together with prejudgment and post-judgment interest and without limitation under 35 U.S.C. § 287;

(d) Enhancing damages pursuant to 35 U.S.C. § 284;

(e) Declaring that royalties shall be payable on each and every future sale by Juniper 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) Awarding attorneys' fees pursuant to 35 U.S.C. § 285 or otherwise permitted by law;

(g) Awarding such other costs 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: May 23, 2023

Respectfully submitted,

/s/ Walter D. Kelley, Jr
Walter D. Kelley, Jr. (VSB No. 21622)
wkelley@hausfeld.com
Tara R. Zurawski (VSB No. 73602)
tzurawski@hausfeld.com
HAUSFELD LLP
888 16th Street, NW, Suite 300
Washington, D.C. 20006
Tel: 202-54-7157
Fax: 202-540-7200

Michael F. Heim (*pro hac* pending)
Texas Bar No. 09380923
mheim@hpcllp.com
R. Allan Bullwinkel (*pro hac* pending)
Texas Bar No. 24064327
abullwinkel@hpcllp.com
Alden G. Harris (*pro hac* pending)
Texas Bar No. 24083138
aharris@hpcllp.com
Eric J. Enger (*pro hac* pending)
Texas Bar No. 24045833
eenger@hpcllp.com
William B. Collier, Jr. (*pro hac* pending)
Texas Bar No. 24097519
wcollier@hpcllp.com
HEIM, PAYNE & CHORUSH, LLP
1111 Bagby St. Ste. 2100
Houston, Texas 77002
Telephone: (713) 221-2000
Facsimile: (713) 221-2021

Max L. Tribble Jr. (*pro hac* pending)
Texas Bar No. 20213950
mtribble@susmangodfrey.com
Joseph S. Grinstein (*pro hac* pending)
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 (*pro hac* pending)
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

Steven M. Seigel (*pro hac* pending)
Washington State Bar No. 53960
sseigel@susmangodfrey.com
SUSMAN GODFREY L.L.P.
401 Union Street, Suite 3000
Seattle, WA 98101
Telephone: (206) 516-3880
Facsimile: (206) 516-3883

ATTORNEYS FOR MONARCH NETWORKING SOLUTIONS LLC